Quantum Information Theory

Yury Holubeu *

November 16, 2025

This note is not intended for distribution. Quantum information theory discussed in detail. The note has solved problems and summary of special topics. Readers who have opened this note for the first time are highly recommended to read the preface.

Contents

Preface and main motivation **21**

I —— Typical Quantum Inform Theory in a Nutshell —— **22**

1 Basic Methods and Concepts **22**
1.1 Basic Methods of Quantum Information . . . 22
1.1.1 Definitions and Meaning of States, Entanglement, and Measurements . . . 22
1.1.2 Typical Quantum Gates . . . 25
1.1.3 Transformations of States, the Simplest Quantum Gates . . . 25
1.1.4 Definitions of Operators and Mappings . . . 26
1.1.5 Density Matrix Formalism . . . 26
1.1.6 Entropies in Quantum Information . . . 27
1.1.7 Basic Quantum Algorithms . . . 27
1.1.8 Quantum Channels: Basics . . . 27
1.1.9 Quantum Channels: Special Features . . . 29
1.2 Other General Basic Topics . . . 29
1.2.1 General ways to compute something with cubits? . . . 29
1.2.2 General ways to compute something with superconductors . . . 29
1.2.3 Experimental Tests of Fundamentals of QM . . . 30

II —— Special Topics in a Nutshell —— **31**

2 Special Well-Researched Topics **31**
2.1 Tensor Networks . . . 31
2.2 Tensor Networks . . . 31
2.3 Quantum Cryptography . . . 31
2.3.1 Ф-л7. MPS, MPO . . . 31
2.3.2 Ф-л8. MERA . . . 31
2.4 Reminder: Basics of QM . . . 31
2.4.1 Ф-л9. Second Quantization . . . 31

3 Some Other Topics **31**
3.1 Exotic Quantum Gates and Transformation . . . 31
3.1.1 Quantum Search . . . 31
3.2 Overview of Main Special Topics . . . 31
3.2.1 Quantum Cryptography: Main Things to Know . . . 31
3.2.2 Quantum Error Correction: Main Things to Know . . . 32
3.3 Holevo's Book . . . 32
3.3.1 Введение . . . 32
3.3.2 X1. Standard Statistical Model of Quantum Mechanics . . . 32
3.3.3 X2. Statistics of Quantum Measurements . . . 32
3.3.4 X3. Evolution of an Open System . . . 32
3.3.5 X4. Consistent and Continuous Measurement Processes . . . 33

*https://yuriholubeu.github.io/, yuri.holubev@gmail.com

3.3.6 X5. Processes in the Fock Space . . . 33
3.4 Wheeler's and Zurek's Book . . . 33
3.5 Some Other Well-Known Articles . . . 33
3.5.1 Decoherence, Einselection, and the Quantum Origins of the Classical by Zurek 33

III Fundamentals of Quantum Information Theory 34

4 Basics of Quantum Information Theory 34
4.1 Quantum Noise . . . 34
4.2 Quantum Transformations . . . 34
4.3 Entropy in Quantum Information . . . 34

5 Quantum Polarization States of Photon by Filippov 34
5.0.1 1. Introduction . . . 34
5.0.2 2. Polarization of Classical Electromagnetic Waves . . . 35
5.0.3 3. Quantum Description of the Polarization of Single Photons . . . 35
5.0.4 4. A Unitary Space . . . 39
5.0.5 5. Measurements and Observables . . . 40
5.0.6 5.4. Phase Shift . . . 44
5.0.7 6. The Poincare Sphere . . . 45
5.0.8 7. The Density Matrix of the Ensemble . . . 45
5.0.9 8. Partially Polarized Light . . . 47
5.0.10 9. Quantum Cryptography . . . 48
5.0.11 10. Two-Photon Entangled States . . . 49
5.0.12 11. Ultra-Dense Coding . . . 51
5.0.13 12. Measurement in the Bell State Basis . . . 51
5.0.14 13. Quantum Teleportation . . . 54
5.0.15 14. Polarization of an Arbitrary Multiphoton State . . . 55
5.0.16 15. Quantum Channels . . . 56

6 Lectures on Mathematical Fundamentals of QM by Amosov 57
6.1 A.1 . . . 58
6.1.1 1.1. Mackey 's Axioms . . . 58
6.1.2 1.2. Schrodinger and Heisenberg's Approaches to Quantum Mechanics . . . 59
6.2 A.2 . . . 61
6.2.1 2.1. The Relationship Between Schrodinger's and Heisenberg's Approaches . . . 61
6.2.2 2.2. Functional Calculus for Self-Adjoint Operators . . . 62
6.2.3 2.3. Nuclear Operators . . . 68
6.2.4 2.4. Further Properties of Nuclear Operators . . . 70
6.3 A.3 . . . 72
6.3.1 3.1. Positive Operator - Valued Measures . . . 72
6.3.2 3.2. Holevo 's Theorem . . . 72
6.3.3 3.3. Classical and Quantum Probability Theories (??!!!) . . . 74
6.3.4 3.4. Quantum Random Variables (Observables) Using the Example of a Quantum Harmonic Oscillator . . . 77
6.3.5 3.5. Randomization . . . 81
6.3.6 3.6. The Ratio of Uncertainties . . . 81
6.3.7 3.7. Classical and Quantum Covariance . . . 82
6.4 A.4 . . . 83
6.4.1 4.1. Composite Quantum Systems . . . 83
6.4.2 4.2. The State of Purification . . . 84
6.4.3 4.3. Tsirelson Boundary . . . 85
6.5 A.5 . . . 88

6.5.1 5.1. Eigenfunctions and Eigenvalues of the Fourier Transform . . . 88
6.5.2 5.2. The Action of a Group of Unitary Operators Associated with a QHO on Canonical Observables . . . 89
6.5.3 5.3. A Family of Unitary Transformations of Canonical Observables . . . 91
6.6 A.6 . . . 92
6.6.1 6.1. The Task of Error- Free Coding . . . 92
6.6.2 6.2. Encoding of Quantum Information . . . 93
6.6.3 6.3. Covariant Positive Operator - Valued Measures . . . 94
6.7 A.7 . . . 96
6.7.1 7.1. Classical and Quantum Random Processes (!!!!) . . . 96
6.7.2 7.2. Symmetric Fock Space . . . 97
6.7.3 7.3. Realization of Wiener and Poisson Processes in Fock's Space . . . 100
6.8 A.8 . . . 102
6.8.1 8.1. Tomographic Representation of Quantum Mechanics . . . 102
6.8.2 8.2. The Finite - Dimensional Case . . . 103
6.8.3 8.3. Representation by Characteristic Functions . . . 103
6.8.4 8.4. Representation by Quasi - Distributions . . . 106
6.8.5 8.5. Optical Tomogram Presentation and Its Dual . . . 108
6.9 A.9 . . . 108
6.9.1 9.1. Quantum Dynamic Mappings . . . 108
6.9.2 9.2. Defacing Channels . . . 111

7 I Fundamental concepts by Nielsen, Chang 113
7.0.1 Preface . . . 113
7.0.2 Nomenclature and notation . . . 120
7.1 1 Introduction and overview . . . 123
7.1.1 1.1 Global perspectives . . . 123
7.1.2 1.1.1 History of quantum computation and quantum information . . . 124
7.1.3 1.1.2 Future directions . . . 133
7.1.4 1.2 Quantum bits . . . 133
7.1.5 1.2.1 Multiple qubits . . . 137
7.1.6 1.3 Quantum computation . . . 138
7.1.7 1.3.1 Single qubit gates . . . 138
7.1.8 1.3.2 Multiple qubit gates . . . 141
7.1.9 1.3.3 Measurements in bases other than the computational basis . . . 142
7.1.10 1.3.4 Quantum circuits . . . 143
7.1.11 1.3.5 Qubit copying circuit? . . . 145
7.1.12 1.3.6 Example: Bell states . . . 146
7.1.13 1.3.7 Example: quantum teleportation . . . 146
7.1.14 1.4 Quantum algorithms . . . 149
7.1.15 1.4.1 Classical computations on a quantum computer . . . 149
7.1.16 1.4.2 Quantum parallelism . . . 151
7.1.17 1.4.3 Deutsch's algorithm . . . 153
7.1.18 1.4.4 The Deutsch-Jozsa algorithm . . . 155
7.1.19 1.4.5 Quantum algorithms summarized . . . 157
7.1.20 1.5 Experimental quantum information processing . . . 163
7.1.21 1.5.1 The Stern-Gerlach experiment . . . 163
7.1.22 1.5.2 Prospects for practical quantum information processing . . . 166
7.1.23 1.6 Quantum information . . . 170
7.1.24 1.6.1 Quantum information theory: example problems . . . 171
7.1.25 1.6.2 Quantum information in a wider context . . . 176
7.2 2 Introduction to quantum mechanics . . . 178
7.2.1 2.1 Linear algebra . . . 179
7.2.2 2.1.1 Bases and linear independence . . . 180

7.2.3 2.1.2 Linear operators and matrices . . . 181
7.2.4 2.1.3 The Pauli matrices . . . 182
7.2.5 2.1.4 Inner products . . . 183
7.2.6 2.1.5 Eigenvectors and eigenvalues . . . 186
7.2.7 2.1.6 Adjoints and Hermitian operators . . . 186
7.2.8 2.1.7 Tensor products . . . 188
7.2.9 2.1.8 Operator functions . . . 191
7.2.10 2.1.9 The commutator and anti-commutator . . . 193
7.2.11 2.1.10 The polar and singular value decompositions . . . 194
7.2.12 2.2 The postulates of quantum mechanics . . . 195
7.2.13 2.2.1 State space . . . 196
7.2.14 2.2.2 Evolution . . . 197
7.2.15 2.2.3 Quantum measurement . . . 200
7.2.16 2.2.4 Distinguishing quantum states . . . 201
7.2.17 2.2.5 Projective measurements . . . 202
7.2.18 2.2.6 POVM measurements . . . 205
7.2.19 2.2.7 Phase . . . 207
7.2.20 2.2.8 Composite systems . . . 208
7.2.21 2.2.9 Quantum mechanics: a global view . . . 210
7.2.22 2.3 Application: superdense coding . . . 211
7.2.23 2.4 The density operator . . . 212
7.2.24 2.4.1 Ensembles of quantum states . . . 213
7.2.25 2.4.2 General properties of the density operator . . . 215
7.2.26 2.4.3 The reduced density operator . . . 219
7.2.27 2.5 The Schmidt decomposition and purifications . . . 222
7.2.28 2.6 EPR and the Bell inequality . . . 224
7.3 3 Introduction to computer science . . . 232
7.3.1 3.1 Models for computation . . . 233
7.3.2 3.1.1 Turing machines . . . 234
7.3.3 3.1.2 Circuits . . . 240
7.3.4 3.2 The analysis of computational problems . . . 245
7.3.5 3.2.1 How to quantify computational resources . . . 246
7.3.6 3.2.2 Computational complexity . . . 248
7.3.7 3.2.3 Decision problems and the complexity classes P and NP . . . 250
7.3.8 3.2.4 A plethora of complexity classes . . . 259
7.3.9 3.2.5 Energy and computation . . . 261
7.3.10 3.3 Perspectives on computer science . . . 269

8 II Quantum computation by Nielsen, Chang 276
8.1 4 Quantum circuits . . . 276
8.1.1 4.1 Quantum algorithms . . . 277
8.1.2 4.2 Single qubit operations . . . 279
8.1.3 4.3 Controlled operations . . . 282
8.1.4 4.4 Measurement . . . 290
8.1.5 4.5 Universal quantum gates . . . 294
8.1.6 4.5.1 Two-level unitary gates are universal . . . 294
8.1.7 4.5.2 Single qubit and CNOT gates are universal . . . 296
8.1.8 4.5.3 A discrete set of universal operations . . . 298
8.1.9 4.5.4 Approximating arbitrary unitary gates is generically hard . . . 303
8.1.10 4.5.5 Quantum computational complexity . . . 305
8.1.11 4.6 Summary of the quantum circuit model of computation . . . 307
8.1.12 4.7 Simulation of quantum systems . . . 308
8.1.13 4.7.1 Simulation in action . . . 309
8.1.14 4.7.2 The quantum simulation algorithm . . . 310

8.1.15 4.7.3 An illustrative example . . . 313
8.1.16 4.7.4 Perspectives on quantum simulation . . . 315
8.1.17 Summary of Chapter 4: Quantum circuits . . . 317
8.2 5 The quantum Fourier transform and its applications . . . 318
8.2.1 5.1 The quantum Fourier transform . . . 319
8.2.2 5.2 Phase estimation . . . 323
8.2.3 5.2.1 Performance and requirements . . . 325
8.2.4 5.3 Applications: order-finding and factoring . . . 327
8.2.5 5.3.1 Application: order-finding . . . 328
8.2.6 The continued fraction expansion . . . 330
8.2.7 5.3.2 Application: factoring . . . 333
8.2.8 5.4 General applications of the quantum Fourier transform . . . 335
8.2.9 5.4.1 Period-finding . . . 336
8.2.10 5.4.2 Discrete logarithms . . . 338
8.2.11 5.4.3 The hidden subgroup problem . . . 340
8.2.12 5.4.4 Other quantum algorithms? . . . 342
8.2.13 Summary of Chapter 5: The quantum Fourier transform and its applications . . . 344
8.3 6 Quantum search algorithms . . . 346
8.3.1 6.1 The quantum search algorithm . . . 346
8.3.2 6.1.1 The oracle . . . 346
8.3.3 6.1.2 The procedure . . . 348
8.3.4 6.1.3 Geometric visualization . . . 349
8.3.5 6.1.4 Performance . . . 351
8.3.6 6.2 Quantum search as a quantum simulation . . . 353
8.3.7 6.3 Quantum counting . . . 360
8.3.8 6.4 Speeding up the solution of NP-complete problems . . . 362
8.3.9 6.5 Quantum search of an unstructured database . . . 363
8.3.10 6.6 Optimality of the search algorithm . . . 366
8.3.11 6.7 Black box algorithm limits . . . 369
8.3.12 Summary of Chapter 6: Quantum search algorithms . . . 372
8.4 7 Quantum computers: physical realization . . . 373
8.4.1 7.1 Guiding principles . . . 374
8.4.2 7.2 Conditions for quantum computation . . . 375
8.4.3 7.2.1 Representation of quantum information . . . 376
8.4.4 7.2.2 Performance of unitary transformations . . . 377
8.4.5 7.2.3 Preparation of fiducial initial states . . . 378
8.4.6 7.2.4 Measurement of output result . . . 378
8.4.7 7.3 Harmonic oscillator quantum computer . . . 379
8.4.8 7.3.1 Physical apparatus . . . 379
8.4.9 7.3.2 The Hamiltonian . . . 380
8.4.10 7.3.3 Quantum computation . . . 382
8.4.11 7.3.4 Drawbacks . . . 382
8.4.12 7.4 Optical photon quantum computer . . . 383
8.4.13 7.4.1 Physical apparatus . . . 383
8.4.14 7.4.2 Quantum computation . . . 386
8.4.15 7.4.3 Drawbacks . . . 391
8.4.16 7.5 Optical cavity quantum electrodynamics . . . 392
8.4.17 7.5.1 Physical apparatus . . . 393
8.4.18 7.5.2 The Hamiltonian . . . 395
8.4.19 7.5.3 Single-photon single-atom absorption and refraction . . . 397
8.4.20 7.5.4 Quantum computation . . . 400
8.4.21 7.6 Ion traps . . . 403
8.4.22 7.6.1 Physical apparatus . . . 404

8.4.23 7.6.2 The Hamiltonian . . . 411
8.4.24 7.6.3 Quantum computation . . . 413
8.4.25 7.6.4 Experiment . . . 416
8.4.26 7.7 Nuclear magnetic resonance . . . 419
8.4.27 7.7.1 Physical apparatus . . . 420
8.4.28 7.7.2 The Hamiltonian . . . 421
8.4.29 7.7.3 Quantum computation . . . 426
8.4.30 7.7.4 Experiment . . . 430
8.4.31 7.8 Other implementation schemes . . . 437
8.4.32 Summary of Chapter 7: Quantum computers: physical realization . . . 442

9 III Quantum information by Nielsen, Chang 445
9.1 8 Quantum noise and quantum operations . . . 445
9.1.1 8.1 Classical noise and Markov processes . . . 446
9.1.2 8.2 Quantum operations . . . 448
9.1.3 8.2.1 Overview . . . 448
9.1.4 8.2.2 Environments and quantum operations . . . 449
9.1.5 8.2.3 Operator-sum representation . . . 451
9.1.6 8.2.4 Axiomatic approach to quantum operations . . . 458
9.1.7 8.3 Examples of quantum noise and quantum operations . . . 464
9.1.8 8.3.1 Trace and partial trace . . . 465
9.1.9 8.3.2 Geometric picture of single qubit quantum operations . . . 465
9.1.10 8.3.3 Bit flip and phase flip channels . . . 466
9.1.11 8.3.4 Depolarizing channel . . . 468
9.1.12 8.3.5 Amplitude damping . . . 470
9.1.13 8.3.6 Phase damping . . . 474
9.1.14 8.4 Applications of quantum operations . . . 476
9.1.15 8.4.1 Master equations . . . 476
9.1.16 8.4.2 Quantum process tomography . . . 479
9.1.17 8.5 Limitations of the quantum operations formalism . . . 484
9.1.18 Summary of Chapter 8: Quantum noise and quantum operations . . . 486
9.2 9 Distance measures for quantum information . . . 487
9.2.1 9.1 Distance measures for classical information . . . 488
9.2.2 9.2 How close are two quantum states? . . . 491
9.2.3 9.2.1 Trace distance . . . 491
9.2.4 9.2.2 Fidelity . . . 497
9.2.5 9.2.3 Relationships between distance measures . . . 503
9.2.6 9.3 How well does a quantum channel preserve information? . . . 505
9.3 10 Quantum error-correction . . . 512
9.3.1 10.1 Introduction . . . 513
9.3.2 10.1.1 The three qubit bit flip code . . . 514
9.3.3 10.1.2 Three qubit phase flip code . . . 518
9.3.4 10.2 The Shor code . . . 519
9.3.5 10.3 Theory of quantum error-correction . . . 522
9.3.6 10.3.1 Discretization of the errors . . . 525
9.3.7 10.3.2 Independent error models . . . 528
9.3.8 10.3.3 Degenerate codes . . . 530
9.3.9 10.3.4 The quantum Hamming bound . . . 531
9.3.10 10.4 Constructing quantum codes . . . 531
9.3.11 10.4.1 Classical linear codes . . . 532
9.3.12 10.4.2 Calderbank-Shor-Steane codes . . . 535
9.3.13 10.5 Stabilizer codes . . . 539
9.3.14 10.5.1 The stabilizer formalism . . . 539
9.3.15 10.5.2 Unitary gates and the stabilizer formalism . . . 543

9.3.16 10.5.3 Measurement in the stabilizer formalism . . . 547
9.3.17 10.5.4 The Gottesman-Knill theorem . . . 548
9.3.18 10.5.5 Stabilizer code constructions . . . 549
9.3.19 10.5.6 Examples . . . 551
9.3.20 10.5.7 Standard form for a stabilizer code . . . 554
9.3.21 10.5.8 Quantum circuits for encoding, decoding, and correction . . . 555
9.3.22 10.6 Fault-tolerant quantum computation . . . 558
9.3.23 10.6.1 Fault-tolerance: the big picture . . . 558
9.3.24 10.6.2 Fault-tolerant quantum logic . . . 565
9.3.25 10.6.3 Fault-tolerant measurement . . . 572
9.3.26 10.6.4 Elements of resilient quantum computation . . . 577
9.3.27 Summary of Chapter 10: Quantum error-correction . . . 579
9.4 11 Entropy and information . . . 582
9.4.1 11.1 Shannon entropy . . . 582
9.4.2 11.2 Basic properties of entropy . . . 583
9.4.3 11.2.1 The binary entropy . . . 583
9.4.4 11.2.2 The relative entropy . . . 586
9.4.5 11.2.3 Conditional entropy and mutual information . . . 587
9.4.6 11.2.4 The data processing inequality . . . 590
9.4.7 11.3 Von Neumann entropy . . . 591
9.4.8 11.3.1 Quantum relative entropy . . . 592
9.4.9 11.3.2 Basic properties of entropy . . . 593
9.4.10 11.3.3 Measurements and entropy . . . 595
9.4.11 11.3.4 Subadditivity . . . 596
9.4.12 11.3.5 Concavity of the entropy . . . 597
9.4.13 11.3.6 The entropy of a mixture of quantum states . . . 598
9.4.14 11.4 Strong subadditivity . . . 599
9.4.15 11.4.1 Proof of strong subadditivity . . . 600
9.4.16 11.4.2 Strong subadditivity: elementary applications . . . 602
9.4.17 Summary of Chapter 11: Entropy and information . . . 605
9.5 12 Quantum information theory . . . 606
9.5.1 12.1 Distinguishing quantum states and the accessible information . . . 608
9.5.2 12.1.1 The Holevo bound . . . 610
9.5.3 12.1.2 Example applications of the Holevo bound . . . 612
9.5.4 12.2 Data compression . . . 614
9.5.5 12.2.1 Shannon's noiseless channel coding theorem . . . 615
9.5.6 12.2.2 Schumacher's quantum noiseless channel coding theorem . . . 620
9.5.7 12.3 Classical information over noisy quantum channels . . . 624
9.5.8 12.3.1 Communication over noisy classical channels . . . 625
9.5.9 12.3.2 Communication over noisy quantum channels . . . 631
9.5.10 12.4 Quantum information over noisy quantum channels . . . 638
9.5.11 12.4.1 Entropy exchange and the quantum Fano inequality . . . 638
9.5.12 12.4.2 The quantum data processing inequality . . . 640
9.5.13 12.4.3 Quantum Singleton bound . . . 644
9.5.14 12.4.4 Quantum error-correction, refrigeration and Maxwell's demon . . . 645
9.5.15 12.5 Entanglement as a physical resource . . . 647
9.5.16 12.5.1 Transforming bi-partite pure state entanglement . . . 649
9.5.17 12.5.2 Entanglement distillation and dilution . . . 654
9.5.18 12.5.3 Entanglement distillation and quantum error-correction . . . 656
9.5.19 12.6 Quantum cryptography . . . 658
9.5.20 12.6.1 Private key cryptography . . . 658
9.5.21 12.6.2 Privacy amplification and information reconciliation . . . 660
9.5.22 12.6.3 Quantum key distribution . . . 662

9.5.23 12.6.4 Privacy and coherent information . . . 667
9.5.24 12.6.5 The security of quantum key distribution . . . 668
9.5.25 Summary of Chapter 12: Quantum information theory . . . 677

10 Quantum Systems, Channels, Information by Holevo 680
10.0.1 Preface . . . 680
10.0.2 Preface to the Second Edition . . . 683
10.1 1 Vectors and Operators . . . 683
10.1.1 1.1 Hilbert Space . . . 683
10.1.2 1.2 Operators . . . 684
10.1.3 1.3 Positivity . . . 685
10.1.4 1.4 Trace and Duality . . . 685
10.1.5 1.5 Convexity . . . 687
10.1.6 1.6 Notes and References . . . 688
10.2 2 States, Observables, Statistics . . . 688
10.2.1 2.1 Structure of Statistical Theories . . . 688
10.2.2 2.1.1 Classical Systems . . . 688
10.2.3 2.1.2 Axioms of Statistical Description . . . 689
10.2.4 2.2 Quantum States . . . 691
10.2.5 2.3 Quantum Observables . . . 693
10.2.6 2.3.1 Quantum Observables from the Axioms . . . 693
10.2.7 2.3.2 Compatibility and Complementarity . . . 694
10.2.8 2.3.3 The Uncertainty Relation . . . 696
10.2.9 2.3.4 Convex Structure of Observables . . . 697
10.2.10 2.4 Statistical Discrimination Between Quantum States . . . 699
10.2.11 2.4.1 Formulation of the Problem . . . 699
10.2.12 2.4.2 Optimal Observables . . . 700
10.2.13 2.5 Notes and References . . . 705
10.3 3 Composite Systems and Entanglement . . . 706
10.3.1 3.1 Composite Systems . . . 706
10.3.2 3.1.1 Tensor Products . . . 706
10.3.3 3.1.2 Naimark's Dilation . . . 707
10.3.4 3.1.3 Schmidt Decomposition and Purification . . . 709
10.3.5 3.2 Quantum Entanglement vs. "Local Realism" . . . 711
10.3.6 3.2.1 Paradox of Einstein-Podolski-Rosen and Bell's Inequalities . . . 711
10.3.7 3.2.2 Mermin-Peres Game . . . 714
10.3.8 3.3 Quantum Systems as Information Carriers . . . 716
10.3.9 3.3.1 Transmission of Classical Information . . . 716
10.3.10 3.3.2 Entanglement and Local Operations . . . 716
10.3.11 3.3.3 Superdense Coding . . . 718
10.3.12 3.3.4 Quantum Teleportation . . . 718
10.3.13 3.4 Notes and References . . . 720
10.4 4 Classical Entropy and Information . . . 721
10.4.1 4.1 Entropy of a Random Variable and Data Compression . . . 721
10.4.2 4.2 Conditional Entropy and the Shannon Information . . . 723
10.4.3 4.3 The Shannon Capacity of the Classical Noisy Channel . . . 725
10.4.4 4.4 The Channel Coding Theorem . . . 727
10.4.5 4.5 Wiretap Channel . . . 731
10.4.6 4.6 Gaussian Channel . . . 732
10.4.7 4.7 Notes and References . . . 733
10.5 5 The Classical-Quantum Channel . . . 734
10.5.1 5.1 Codes and Achievable Rates . . . 734
10.5.2 5.2 Formulation of the Coding Theorem . . . 735
10.5.3 5.3 The Upper Bound . . . 737

10.5.4 5.4 Proof of the Weak Converse . . . 741
10.5.5 5.5 Typical Projectors . . . 744
10.5.6 5.6 Proof of the Direct Coding Theorem . . . 748
10.5.7 5.7 The Reliability Function for Pure-State Channel . . . 750
10.5.8 5.8 Notes and References . . . 753
10.6 6 Quantum Evolutions and Channels . . . 754
10.6.1 6.1 Quantum Evolutions . . . 754
10.6.2 6.2 Completely Positive Maps . . . 756
10.6.3 6.3 Definition of the Channel . . . 761
10.6.4 6.4 Entanglement-Breaking and PPT Channels . . . 763
10.6.5 6.5 Quantum Measurement Processes . . . 765
10.6.6 6.6 Complementary Channels . . . 767
10.6.7 6.7 Covariant Channels . . . 770
10.6.8 6.8 Qubit Channels . . . 773
10.6.9 6.9 Notes and References . . . 774
10.7 7 Quantum Entropy and Information Quantities . . . 775
10.7.1 7.1 Quantum Relative Entropy . . . 775
10.7.2 7.2 Monotonicity of the Relative Entropy . . . 776
10.7.3 7.3 Strong Subadditivity of the Quantum Entropy . . . 780
10.7.4 7.4 Continuity Properties . . . 782
10.7.5 7.5 Information Correlation, Entanglement of Formation, and Conditional Entropy 783
10.7.6 7.6 Entropy Exchange . . . 787
10.7.7 7.7 Quantum Mutual Information . . . 789
10.7.8 7.8 Notes and References . . . 791
10.8 8 The Classical Capacity of Quantum Channels . . . 792
10.8.1 8.1 The Coding Theorem . . . 792
10.8.2 8.2 The χ-Capacity . . . 794
10.8.3 8.3 The Additivity Problem . . . 796
10.8.4 8.3.1 The Effect of Entanglement in Encoding and Decoding . . . 796
10.8.5 8.3.2 A Hierarchy of Additivity Properties . . . 799
10.8.6 8.3.3 Some Entropy Inequalities . . . 801
10.8.7 8.3.4 Additivity for Complementary Channels . . . 803
10.8.8 8.3.5 Nonadditivity of Quantum Entropy Quantities . . . 804
10.8.9 8.4 Notes and References . . . 810
10.9 9 Entanglement-Assisted Classical Communication . . . 811
10.9.1 9.1 The Gain of Entanglement Assistance . . . 811
10.9.2 9.2 The Classical Capacities of Quantum Observables . . . 814
10.9.3 9.3 Proof of the Converse Coding Theorem . . . 818
10.9.4 9.4 Proof of the Direct Coding Theorem . . . 819
10.9.5 9.5 Notes and References . . . 822
10.10 10 Transmission of Quantum Information . . . 822
10.10.1 10.1 Quantum Error-Correcting Codes . . . 823
10.10.2 10.1.1 Error Correction by Repetition . . . 823
10.10.3 10.1.2 General Formulation . . . 824
10.10.4 10.1.3 Necessary and Sufficient Conditions for Error Correction . . . 825
10.10.5 10.1.4 Coherent Information and Perfect Error Correction . . . 826
10.10.6 10.2 Fidelities for Quantum Information . . . 829
10.10.7 10.2.1 Fidelities for Pure States . . . 829
10.10.8 10.2.2 Relations Between the Fidelity Measures . . . 831
10.10.9 10.2.3 Fidelity and the Bures Distance . . . 832
10.10.10 10.3 The Quantum Capacity . . . 835
10.10.11 10.3.1 Achievable Rates . . . 835
10.10.12 10.3.2 The Quantum Capacity and the Coherent Information . . . 838

10.10.13 10.3.3 Degradable Channels . . . 840
10.10.14 10.4 The Private Classical Capacity and the Quantum Capacity . . . 842
10.10.15 10.4.1 The Quantum Wiretap Channel . . . 842
10.10.16 10.4.2 Proof of the Private Capacity Theorem . . . 844
10.10.17 10.4.3 Large Deviations for Random Operators . . . 849
10.10.18 10.4.4 The Direct Coding Theorem for the Quantum Capacity . . . 851
10.10.19 10.5 Notes and References . . . 856
10.11 11 Channels with Constrained Inputs . . . 857
10.11.1 11.1 Convergence of Density Operators . . . 858
10.11.2 11.2 Quantum Entropy and Relative Entropy . . . 860
10.11.3 11.3 Constrained c-q Channel . . . 862
10.11.4 11.4 Classical-Quantum Channel with Continuous Alphabet . . . 864
10.11.5 11.5 Constrained Quantum Channel . . . 866
10.11.6 11.6 Entanglement-Assisted Capacity of Constrained Channels . . . 868
10.11.7 11.7 Entanglement-Breaking Channels in Infinite Dimensions . . . 870
10.11.8 11.8 Notes and References . . . 873
10.12 12 Gaussian Systems . . . 874
10.12.1 12.1 Preliminary Material . . . 875
10.12.2 12.1.1 Spectral Decomposition and Stone's Theorem . . . 875
10.12.3 12.1.2 Operators Associated with the Heisenberg Commutation Relation . . . 877
10.12.4 12.1.3 Classical Signal Plus Quantum Noise . . . 879
10.12.5 12.1.4 The Classical-Quantum Gaussian Channel . . . 882
10.12.6 12.2 Canonical Commutation Relations . . . 883
10.12.7 12.2.1 Weyl-Segal Canonical Commutation Relation . . . 883
10.12.8 12.2.2 The Symplectic Space . . . 885
10.12.9 12.2.3 Dynamics, Quadratic Operators, and Gauge Transformations . . . 887
10.12.10 12.3 Gaussian States . . . 889
10.12.11 12.3.1 Characteristic Function . . . 889
10.12.12 12.3.2 Definition and Properties of Gaussian States . . . 890
10.12.13 12.3.3 The Density Operator of Gaussian State . . . 895
10.12.14 12.3.4 Entropy of a Gaussian State . . . 896
10.12.15 12.3.5 Separability and Purification . . . 898
10.12.16 12.4 Gaussian Channels . . . 901
10.12.17 12.4.1 Open Bosonic Systems . . . 901
10.12.18 12.4.2 Gaussian Channels: Basic Properties . . . 904
10.12.19 12.4.3 Gaussian Observables . . . 905
10.12.20 12.4.4 Gaussian Entanglement-Breaking Channels . . . 907
10.12.21 12.5 The Capacities of Gaussian Channels . . . 909
10.12.22 12.5.1 Maximization of the Mutual Information . . . 909
10.12.23 12.5.2 Gauge Covariant Channels I . . . 911
10.12.24 12.5.3 Maximization of the Coherent Information . . . 912
10.12.25 12.5.4 The Classical Capacity . . . 913
10.12.26 12.6 The Case of Single Mode . . . 927
10.12.27 12.6.1 Classification of Gaussian Channels . . . 927
10.12.28 12.6.2 Entanglement-Breaking Channels . . . 931
10.12.29 12.6.3 Attenuation/Amplification/Classical Noise Channel . . . 932
10.12.30 12.6.4 Estimating the Quantum Capacity . . . 935
10.12.31 12.7 Notes and References . . . 938
10.12.32 Bibliography . . . 941

11 Quantum supremacy using a programmable SC processor by Google AI Quantum 952
11.1 Device design and architecture . . . 952
11.2 Fabrication and layout . . . 953
11.3 Qubit control and readout . . . 954
11.3.1 Control . . . 954
11.3.2 Readout . . . 955
11.4 XEB theory . . . 959
11.4.1 XEB of a small number of qubits . . . 959
11.4.2 XEB of a large number of qubits . . . 963
11.4.3 Two limiting cases . . . 965
11.4.4 Measurement errors . . . 966
11.5 Quantifying errors . . . 967
11.6 Metrology and calibration . . . 969
11.6.1 Calibration overview . . . 969
11.6.2 Calibration procedure . . . 970
11.6.3 Two-qubit gate metrology . . . 976
11.6.4 Grid readout calibration . . . 985
11.6.5 Summary of system parameters . . . 987
11.7 Quantum circuits . . . 992
11.7.1 Background . . . 992
11.7.2 Overview and technical requirements . . . 992
11.7.3 Circuit structure . . . 992
11.7.4 Randomness . . . 993
11.7.5 Quantum gates . . . 993
11.7.6 Programmability and universality . . . 994
11.7.7 Circuit variants . . . 997
11.8 Large scale XEB results . . . 999
11.8.1 Limitations of full circuits . . . 1000
11.8.2 Patch circuits: a quick performance indicator for large systems . . . 1001
11.8.3 Elided circuits: a more rigorous performance estimator for large systems . . . 1002
11.8.4 Choice of unitary model for two-qubit entangling gates . . . 1003
11.8.5 Understanding system performance: error model prediction . . . 1005
11.8.6 Distribution of bitstring probabilities . . . 1007
11.8.7 Statistical uncertainties of XEB measurements . . . 1013
11.8.8 System stability and systematic uncertainties . . . 1015
11.8.9 The fidelity result and the null hypothesis on quantum supremacy . . . 1017
11.9 Sensitivity of XEB to errors . . . 1018
11.10 Classical simulations . . . 1021
11.10.1 Local Schrödinger and Schrödinger-Feynman simulators . . . 1021
11.10.2 Feynman simulator . . . 1022
11.10.3 Supercomputer Schrödinger simulator . . . 1029
11.10.4 Simulation of random circuit sampling with a target fidelity . . . 1030
11.10.5 Treewidth upper bounds and variable elimination algorithms . . . 1036
11.10.6 Computational cost estimation for the sampling task . . . 1039
11.10.7 Understanding the scaling with width and depth of the computational cost of verification . . . 1041
11.10.8 Energy advantage for quantum computing . . . 1044
11.11 Complexity-theoretic foundation of the experiment . . . 1045
11.11.1 Error model . . . 1047
11.11.2 Definition of computational problem . . . 1047
11.11.3 Computational hardness of unbiased-noise sampling . . . 1048
11.11.4 Proof of Theorem 1 . . . 1049

12 Quantum Probability and Quantum Statistics by Holevo **1051**
12.0.1 Introduction . . . 1051
12.1 Standard Statistical Model of Quantum Mechanics . . . 1060
12.1.1 1. Basic Concepts . . . 1060
12.1.2 2. Symmetries, Kinematics, Dynamics . . . 1067
12.1.3 3. Composite Systems . . . 1072
12.1.4 4. The Problem of Hidden Parameters . . . 1075
12.2 Statistics of Quantum Measurements . . . 1080
12.2.1 1. Generalized Observables . . . 1080
12.2.2 2. The Quantum Theory of Statistical Solutions . . . 1084
12.2.3 3. Covariant Observables . . . 1093
12.3 Evolution of an Open System . . . 1100
12.3.1 1. Transformations of Quantum States and Observables . . . 1100
12.3.2 2. Quantum Dynamical Semigroups . . . 1104
12.4 Consistent and Continuous Measurement Processes . . . 1113
12.4.1 1. Statistics of Successive Measurements . . . 1113
12.4.2 2. Continuous Measurement Processes . . . 1120
12.5 Processes in the Fock Space . . . 1129
12.5.1 1. Quantum Stochastic Calculus . . . 1129
12.5.2 2. Расширения в пространстве Фока . . . 1137

IV Problems **1148**

13 General Questions **1148**
13.1 Questions to Check Basic General Knowledge . . . 1148
13.2 Questions to Check Basic Technical Knowledge . . . 1148
13.2.1 Problems about States, Entanglement . . . 1148

14 Typical Problems **1150**
14.1 Problems about Basic Models (!!) . . . 1150
14.1.1 Problems about Qubits . . . 1150
14.1.2 Problems about Qutrits, Exotic Qubits . . . 1150

15 Other Problems (????) **1150**
15.0.1 Other Problems (????) . . . 1150
15.0.2 Problems about Special Quantum Channels (?????) . . . 1152

V Other Basic Topics **1153**

16 Topological phases and quantum computation Kitaev, Laumann **1153**
16.1 Introduction: The quest for protected qubits . . . 1153
16.2 Topological phenomena in 1D: boundary modes in the Majorana chain . . . 1154
16.2.1 Nature of topological degeneracy (spin language) . . . 1155
16.2.2 Reduction of TFIM to SPSC by the Jordan-Wigner transformation . . . 1155
16.2.3 Majorana operators . . . 1156
16.2.4 General properties of quadratic fermionic Hamiltonians . . . 1157
16.2.5 Why are the boundary modes robust? . . . 1158
16.3 The two-dimensional toric code . . . 1159
16.3.1 Ground states . . . 1160
16.3.2 Excitations . . . 1160
16.4 Abelian anyons and quasiparticle statistics . . . 1161
16.4.1 Superselection sectors and fusion rules . . . 1164
16.4.2 Mutual statistics implies degeneracy on the torus . . . 1165

16.4.3 The toric code in a field: perturbation analysis . . . 1166
16.4.4 Robustness of the topological degeneracy . . . 1167
16.4.5 Emergent symmetry: gauge formulation . . . 1167
16.5 The honeycomb lattice model . . . 1168
16.5.1 A (redundant) representation of a spin by 4 Majorana operators . . . 1169
16.5.2 Solving the Honeycomb Model using Majoranas . . . 1169
16.5.3 Fermionic spectrum in the honeycomb lattice model . . . 1171
16.5.4 Quasiparticle statistics in the gapped phase . . . 1172
16.5.5 Nonabelian phase . . . 1174
16.5.6 Robustness of chiral modes . . . 1176

17 Entanglement in quantum critical phenomena by Vidal, Latorre, Rico, Kitaev 1178

18 What limits the simulation of quantum computers? by Zhou, Stoudenmire, Waintal 1185
18.1 Introduction . . . 1186
18.2 Possible strategies for approximate simulations of quantum circuits . . . 1187
18.3 Noisy algorithm in one dimension . . . 1188
18.3.1 MPS representation of the state . . . 1188
18.3.2 Random Quantum Circuit . . . 1190
18.3.3 Effective two-qubit gate fidelity . . . 1190
18.4 Links between two-qubit and multi-qubit fidelity . . . 1191
18.4.1 Multi-qubit fidelity . . . 1191
18.4.2 Other fidelity metrics . . . 1193
18.5 Random Tensor Theory of ϵ_∞ . . . 1194
18.6 Algorithms for getting beyond ϵ_∞ . . . 1195
18.6.1 Grouped MPS State and Extraction Algorithm . . . 1196
18.6.2 Application to a two dimensional circuit . . . 1196
18.6.3 Split-and-Merge algorithm for more complex gates . . . 1197
18.7 Discussion . . . 1198

19 How the Result of a Measurement of a Component of the Spin of a Spin-$\frac{1}{2}$ Particle Can Turn Out to be 100 by Aharonov, Albert, and Vaidman (1987) 1209

20 The Physical Implementation of Quantum Computation by DiVincenzo 1214
20.1 Introduction . . . 1214
20.2 Why *quantum* information processing? . . . 1214
20.3 Realizing quantum computation . . . 1215
20.4 Desiderata for quantum communication . . . 1222
20.5 Summary . . . 1223

21 Decoherence, Einselection, and the Quantum Origins of the Classical by Zurek 1224
21.1 Introduction . . . 1224
21.1.1 The problem: Hilbert space is big . . . 1225
21.1.2 Decoherence and einselection . . . 1226
21.1.3 The nature of the resolution and the role of envariance . . . 1227
21.1.4 Existential Interpretation and 'Quantum Darwinism' . . . 1228
21.2 Quantum Measurements . . . 1229
21.2.1 Quantum conditional dynamics . . . 1230
21.2.2 Information transfer in measurements . . . 1235
21.2.3 "Collapse" analogue in a classical measurement . . . 1236
21.3 Chaos and Loss of Coherence . . . 1238
21.3.1 Loss of the quantum-classical correspondence . . . 1238
21.3.2 Moyal bracket and Liouville flow . . . 1241
21.3.3 Symptoms of correspondence loss . . . 1241

21.4 Environment-Induced Superselection . . . 1243
21.4.1 Models of einselection . . . 1244
21.4.2 Einselection as the selective loss of information . . . 1248
21.4.3 Decoherence, entanglement, dephasing, and noise . . . 1251
21.4.4 Predictability sieve and einselection . . . 1253
21.5 Einselection in phase space . . . 1254
21.5.1 Quantum Brownian motion . . . 1255
21.5.2 Decoherence in quantum Brownian motion . . . 1259
21.5.3 Predictability sieve in phase space . . . 1263
21.5.4 Classical limit in phase space . . . 1264
21.5.5 Decoherence, chaos, and the Second Law . . . 1266
21.6 Einselection and Measurements . . . 1270
21.6.1 Objective existence of einselected states . . . 1270
21.6.2 Measurements and memories . . . 1272
21.6.3 Axioms of quantum measurement theory . . . 1272
21.6.4 Probabilities from Envariance . . . 1276
21.7 Environment as a Witness . . . 1284
21.7.1 Quantum Darwinism . . . 1285
21.7.2 Observers and the Existential Interpretation . . . 1290
21.7.3 Events, Records, and Histories . . . 1291
21.8 Decoherence in the Laboratory . . . 1294
21.8.1 Decoherence due to entangling interactions . . . 1294
21.8.2 Simulating decoherence with classical noise . . . 1296
21.8.3 Analogue of decoherence in a classical system . . . 1297
21.8.4 Taming decoherence . . . 1298
21.9 Concluding Remarks . . . 1301

VI Experiments for Quantum Information Theory 1305

22 Experimental Realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A New Violation of Bell's Inequalities by Aspect, Grangier, et al. (1981) 1305

VII Quantum Computing 1310

VIII Creation of a Quantum Computer 1311

IX Quantum Error Correction 1312

X Some Philosophical and Exotic Theories of Quantum Information 1313

23 Quantum Theory and Measurement Edited by John Archibald Wheeler and Wojciech Hubert Zurek 1313
23.0.1 Preface . . . 1313

24 I. Questions of Principle 1321
24.1 1.1 The Bohr-einstein Dialogue . . . 1321
24.2 I. 1 Discussion with Einstein on Epistemological Problems in Atomic Physics . . . 1325
24.3 I. 2 Born's Probabilistic Interpretation . . . 1348
24.4 1.2 On the Quantum Mechanics of Collisions by Max Born . . . 1349

24.5 I. 3 the Principle of Indeterminacy . . . 1352
24.6 I. 3 the Physical Content of Quantum Kinematics and Mechanics . . . 1355
24.7 I. 4 Complementarity . . . 1372
24.8 I. 4 the Quantum Postulate and the Recent Development of Atomic Theory . . . 1373
24.9 I. 5 the Uncertainty Principle . . . 1389
24.10 I. 6 the Wave Mechanics of α-ray Tracks . . . 1390
24.11 I. 7 Knowledge of Past and Future in Quantum Mechanics . . . 1395
24.12 I. 8 the Einstein-podolsky-rosen Paper . . . 1397
24.13 I. 9 Bohr's Reply . . . 1401
24.14 1. 9 Quantum Mechanics and Physical Reality . . . 1403
24.15 I. 10 Can Quantum-mechanical Description of Physical Reality Be Considered Complete? 1403
24.16 I. 11 Present Situation in Quantum Mechanics: a Translation of Schrdinger's "cat Paradox" Paper . . . 1410
24.16.1 Introduction . . . 1410
24.16.2 1. The L'hysics of Models . . . 1411
24.16.3 3. Examples of Probability Predictions . . . 1414
24.16.4 4. (an One Basc the Theory on Ideal Enswhles.' . . . 1416
24.16.5 5. Are the L'aridbles Really Blarra!' . . . 1417
24.16.6 6. The Didherativ-unall-face of the Epistemanaical Vicupount . . . 1418
24.16.7 7. The ψ-function As Expectation-catalog . . . 1419
24.16.8 8. Theory of Measurement, Part One . . . 1419
24.16.9 9. The ψ-function As Description of State . . . 1421
24.16.10 10. Theory of Measurement. Fart Two . . . 1422
24.16.11 11. Resolution of the "entanglement." Result Depondent on the Experimenter's Intention . . . 1425
24.16.12 12. An Example . . . 1426
24.16.13 13. Continuation of the Example: All Possible Mcasurcments Are Entangled Uncquiwocally . . . 1427
24.16.14 14. Imerdependente of the Emanylancht. Consideration of the Streial Role of Tame . . . 1429
24.16.15 15. Natural Laze or Calculating Disite? . . . 1431
24.17 I. 12 Remarks on the Mind-body Question by Wigner . . . 1433
24.17.1 Introductory Comments . . . 1433
24.17.2 The Language of Quantum Mechanics . . . 1434
24.17.3 An Example . . . 1435
24.17.4 The Reasons for Materialism . . . 1436
24.17.5 Simplest Answer to the Mind-body Question . . . 1437
24.17.6 More Difficult Questions . . . 1439
24.17.7 Non-linearity of Equations As Indication of Life . . . 1440
24.18 I. 13 Law without Law by Wheeler . . . 1441

25 II Interpretations of the Act of Measurement 1463
25.1 II. 1 the Theory of Observation in Quantum Mechanics by London, Bauer . . . 1463
25.1.1 Introduction . . . 1463
25.1.2 §1. Resum of the Principles of Quantum Physics . . . 1465
25.1.3 §2. Vector Notation . . . 1471
25.1.4 §3. Statistics and Objectivity . . . 1474
25.1.5 §4. Mixtures and Pure States . . . 1475
25.1.6 §5. the Statistical Operator . . . 1477
25.1.7 §6. Some Mathematical Properties of Statistical Matrices . . . 1479
25.1.8 §7. the Statistical Operator and Thermodynamics . . . 1481
25.1.9 §8. the Irreducibility of the Pure Case . . . 1482
25.1.10 §9. Statistics of a System Composed of Two Subsystems . . . 1484
25.1.11 §10. Reversible and Irreversible Evolution . . . 1487

25.1.12 §11. Measurement and Observation. the Act of Objectification . . . 1488
25.1.13 §12. an Example of Measurement . . . 1490
25.1.14 §13. Individuality and Pure Case . . . 1493
25.1.15 §14. Scientific Community and Obiectivity . . . 1494
25.2 II. 2 Interpretation of Quantum Mechanics by Wigner . . . 1496
25.2.1 §1. Problems Raised by Quantum Theory Before the Advent of Quantum Mechanics . . . 1496
25.2.2 §2. the Mathematical Formalism of Quantum Mechanics . . . 1502
25.2.3 §3. Direct Product and Quantum Mechanical Description of the Measuring Process 1509
25.2.4 §4. the Physics of the Measurement Description (35) . . . 1514
25.2.5 §5. Other Proposed Resolutions of the Measurement Paradox . . . 1518
25.2.6 §6. Experimental Tests of Bell's Inequality . . . 1523
25.2.7 §7. Probifms of the Standard Interpretation: Unmeasurable Quantities . . . 1524
25.2.8 Summary . . . 1536
25.3 II. 3 "relative State" Formulation of Quantum Mechanics by Everett (1957) . . . 1537
25.3.1 1. Introduction . . . 1537
25.3.2 2. Realm of Applicability of the Conventional or "external Observation" Formulation of Qm . . . 1538
25.3.3 3. Quantum Mechanics Internal to an Isolated System . . . 1539
25.3.4 4. Concept of Relative State . . . 1540
25.3.5 5. Observation . . . 1542
25.3.6 6. Discussion . . . 1551
25.4 II. 4 the Problem of Measurement by Wgnek . . . 1551
25.4.1 Introduction . . . 1551
25.4.2 The Orthodox View . . . 1553
25.4.3 Consistency Of the Orthodox View . . . 1553
25.4.4 Critiques Of the Orthodox Theory . . . 1555
25.4.5 What Is the State Vector? . . . 1559
25.4.6 Problems Of the Orthodox View . . . 1560
25.5 II. 5 on the Interpretation of Measurement in Quantum Theory by Zen (1969) . . . 1562

26 III "Hidden Variables" versus "Phenomenon" and Complementarity 1569
26.1 III.1 Polyelectrons . . . 1569
26.1.1 Summary . . . 1569
26.1.2 Possibility Of Testing Some of the Present Predictions of Pair Theory . . . 1569
26.2 III.2 Paradox of Einstein, Rose, and Podolsky by Bohm . . . 1571
26.3 III.3 Suggested Interpretation in Terms of "Hidden" Variables", I . . . 1579
26.3.1 1. Introduction . . . 1580
26.3.2 2. The Usual Physical Interpretation of the Quantum Theory . . . 1581
26.3.3 3. Criticism of the Usual Interpretation of the Quantum Theory . . . 1583
26.3.4 4. New Physical Interpretation of Schroedinger's Equation . . . 1585
26.3.5 5. The Stationary State . . . 1589
26.3.6 6. The Many-body Problem . . . 1592
26.3.7 7. Transitions between Stationary States. the Franck-hertz Experiment . . . 1593
26.3.8 8. Penetration of a Barrier . . . 1598
26.3.9 9. Possible Modifications in Mathematical Formiuzation Leading to Experivien-tal Proof That New Interpretation . . . 1599
26.4 III.3 Suggested Interpretation in Terms of "Hidden" Variables", II . . . 1600
26.4.1 10. Summary and Conclusions . . . 1601
26.4.2 1. Introduction . . . 1602
26.4.3 Theory . . . 1603
26.4.4 Appendices . . . 1614
26.5 III.4 On the Problem of Hidden Variables in Quantum Mechanics* . . . 1621
26.5.1 I. Introduction . . . 1621

26.5.2 II. Assumptios, and a Simple Example . . . 1622
26.5.3 III. Von Neumann . . . 1624
26.5.4 iV. Jauch and Piron . . . 1625
26.5.5 V. Gleason . . . 1626
26.5.6 VI. Locality and Separability . . . 1629
26.5.7 Acknowledgments . . . 1630
26.6 III.5 On the Einstein Podolsky Rosen Paradox* . . . 1631
26.6.1 1. Introduction . . . 1631
26.6.2 II. Formulation . . . 1631
26.6.3 iii. Illustration . . . 1632
26.6.4 IV. Contradiction . . . 1633
26.6.5 V. Generalization . . . 1635
26.6.6 VI. Conclusion . . . 1635
26.7 III.6 Proposed Experiment to Test Local Hidden-variable Theories by Clauser, Horne, Shimony, Holt . . . 1636
26.8 III.7 Experimental Test of Local Hidden-variable Theories by Freedman, Ciauser . . . 1641
26.9 III.8 Experimental Test of Local Hidden-variable Theories* . . . 1646
26.10 III.9 Quantum Mechanics and Hidden Variables: a Test of Bell's Inequality by the Measurement of the Spin Correlation in Low-energy Proton-proton Scattering . . . 1652
26.10.1 I. Introduction . . . 1652
26.10.2 II. Bell's Inequality . . . 1653
26.10.3 III. Description of a "perfect" Experimental Setup and Discussion of Realized Experiments . . . 1654
26.10.4 IV. Measurement of the Spin Correiation in Low-energy Proton-proton Scattering 1657
26.10.5 A. The Experimental Setup . . . 1657
26.10.6 B. Design of the Experimental Device . . . 1661
26.10.7 D. Measurement of the Analyzing Power . . . 1662
26.10.8 E. Electronics Associated with Coincidence Measurements . . . 1663
26.10.9 F. The Geometric Correlation . . . 1666
26.10.10 G. Final Results . . . 1669
26.10.11 V. Conclusion . . . 1669
26.11 III.10 Proposed Experiment to Test the Nonseparability of Quantum Mechanics by Aspect 1670
26.11.1 I. Test of the Principle of Separability . . . 1671
26.11.2 II. Proposed Experimental Scheme and Corresponding Generalized Bell Inequalities 1673
26.11.3 III. Testable Inequalities . . . 1676
26.11.4 IV. Overall Experimental Setup . . . 1677
26.11.5 V. Brief Conclusion and Acknowledgments . . . 1679
26.11.6 Appendix . . . 1679
26.12 III.11 Complementarity in the Double-slit Experiment: Quantum Nonseparability and a Quantitative Statement of Bohr's Principle . . . 1683
26.12.1 I. Introduction . . . 1683
26.12.2 II. Approximate Path-determination . . . 1685
26.12.3 III. Correlation between the Measured Momentum and the Corresponding Interference Pattern . . . 1688
26.12.4 IV. Einstein-rosen-podolsky "paradox" in the Double-slit Experiment . . . 1690
26.12.5 V. Information and the Complementarity Principle . . . 1692
26.12.6 Acknowledgments . . . 1696
26.12.7 Appendix A: Multiplate Double-slit Experiment . . . 1696
26.12.8 Appendix B: Outline of a Proof That the Pure State Minimizes the Loss of Information . . . 1699
26.13 III.12 Complementarity in the Double-slit Experiment: on Simple Realizable Systems for Observing Intermediate Particle-wave Behavior . . . 1701
26.14 III.13 A "delayed-choice" Quantum Mechanics Experiment by Wickes, Alley, Jakubowicz 1703

27 IV. Field Measurements **1707**
27.1 IV.1 Extension of the Uncertainty Principle to Relativistic Quantum Theory by Landau, Peierls . . . 1707
27.1.1 1. Introduction . . . 1707
27.1.2 2. The Concept of Measurement in Wave Mechanics . . . 1707
27.1.3 3. Momentum Measurement in the Relativistic Case . . . 1709
27.1.4 4. Field Measurement . . . 1711
27.1.5 5. Measurements on Light Quanta . . . 1712
27.1.6 6. Measurements on Material Particles . . . 1713
27.1.7 7. Mathematical Failure of the Methods of Wave Mechanics . . . 1714
27.1.8 8. Conclusions . . . 1714
27.2 IV.2 The Measurability of the Electromagnetic Field . . . 1716
27.3 IV. 2 on the Question of the Measurability of Electromagnetic Field Quantities by Bohr, Rosenfeld . . . 1717
27.3.1 1. Introduction . . . 1717
27.3.2 2. Measurability of Fields According to Quantum Theory . . . 1719
27.3.3 3. Presuppositions for Physical Field Measurements . . . 1724
27.3.4 4. Calculation of the Field Effects of the Test Body . . . 1731
27.3.5 5. Measurement of Single Field Averages . . . 1733
27.3.6 Б. Measurability of Two-fold Averages of a Field Component . . . 1736
27.3.7 7. Measurability of Two Averages of Different Field Components . . . 1740
27.3.8 8. Concluding Remarks . . . 1742
27.3.9 Literature . . . 1742
27.4 IV.3 Field and Charge Measurements in Quantum Electrodynamics by Bohr, Rosenfeld 1743
27.4.1 Introduction . . . 1743
27.4.2 1. Measurements of Electromagnetic Fields . . . 1744
27.4.3 3. Charge-current Measurements in Pair Theory . . . 1748
27.4.4 4. Concluding Remarks . . . 1749

28 V Irreversibility and Quantum Theory **1750**
28.1 V.1 On the Decrease of Entropy in a Thermodynamic System by the Intervention of Intelligent Beings by Szilard . . . 1750
28.2 V.2 Measurement and Reversibility by Von Neumann . . . 1764
28.2.1 1. Measurement and Reversibility . . . 1764
28.2.2 2. Thermodynamical Considerations . . . 1770
28.2.3 3. Reversibility and Equilibrium Problems . . . 1780
28.2.4 4. The Macroscopic Measurement . . . 1791
28.3 V.2 The Measuring Process by Von Neumann . . . 1800
28.3.1 1. Formulation of the Problem . . . 1800
28.3.2 2. Composite Systems . . . 1802
28.3.3 3. Discussion of the Measuring Process . . . 1810
28.4 V.3 The Ergodic Behavior of Qntumm Many-body Systems by Van Hove . . . 1814
28.5 V.4 Quantum Theory of Measurement and Ergodicity Conditions . . . 1821
28.5.1 1. Introduction . . . 1821
28.5.2 2. Macro-states of the Measuring Apparatus . . . 1822
28.5.3 3. Basic Assumptions of Quantum Theory . . . 1823
28.5.4 4. Consequences of the Preceding Assumptions . . . 1824
28.5.5 5. Von Neumann's Theory of the Measuring Process . . . 1825
28.5.6 6. Criticism of Von Neumann's Point of View . . . 1826
28.5.7 7. Hints for an Objectivistic Interpretation of the Measuring Process . . . 1828
28.5.8 8. Analysis of the Physical Characteristics of Some Typical Measuring Apparatus 1829
28.5.9 9. Outline of a Theory of the Macroscopic Bodies . . . 1831
28.5.10 10. Schematization of the Measuring Apparatus and Mathematical Theory of the Measuring Process . . . 1833

28.5.11 11. Limitations on the Kind of Quantities Actually Observable; Measurements on Macroscopic Bodies . . . 1835
28.5.12 12. Theory of the Measuring Process under "weak" Ergodicity Conditions . . . 1837
28.6 V.5 Time Symmetry in the Quantum Process of Measurement* . . . 1841
28.6.1 I. Introduction . . . 1842
28.6.2 II. Sequences of Observations . . . 1843
28.6.3 III. Asymptotic Procedures . . . 1846
28.6.4 IV. Direct Prediction . . . 1849
28.7 V.6 Lyapounov Variable: Entropy and Measurement in Quantum Mechanics . . . 1851
28.7.1 1. Introduction . . . 1851
28.7.2 2. Incompatibility between the Existence of Entropy Operator and the Semi-boundness of Generator of Time-evolution . . . 1854
28.7.3 3. The Entropy Superoperator . . . 1856
28.7.4 4. Nonfactorizability of Entropy Superoperators . . . 1858
28.7.5 5. Concluding Remarks . . . 1860
28.8 Teleporting An Unknown Quantum State Via Dual Classical and Einstein-podolsky-rosen Channels by Bennett, Brassard, Crépeau, Jozsa, Peres, Wootters . . . 1861
28.9 V. 7 Can We Undo Quantum Measurements? by Peres . . . 1866
28.9.1 Theory . . . 1867
28.9.2 Appendix: a More Realistic Model . . . 1870

29 VI Accuracy of Measurements: Quantum Limitations 1873
29.1 VI.1 The Unmeasurability of the Spin of a Free Electron . . . 1873
29.2 VI.1 Magnetic Moment of the Electron by Miott, Massey . . . 1874
29.3 VI.2 Measurement of Quantum Mechanical Operators by Araki, Yanase . . . 1878
29.3.1 1. Introduction . . . 1879
29.3.2 2. Impossibility of an Exact Measurement of an Operator Which Does Not Commute with a Conserved Quantity with a Conserved Quantity . . . 1879
29.3.3 3. Possibility of an Approximate Measurement . . . 1882
29.4 VI.3 Optimal Measuring Apparatus by Yanse . . . 1888
29.4.1 1. Introduction . . . 1888
29.4.2 2. Minimization of the Malfunctioning Probability . . . 1889
29.4.3 3. Conclusions and Discussions . . . 1892
29.5 VI.4 Time in the Quantum Theory and the Uncertainty Relation for Time and Energy by Aharonov, Bohm . . . 1892
29.5.1 1. Historical Summary of the State of the Problem of Time Measremenent Inv the Quantum Theory . . . 1893
29.5.2 2. Criticism of Commonly Accepted Interpretations of the Time-energy Uncertainty Relation . . . 1897
29.5.3 3. Treatment of Time of Measurement in Terms of the Mathematical Formalism of the Quantum Theory . . . 1899
29.5.4 4. Example of a Reproducible Measurement of Energy in a Well-defined Time . 1904
29.5.5 5. Summary and Conclusions . . . 1907
29.6 VI.5 The Fundamental Noise Limit of Linear Amplifiers by Heffner . . . 1908
29.6.1 Summary . . . 1908
29.6.2 Introduction . . . 1908
29.6.3 The Uncertainty Principle . . . 1909
29.6.4 Minimum Noise Temperature of a Linear Amplifier . . . 1912
29.6.5 The Implications of the Minimum Noise Limit . . . 1915
29.7 VI.6 Quantum Noise in Linear Amplifiers by Haus, Mullen . . . 1915
29.7.1 Introduction . . . 1916
29.7.2 I. Noise Figure . . . 1916
29.7.3 II. The Equations of Linear Amplifiers . . . 1919
29.7.4 III. Amplifier Noise . . . 1922

29.7.5 IV. Simultaneous Phase and Amplitude Measurements . . . 1925
29.7.6 APPENDIX. Radiative Attenuation Noise . . . 1926
29.8 VI.7 Optical Channels: Practical Limits with Photon Counting . . . 1927
29.9 VI. 8 Quantum Nondemolition Measurements by Braginsky, Vuruntsuv, Thorne . . . 1932
29.9.1 Resonant-bar Gravitational-wave . . . 1935
29.9.2 General Theory of Quantum . . . 1936
29.9.3 Position Measurements . . . 1940
29.9.4 Energy Mieasurements . . . 1943
29.9.5 Back-action-evading Measurements of $\hat{x}_1$ . . . 1945
29.9.6 Thermal Noise in the Oscillator and Amplifier . . . 1947
29.9.7 Prospects For Stroboscopic Measurements . . . 1948
29.9.8 Prospects For Single-transducer Back-action-evading Measurements . . . 1949
29.10Guide To Some Further Literature . . . 1952
29.10.1 I. Questions of Principle . . . 1952
29.10.2 II. Interpretations of the Act of Measurement . . . 1954
29.10.3 IV. Field Measurements . . . 1960
29.10.4 VI. Irreversibility and Quantum Theory . . . 1961
29.10.5 Vi.accuracy of Measurements: Quantum Limitations . . . 1963

XI Appendix 1966

A Introduction 1966
A.1 Literature . . . 1966
A.1.1 Main Literature . . . 1966
A.1.2 Extra Literature . . . 1967
A.2 Puzzles for Different Cases . . . 1967
A.2.1 Puzzles in Everyday life . . . 1967
A.2.2 General Fundamental Topics to Discuss . . . 1968

B Mathematics, Physics, Programming 1968
B.0.1 Linear Algebra . . . 1968
B.0.2 NCh.1: Notes on basic probability theory . . . 1969
B.0.3 NCh.2: Group theory . . . 1970
B.0.4 NCh.3: The Solovay-Kitaev theorem . . . 1975
B.0.5 NCh.4: Number theory . . . 1982
B.0.6 NCh.5: Public key cryptography and the RSA cryptosystem . . . 1994
B.0.7 NCh.6: Proof of Lieb's theorem . . . 1998
B.1 Programming . . . 2002

C Bibliography 2003

Preface and main motivation

Let's discuss some minimum knowledge and motivation that would be good to understand for studying the subject.

Квантовая теория информации очень четко говорит об одном из самого важного в квантовой и фундаментального в механике: о состояниях, измерениях, их преобразованиях

(напишу тут подробно, что это на самом деле крутейший предмет. Спустя 1.5 года как на физтехе прошел понял, что это очень очень стоит того, чтобы очень много в нем просиживать, и все-таки пройти вдоль и поперек его!)

Квантовая теория информации в 2023 году многое может дать для устройства на работу, для приложений квантовой механики

(раскрою, что это один из самых прикладных предметов, один из самых востребованных. Чисто можно начать зарабатывать только за счет того, что 1 этот предмет и поймешь! Так что он один из самых важных, по крайней мере в 2023 году. Проверю потом еще эти утверждения, но пока очень в это верю.)

Одни из лучших идейных головоломок

Одни из лучших технических головоломок

Part I
Typical Quantum Inform Theory in a Nutshell

1 Basic Methods and Concepts

1.1 Basic Methods of Quantum Information

1.1.1 Definitions and Meaning of States, Entanglement, and Measurements

Типичные состояния

Состояния Белла для двух кубитов:

$$|\psi_+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
$$|\psi_-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$
$$|\varphi_+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$
$$|\varphi_-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Это О.Н.Б. из перепутанных состояний

Чистые / факторизованные

Чистые могут быть перепутанными или не перепутанными.
Чистые не перепутанные:

$$\psi_{AB} = \psi_A \otimes \psi_B$$

$$\rho_{AB} = |\psi\rangle\langle\psi| = |\varphi\rangle\langle\varphi| \otimes |\xi\rangle\langle\xi|$$

$$\rho_{AB} = \rho_A \otimes \rho_B$$

Чистые перепутанные:

$$\psi_{AB} \neq \psi_A \otimes \psi_B$$

$$\psi_{AB} = |\psi\rangle\langle\psi| \neq |\varphi\rangle\langle\varphi| \otimes |\xi\rangle\langle\xi|$$

здесь нет вообще корреляций.
(???!!! примеры??!!!)

Смешанные состояния

Смешанные не перепутанные:

$$\rho_{AB} \neq |\psi\rangle \langle\psi|$$

$$\rho^{AB} = \sum_k p_k \rho_k^A \otimes \rho_k^B,$$

где p_k - коэффициенты в выпуклой сумме.

(???!!! примеры??!!!)

сепарабельные / распутанные / не запутанные / состояния

Физический смысл незапутанных состояний в том, что если у нас есть физическая величина, состоящая из тензорного произведения величины одной части системы F и величины второй части системы G есть произведение их средних значений

$$\langle F \otimes G\rangle = \langle F\rangle \cdot \langle G\rangle.$$

Кстати, если было бы перепутанное, то $\langle F \otimes G\rangle \neq \langle F\rangle \cdot \langle G\rangle$, то ест были бы корреляции.

Другими словами, можно брать произведение результатов.

(там что я измеряю X, коллега измеряет У, мы перемножаем их и считаем матожидание)

Проверка сепарабельности делается следующими способами.

Критерий Переса-Городецких:

$$\rho_{AB}^{T_B} \geq 0 \quad \Longrightarrow \quad \text{сепарабельно}$$

$$\rho_{AB}^{T_B} \geq 0 \quad \underbrace{\Longleftarrow}_{dimH_A \cdot dimH_B \leq 6} \quad \text{сепарабельно}$$

В частности для двух кубитов, критерий Переса-Городецких утверждает, что их матрица плотности является сепарабельной тогда и только тогда, когда она остается матрицей плотности при частичном транспонировании.

(ниже где-то он доказан)

Коррелированные (классическим и квантовым образом) состояния

Коррелированные состояния - это состояния, у которых $\rho_{AB} \neq \rho_A \otimes \rho_B$.

(?? только так определяются, никак иначе?)

Есть классическая корреляция, когда можно представить в виде выпуклой суммы

$$\rho_{AB} = \sum_k p_k \rho_A^k \otimes \rho_B^k$$

Есть квантовая корреляция, когда

$$\rho_{AB} \neq \sum_k p_k \rho_A^k \otimes \rho_B^k$$

это же запутанность.

Свойства:

множество всех сепарабельных состояний для данной системы выпукло.

Критерий Переса-Городецких

Критерий Переса-Городецких:

$$\rho_{AB}^{T_B} \geq 0 \quad \Longrightarrow \quad \text{сепарабельно}$$

$$\rho_{AB}^{T_B} \geq 0 \quad \underbrace{\Longleftarrow}_{\dim H_A \cdot \dim H_B \leq 6} \quad \text{сепарабельно}$$

(тут указание на доказательство)

Запутанные состояния

Запутанность, это когда

$$\rho_{AB} \neq \sum_k p_k \rho_A^k \otimes \rho_B^k$$

Критерии:
ранг Шмидта больше 2.
(по определению его, см. разложение Шмидта.)
(?? примеры !!!)
Свойства:
множество всех квантово перепутанных состояний для данной системы не выпукло.
(?? энтропия перепутанности???)
Также есть:
максимально перепутанное состояние:
(напишу потом)
(???? как получить запутанное состояние? типичный вопрос)

Квантовый инструмент

POVM - мера, соответствующая измерению

POVM - это мера E, которая сопоставляется каждому исходу,
удовлетворяющая $E = E^+ \geq 0$, и вероятность каждого исхода вычисляется по

$$p(i) = \mathrm{tr}(\rho E_i)$$

Теорема Озавы утверждает, что для любого инструмента $\mathscr{M}$ и любого состояния S существует семейство апостериорных состояний $\{S_x; x \in \mathscr{Q}\}$, т. е. операторов плотности S_x, таких что:

1. функция $x \to \mathrm{Tr}\, S_x Y \mu_s$-измерима для любого $Y \in \mathscr{F}(\mathscr{C})$;
2. $\mathrm{Tr}\, \mathscr{M}(B)[S]Y = \int\limits_B (\mathrm{Tr}\, S_x Y)\, \mu_s(dx)$.

Теорема Озавы имеет принципиальное значение, поскольку демонстрирует согласованность понятия (вполне положительного) инструмента со стандартным формализмом квантовой механики.

Взаимно несмещенный базис (??!!)

Квантовый канал

Квантовый канал - это линейное, вполне положительное отображение, сохраняющее след.

(тут пояснение про вполне положительность, что за определение)

1.1.2 Typical Quantum Gates

(??? for all basic problems about them)

1.1.3 Transformations of States, the Simplest Quantum Gates

(по идее тут и хватит для простых вентелей)

О разложении Шмидта

Разложение Шмидта

$$\left|\psi^{AB}\right\rangle \in \mathcal{H}^A \otimes \mathcal{H}^B \quad \dim \mathcal{H}^A = d \leqslant D = \dim \mathcal{H}^B$$

$$\left|\psi^{AB}\right\rangle = \sum_{i=1}^{d}\sum_{j=1}^{D} c_{ij}|i\rangle \otimes |j\rangle$$

$$c_{ij} = \sum_{k=1}^{d} U_{ik}\lambda_k V_{kj}$$

Разложение Шмидта

$$\left|\psi^{AB}\right\rangle \in \mathcal{H}^A \otimes \mathcal{H}^B \quad \dim \mathcal{H}^A = d \leqslant D = \dim \mathcal{H}^B$$

$$\left|\psi^{AB}\right\rangle = \sum_{i=1}^{d}\sum_{j=1}^{D}\sum_{k=1}^{d} U_{ik}\lambda_k V_{kj}|i\rangle \otimes |j\rangle$$

$$\left|\psi^{AB}\right\rangle = \sum_{k=1}^{d} \lambda_k \left(\sum_{i=1}^{d} U_{ik}|i\rangle\right) \otimes \left(\sum_{j=1}^{D} V_{kj}|j\rangle\right)$$

$$\left|\psi^{AB}\right\rangle = \sum_{k=1}^{d} \lambda_k \left|f_k\right\rangle \otimes \left|g_k^*\right\rangle, \qquad \langle f_k|f_l\rangle = \langle g_k|g_l\rangle = \delta_{kl}$$

Пример: Запишите разложение Шмидта для состояния

$$\frac{1}{2}(|H\rangle \otimes |H\rangle + |H\rangle \otimes |V\rangle + |V\rangle \otimes |H\rangle - |V\rangle \otimes |V\rangle)$$

$$\frac{1}{2}(|H\rangle \otimes |H\rangle + |H\rangle \otimes |V\rangle + |V\rangle \otimes |H\rangle - |V\rangle \otimes |V\rangle) =$$

$$= \frac{1}{2}|H\rangle \otimes (|H\rangle + |V\rangle) + \frac{1}{2}|V\rangle \otimes (|H\rangle - |V\rangle) =$$

$$= \frac{1}{\sqrt{2}}\left[|H\rangle \otimes \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle) + |V\rangle \otimes \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)\right]$$

$$= \frac{1}{\sqrt{2}}\left[\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}\right]$$

Разложение Шмидта

$$\left|\psi^{AB}\right\rangle \in \mathcal{H}^A \otimes \mathcal{H}^B \quad \dim \mathcal{H}^A = d \leqslant D = \dim \mathcal{H}^B$$

$$\left|\psi^{AB}\right\rangle = \sum_{k=1}^{d} \lambda_k \left|f_k\right\rangle \otimes \left|g_k\right\rangle, \quad \langle f_k|f_l\rangle = \langle g_k|g_l\rangle = \delta_{kl}$$

$$\lambda_k \geqslant 0$$

Ранг Шмидта r - число ненулевых λ_k

$$\left|\psi^{AB}\right\rangle = \sum_{k=1}^{r} \lambda_k \left|f_k\right\rangle \otimes \left|g_k\right\rangle$$

Для факторизованных состояний $r = 1$, для перепутанных $r > 1$
Обозначения для стандартного базиса кубитных состояний

$$\begin{array}{rll} |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} & & \mathbb{C}^2 \\ |00\rangle = |0\rangle \otimes |0\rangle, & |01\rangle = |0\rangle \otimes |1\rangle, & \\ |10\rangle = |1\rangle \otimes |0\rangle, & |11\rangle = |1\rangle \otimes |1\rangle & \mathbb{C}^{2^2} \end{array}$$

(ладно, я скоро пойму, но еще подумать нужно)

Принципиальная схема квантового компьютера

(картинку от Филиппова вставлю, там и обсуждение короткое этого.)

1.1.4 Definitions of Operators and Mappings

(подробно обсужу определения, укажу критерии и места применения)

Положительность оператора

Матрица плотности подсистем

Блочная положительность оператора

Положительное отображение / оператор

(тут укажу следствия и где оно нужно)

Вполне положительное отображение (?!!)

Вполне положительное отображение - это линейное отображение Φ_t, для которого отображение $\Phi_t \otimes \mathrm{Id}_k$ является положительным для всех $\mathrm{Id}_k : \mathcal{B}(\mathcal{H}_k) \to \mathcal{B}(\mathcal{H}_k)$, $k = 1, 2, \ldots$

пример вполне положительного отображения: $\Phi[\varrho] = A\varrho A^\dagger$ $(\Phi \otimes \mathrm{Id})[X] = A \otimes I \cdot X \cdot A^\dagger \otimes I$ $X = \sum\limits_i \lambda_i \left|\psi_i\right\rangle \left\langle\psi_i\right| \geqslant 0$ $(\Phi \otimes \mathrm{Id})[X] = \sum\limits_i \lambda_i \underbrace{A \otimes I \left|\psi_i\right\rangle}_{|\varphi_i\rangle} \underbrace{\left\langle\psi_i\right| A^\dagger \otimes I}_{\langle\varphi_i|} \geqslant 0$

Пример вполне положительного отображения: $\Phi[\varrho] = \sum\limits_k A_k \varrho A_k^\dagger$ представление крауса

Пример не вполне положительного отображения: транспонирование $(\Phi \otimes \mathrm{Id})[\varrho_{AB}] \equiv \varrho_{AB}^\urcorner \not\geqslant 0$

Матрица Чоя

Деполяризующее отображение (???!!!)

1.1.5 Density Matrix Formalism

Свидетель перепутанности

Выпуклость матриц плотности

(опишу, что про это известно)

Критерий Переса-Городецких

Критерий Переса-Городецких: Матрица плотности двух кубитов является сепарабельной тогда и только тогда, когда она остается матрицей плотности при частичном транспонировании.

(пример, что над большей чем 6 размерностью крит П-Г не работает??)

1.1.6 Entropies in Quantum Information

Основные формулы

(?????)

Обзор энтропий

неравенство Араки-Либа

Смысл энтропии

1.1.7 Basic Quantum Algorithms

6.1 Probabilistic classical computer

6.2 Quantum parallelism

6.3 Deutsch's algorithm

6.4 Quantum Fourier Transform

6.5 Phase estimation

6.6 Order-finding

6.7 Shor's algorithm

1.1.8 Quantum Channels: Basics

О словах

δ-типичные слова

δ-типичное слово - слово w длины n, имеющее вероятность p_w, если

$$2^{-n(H(X)+\delta)} < p_w < 2^{-n(H(X)-\delta)}$$

Для записи $N \approx 2^{nH(X)}$ типичных слов требуется $\log_2 N \approx nH(X)$ бит, т.е. $H(X)$ бит на символ!

Утверждение. Любой код, использующий битовые строки длины $n(H(X) - \delta)$, имеет асимптотически неисчезающую вероятность ошибки, стремящуюся к единице при $n \to \infty$.

Схема сжатия в $1/R$ раз:

$\mathcal{E}^{(n)} : (x_1, x_2, \ldots, x_n) \to$ битовая строка длины nR

Схема развертывания:

$\mathcal{D}^{(n)}$: битовая строка длины $nR \to (x_1, x_2, \ldots, x_n)$

Схема сжатия-развертывания надежна, если

$$\mathrm{P}\left\{\mathcal{D}^{(n)}\left(\mathcal{E}^{(n)}\left(x_1, x_2, \ldots, x_n\right)\right) = (x_1, x_2, \ldots, x_n)\right\} \to 1$$

при $n \to \infty$.

Теорема Шеннона: для надежной схемы $R \geqslant H(X)$.

Изоморфизм Чоя-Ямолковского - критерий квантового канала

Согласно изоморфизму Чоя-Ямиолковского,

линейное отображение Φ является квантовым каналом тогда и только тогда,

когда соответствующая матрица Чоя Ω_Φ является матрицей плотности, удовлетворяющей условию $\operatorname{tr}_1 \Omega_\Phi = \frac{1}{d} I$.

Необходимость следует тривиально из определений.

(??? как????)

дия доказательства достаточности рассмотрим формулу обращения:

$$\Phi[X] = d \operatorname{tr}_2 \left[\Omega_\Phi \cdot I \otimes X^\top\right]$$

$$d \operatorname{tr}_2 \left[\Omega_\Phi \cdot I \otimes X^\top\right] = \operatorname{tr}_2 \left[\sum_{i,j=1}^{d} \Phi[|i\rangle\langle j|] \otimes |i\rangle\langle j| \cdot I \otimes X^\top\right] =$$

$$= \operatorname{tr}_2 \left[\sum_{i,j=1}^{d} \Phi[|i\rangle\langle j|] \otimes |i\rangle\langle j| X^\top\right] = \sum_{i,j=1}^{d} \Phi[|i\rangle\langle j|] \left\langle j \left| X^\top \right| i \right\rangle =$$

$$= \sum_{i,j=1}^{d} \Phi[|i\rangle\langle j|]\langle i|X|j\rangle = \Phi \left[\sum_{i,j=1}^{d} |i\rangle\langle i|X|j\rangle\langle j|\right] = \Phi[X]$$

$\Phi[X] = d \operatorname{tr}_2 \left[\Omega_\Phi \cdot I \otimes X^\top\right]$ $\operatorname{tr}_1 \Omega_\Phi = \frac{1}{d} I$ $\operatorname{tr}[\Phi[X]] = d \operatorname{tr} \left[\Omega_\Phi \cdot I \otimes X^\top\right] = d \operatorname{tr} \left[\operatorname{tr}_1 \left[\Omega_\Phi\right] X^\top\right] = \operatorname{tr} \left[I \cdot X^\top\right] = \operatorname{tr}[X]$

$$\Omega_\Phi = \sum_k \lambda_k |\psi_k\rangle \langle\psi_k| \quad \text{- спектральное разложение} \quad \lambda_k \geqslant 0, \quad |\psi_k\rangle \in \mathcal{H} \otimes \mathcal{H}$$

$$|\psi_k\rangle = \sum_i \mu_i^{(k)} \left|f_i^{(k)}\right\rangle \otimes \left|g_i^{(k)}\right\rangle \text{ - разложение шмидта для каждого вектора}$$

$$\Omega_\Phi = \sum_{k,i,j} \lambda_k \mu_i^{(k)} \mu_j^{(k)} \left|f_i^{(k)}\right\rangle \left\langle f_j^{(k)}\right| \otimes \left|g_i^{(k)}\right\rangle \left\langle g_j^{(k)}\right|$$

$$\Phi[X] = d \operatorname{tr}_2 \left[\sum_{k,i,j} \lambda_k \mu_i^{(k)} \mu_j^{(k)} \left|f_i^{(k)}\right\rangle \left\langle f_j^{(k)}\right| \otimes \left|g_i^{(k)}\right\rangle \left\langle g_j^{(k)}\right| \cdot I \otimes X^\top\right] =$$

$$= d \sum_{k,i,j} \lambda_k \mu_i^{(k)} \mu_j^{(k)} \left|f_i^{(k)}\right\rangle \left\langle f_j^{(k)}\right| \left\langle \overline{g_i^{(k)}} | X | \overline{g_j^{(k)}} \right\rangle$$

(тут пример применения и указание случаев)

Ф-л1. Классическая теория передачи информации

(общие концепции тут)

Ф-л2. Классическая информация через квантовые каналы

Ф-л3. Пропускная способность в терминах «сжатия квантовой информации». Аддитивность классической пропускной способности для канала, разрушающего перепутанность.

(я хз, о чем тут, скорее всего какие-то общие умные слова)

Суть

(!!!! тут определение!!!!)

О пропускной способности канала

$p(y|x)$-стоохсстическая матрица вероятностей переходов

$$p(y|x) \geqslant 0, \quad \sum_y p(y|x) = 1$$

Унистахостичность канала

(?? для задачи актуально понять определение??)

О канале Ландау-Стритера

1.1.9 Quantum Channels: Special Features

Ф-л4 Взаимная информация, Сверхплотное кодирование, Пропускная способность с перепутанностью

Ф-л5 Невозможность клонирования квантовой информации, «телепортация», квантовая пропускная способность

Theorem 4.2 (No-cloning).
(??? add to the theory! is it a good proof?? maybe no)
There exist no unitary $U : \mathcal{H} \otimes \mathcal{H} \to \mathcal{H} \otimes \mathcal{H}$ such that for every quantum state $|\psi\rangle \in \mathcal{H}$

$$U : |\psi\rangle \otimes |e\rangle \mapsto |\psi\rangle \otimes |\psi\rangle,$$

where $|e\rangle \in \mathcal{H}$ in a arbitrary quantum state. Proof. Let us suppose there is such a unitary operator U. Given two quantum states $|\psi\rangle, |\varphi\rangle \in \mathcal{H}$, we have

$$U(|\psi\rangle \otimes |e\rangle) = |\psi\rangle \otimes |\psi\rangle$$
$$U(|\varphi\rangle \otimes |e\rangle) = |\varphi\rangle \otimes |\varphi\rangle$$

On the one hand, taking the inner product of the two states on the l.h.s. yields

$$\big(\not{f}_\psi| \otimes \langle e|\big)U^\dagger U(|\varphi\rangle \otimes |e\rangle) = \langle\psi|\varphi\rangle\langle e|e\rangle = \langle\psi|\varphi\rangle,$$

where we used the fact $U^\dagger U = \mathbb{1}$ and $\langle e|e\rangle = 1$. On the other hand, taking the inner of the states on the r.h.s. yields $\langle\psi|\varphi\rangle^2$. There are only two possibilities, either $\langle\psi|\varphi\rangle = 0$ or $\langle\psi|\varphi\rangle = 1$, implying that either $|\psi\rangle$ and $|\varphi\rangle$ are orthogonal or they are equal. This means that it is only possible to clone states that are orthogonal to one another, and thus that we cannot find a unitary cloning arbitrary qubits.

1.2 Other General Basic Topics

1.2.1 General ways to compute something with cubits?

(в духе, допустим есть кубит, как с помощью этого можно было бы сделать квантовый компьютер? Важный идейный вопрос)

1.2.2 General ways to compute something with superconductors

(в духе, допустим что-то есть в сверхпроводимости, как с помощью этого можно было бы сделать квантовый компьютер? Важный идейный вопрос)

1.2.3 Experimental Tests of Fundamentals of QM

Об экспериментах Аспе

(см. Филлипов, пока не актуально. в теории сперва напишу, большая тема.)

Part II
Special Topics in a Nutshell

2 Special Well-Researched Topics

2.1 Tensor Networks

(maybe one subsection will be enough)

2.2 Tensor Networks

(maybe one subsection will be enough)

2.3 Quantum Cryptography

(maybe one subsection will be enough)

2.3.1 Ф-л7. MPS, MPO

(????)

2.3.2 Ф-л8. MERA

(????)

2.4 Reminder: Basics of QM

2.4.1 Ф-л9. Second Quantization

(хз, мб удалю, мб это и не нужно, посмотрим)

3 Some Other Topics

3.1 Exotic Quantum Gates and Transformation

(такого много можно увидеть, здесь подробно про них и типичные схемы и алгоритмы напишу)

3.1.1 Quantum Search

Основные формулы (????)

Ускорение в сравнении с классикой $\sqrt{N}$.

3.2 Overview of Main Special Topics

3.2.1 Quantum Cryptography: Main Things to Know

(???)

3.2.2 Quantum Error Correction: Main Things to Know

(???)

3.3 Holevo's Book

(надо все это выгружать, потому что иначе я ничего не пойму.)

3.3.1 Введение

0.1. Конечномерные системы 9 0.2. Общие постулаты статистического описания 11 0.3. Классические и квантовые системы 1- 0.4. Рандомизация в классической и квантовой статистике.. 14 0.5. Выпуклая геометрия разложений единицы и фундаментальные пределы точности 15 0.6. Проблема соответствия 16 0.7. Повторные и непрерывные измерения 16 0.8. Необратимая динамика.. 1В 0.9. Квантовые случайные процессы 18

3.3.2 X1. Standard Statistical Model of Quantum Mechanics

§ 1. Основные понятия Ш 1.1. Операторы в Гильбертовом пространстве Ш
2. Оператор плотности 21 1.3. Спектральная мера 22 1.4. Статистический постулат 22 1.5. Совместимые наблюдаемые 23 1.6. Простейший пример 25 § 2. Симметрии, кинематика, динамика 27 2.1. Группы симметрии 27 2.2. Однопараметрические группы 2 2.3. Соотношения Г. Вейля „.... 29 2.4. Гауссовские состояния. 32
§ 3. Составные системы 33 3.1. Тензорное произведение гильбертовых пространств... 33 3.2. Произведение квантовых состояний 34 3.3. Независимость и предельные теоремы..... 35
§ 4. Проблема скрытых параметров 37 4.1. Скрытые параметры и квантовая дополнительность... 37 4.2. Скрытые параметры и квантовая целостность.... 39 4.3. Структура множества квантовых корреляций..... 42

3.3.3 X2. Statistics of Quantum Measurements

§ 1. Обобщенные наблюдаемые 43 1.1. Разложения единицы 43 1.2. Обобщенная статистическая модель квантовой механики.. 45 1.3. Геометрия множества обобщенных наблюдаемых... 47
§ 2. Квантовая теория статистических решений 49 2.1. Проверка гипотез 49 2.2. Байесовская задача 50 2.3. Пропускная способность квантового канала связи... 53 2.4. Общая формулировка 55 2.5. Квантовые неравенства Рао—Крамера 57
§ 3. Ковариантные наблюдаемые 60 3.1. Формулировка проблемы 60 3.2. Структура ковариантного разложения единицы.... 61
3.3. Обобщенные системы импримитивности 62 3.4. Случай абелевой группы 63 3.5. Каноническая сопряженность в квантовой механике... 65 3.6. Локализуемость 68

3.3.4 X3. Evolution of an Open System

§ 1. Преобразования квантовых состояний и наблюдаемых... 69 1.1. Вполне положительные отображения 69 1.2 Операции, динамические отображения 71 1.3. Условные ожидания 73

§ 2. Квантовые динамические полугруппы 74 2.1. Определение и примеры 74 2.2. Инфинитезимальный оператор 75 2.3. Свойство консервативности 77 2.4. Ковариантные эволюции 79 2.5. Эргодические свойства 80 2.6. Расширения динамических полугрупп 81

3.3.5 X4. Consistent and Continuous Measurement Processes

§ 1. Статистика последовательных измерений 85 1.1. Понятие инструмента 85 1.2. Представление вполне положительного инструмента... 87 1.3. Три уровня описания квантовых измерений 89 1.4. Воспроизводимость 90 1.5. Измерения непрерывных наблюдаемых 91

§ 2. Процессы непрерывного измерения 93 2.1. Неразрушающие измерения 93 2.2. «Квантовый парадокс Зенона» 95 2.3. Предельная теорема для сверток инструментов.... 96 2.4. Сверточные полугруппы инструментов -98 2.5. Инструментальные процессы *00

3.3.6 X5. Processes in the Fock Space

§ 1. Квантовое стохастическое исчисление ’03 1.1. Основные определения –03 1.2. Стохастический интеграл 105 1.3. Квантовая формула Ито 108 1.4. Квантовые стохастические дифференциальные уравнения. ПО

§ 2. Расширения в пространстве Фока. 113 2.L Винеровский и пуассоновский процессы в пространстве Фока 114 2.2. Стохастические эволюции и расширения динамических полугрупп 116 2.3. Расширения инструментальных процессов 119 2.4. Стохастические представления процессов непрерывного измерения 121 2.5. Нелинейные стохастические уравнения апостериорной динамики

3.4 Wheeler’s and Zurek’s Book

(??? read it later)

3.5 Some Other Well-Known Articles

(??? read it later)

3.5.1 Decoherence, Einselection, and the Quantum Origins of the Classical by Zurek

(???)

Part III
Fundamentals of Quantum Information Theory

4 Basics of Quantum Information Theory

(?? I'll write later)

4.1 Quantum Noise

(??????????????)

4.2 Quantum Transformations

(??????????????)

4.3 Entropy in Quantum Information

(??????????????)

5 Quantum Polarization States of Photon by Filippov

Рассматриваются вопросы квантового описания поляризационных состояний одиночных и перепутанных фотонов. Вводятся параметры Стокса, сфера Пуанкаре, чистые и смешанные состояния, матрица плотности ансамбля и подсистемы, перепутанные состояния. Излагаются принципы использования поляризационных состояний света в квантово-информационных приложениях: квантовой криптографии, сверхплотном кодировании, квантовой телепортации. Рассматриваются общие принципы динамики открытых квантовых систем. Вводится понятие квантового канала, приводятся примеры дефазирующего и деполяризационного каналов для поляризационных состояний фотонов.

5.0.1 1. Introduction

Поляризационные состояния электромагнитного поля служат своеобразным связующим звеном, наглядно показывающим связь между законами классической электродинамики, справедливыми для волн большой интенсивности, и законами квантового мира, определяющими поведение одиночных фотонов. Этому способствуют как компактное теоретическое описание, так и (в большей степени) относительно простые экспериментальные методы работы с оптическими поляризационными состояниями. Именно при помощи поляризационных состояний впервые были продемонстрированы такие сугубо квантовые явления, как нарушение неравенств Белла [1], протокол квантовой криптографии [2], квантовое сверхплотное кодирование [3], квантовая телепортация [4]. Таким образом, изучение квантовых поляризационных состояний необходимо для успешного освоения квантовых информационных технологий, особенно в области квантовой коммуникации. Кроме того, основные принципы и постулаты квантовой механики (пространство состояний, принцип суперпозиции,

физические наблюдаемые и измерения) находят своё простое выражение в экспериментах с поляризацией одиночных фотонов. Учёт дополнительных степеней свободы (например, частотный спектр) позволяет демонстрировать с помощью поляризационных состояний динамику открытых квантовых систем и познакомить с понятиями матрицы плотности и квантового канала, активно используемых в квантовой теории информации [5].

5.0.2 2. Polarization of Classical Electromagnetic Waves

Рассмотрим плоскую монохроматическую электромагнитную волну с частотой ω, распространяющуюся со скоростью света c вдоль оси z. Волновой вектор $\mathbf{k} \| z, k = \omega/c$. Вектор напряженности электрического поля $\mathbf{E} \perp \mathbf{k}$ и поэтому имеет нулевую компоненту $E_z = 0$. Из уравнений Максвелла следует, что векторная функция $\mathbf{E}$ является гармонической функцией переменной ($kz - \omega t$), называемой фазой:

$$\mathbf{E} = \begin{pmatrix} E_x \\ E_y \\ E_z \end{pmatrix} = \begin{pmatrix} E_1 \cos(kz - \omega t + \varphi_1) \\ E_2 \cos(kz - \omega t + \varphi_2) \\ 0 \end{pmatrix} \tag{1}$$

где φ_1 и φ_2 - сдвиги фазы для горизонтальной и вертикальной компонент поля.

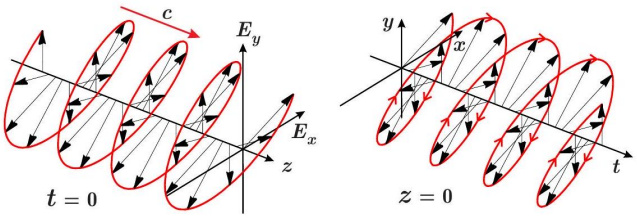


Рис. 1. Слева: напряжённость поля в зависимости от координаты z при фиксированном времени. Справа: зависимость напряжённости поля в фиксированной точке от времени. Здесь и далее будем использовать сокращённые обозначения: $E_{x} \leftrightarrow x, E_{y} \leftrightarrow y$

Для фиксированного момента времени $t = 0$ геометрическое место точек

$$(E_1 \cos(kz + \varphi_1), E_2 \cos(kz + \varphi_2), z) \tag{2}$$

представляет собой винтовую линию (рис. 1).
Для фиксированной координаты $z = 0$ геометрическое место точек

$$(E_1 \cos(-\omega t + \varphi_1), E_2 \cos(-\omega t + \varphi_2), t) \tag{3}$$

также представляет собой винтовую линию, но с противоположной ориентацией (рис. 1). Для фиксированной координаты при увеличении времени t конец вектора $\mathbf{E}$ описывает в xy-плоскости эллипс (рис. 2).

5.0.3 3. Quantum Description of the Polarization of Single Photons

Явление фотоэффекта и другие эксперименты по поглощению света показывают, что электромагнитная энергия поглощается квантами, т.е. порциями $\hbar\omega$, где $\hbar \approx 1,05 \cdot 10^{-27}$ эрг•с - постоянная Планка. Кроме того, будем считать, что переносчиками электромагнитной энергии являются особые частицы - фотоны, несущие квант энергии.

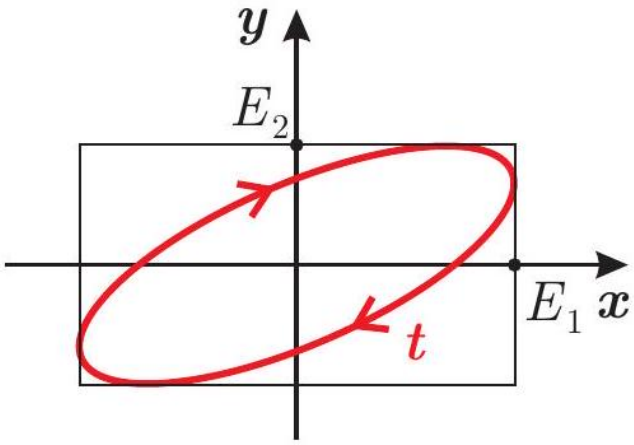


Рис. 2. Эллипс, описываемый вектором напряжённости поля с увеличением времени

Рассмотрим монохроматическую электромагнитную волну с определённой поляризацией. Тогда и все фотоны в волне обладают этой определённой поляризацией. Рассмотрим единичный фотон. С одной стороны, единичный фотон ведёт себя подобно исходной волне (волновые свойства), а с другой стороны, фотон может быть поглощён детектором только полностью или не поглощён вовсе (свойства частицы). Таким образом, имеет место корпускулярно-волновой дуализм.

Для квантового описания единичного фотона мы можем абстрагироваться от абсолютных значений E_1 и E_2, важен лишь вид той винтовой линии, которую описывает в пространстве вектор E. Удобно задать эту форму также вектором, только двумерным, а не трёхмерным, поскольку всегда $E_z = 0$. Далее, вид винтовой линиии определяет не только соотношение между E_1 и E_2, а также соотношение между сдвигами фаз φ_1 и φ_2. Как и в оптике, нагляднее всего соотношение между фазами можно увидеть с помощью комплексных амплитуд $E_1 e^{i(kz-\omega t+\varphi_1)}$ и $E_2 e^{i(kz-\omega t+\varphi_2)}$, действительные части которых равны $E_1 \cos(kz - \omega t + \varphi_1)$ и $E_2 \cos(kz - \omega t + \varphi_2)$ соответственно.

Перейдём на новый уровень абстракции и для описания единичного фотона (вида винтовой линии) будем использовать следующий комплексный вектор, известный в оптике как вектор Джонса:

$$\begin{pmatrix} E_1 \cos(kz - \omega t + \varphi_1) \\ E_2 \cos(kz - \omega t + \varphi_2) \\ 0 \end{pmatrix} \rightarrow |\psi\rangle = \frac{1}{\sqrt{E_1^2 + E_2^2}} \begin{pmatrix} E_1 e^{i(kz-\omega t+\varphi_1)} \\ E_2 e^{i(kz-\omega t+\varphi_2)} \end{pmatrix} \tag{4}$$

в котором намеренно подчёркивается тот факт, что интенсивность нас теперь не интересует (мы имеем дело с одним фотоном).

Далее заметим, что общий фазовый множитель $e^{i(kz-\omega t)}$ присущ самой волне, поскольку мы изначально рассматривали монохроматическую волну. Само значение ω определяет шаг винтовой линии ($\lambda = 2\pi c/\omega$) или угловую скорость, с которой вектор $\mathbf{E}$ описывает эллипс в плоскости xy. Сама форма эллипса задаётся лишь соотношением между $E_1 e^{i\varphi_1}$ и $E_2 e^{i\varphi_2}$. По этой причине нас не интересуют сами зна-

чения φ_1 и φ_2, а интересует лишь разность фаз $\varphi_2 - \varphi_1$ - именно она вкупе с отношением E_1/E_2 определяет форму эллипса. Это означает, что физически следующие записи состояния (4) эквивалентны:

$$\frac{1}{\sqrt{E_1^2+E_2^2}}\begin{pmatrix}E_1e^{i(kz-\omega t+\varphi_1)}\\E_2e^{i(kz-\omega t+\varphi_2)}\end{pmatrix}\longleftrightarrow\frac{1}{\sqrt{E_1^2+E_2^2}}\begin{pmatrix}E_1e^{i\varphi_1}\\E_2e^{i\varphi_2}\end{pmatrix}\longleftrightarrow$$
$$\longleftrightarrow\frac{1}{\sqrt{E_1^2+E_2^2}}\begin{pmatrix}E_1\\E_2e^{i(\varphi_2-\varphi_1)}\end{pmatrix} \tag{5}$$

Физическая эквивалентность означает, что все выводимые нами заключения о наблюдаемых экспериментально величинах должны быть одинаковы для перечисленных выше математических записей состояния.

Запишем некоторые состояния в новых обозначениях. Состояние с горизонтальной поляризацией $(E_1 \neq 0, E_2 = 0) : |H\rangle = \binom{1}{0}$. Состояние с вертикальной поляризацией $(E_1 = 0, E_2 \neq 0) : |V\rangle = \binom{0}{1}$.

Произвольное состояние поляризации фотона имеет вид

$$|\psi\rangle = \begin{pmatrix}c_1\\c_2\end{pmatrix} = c_1\begin{pmatrix}1\\0\end{pmatrix} + c_2\begin{pmatrix}0\\1\end{pmatrix} = c_1|H\rangle + c_2|V\rangle, \tag{6}$$

где $c_1, c_2 \in \mathbb{C}, |c_1|^2 + |c_2|^2 = 1$, представляет собой суперпозицию состояний $|H\rangle$ и $|V\rangle$. Данное математическое описание имеет наглядную физическую интерпретацию: мы имеем дело со сложением гармонических колебаний в x и y направлениях.

Если аргументы φ_1 и φ_2 комплексных чисел c_1 и c_2 совпадают или различаются на π, т.е. $\varphi_1 = \varphi_2$ или $\varphi_2 - \varphi_1 = \pm\pi$, то имеем дело с линейной поляризацией (эллипс вырождается в прямую, рис. 3).

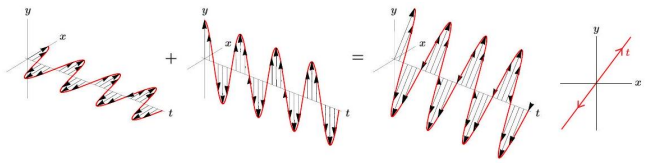


Рис. 3. Состояние $\frac{3}{5}|H\rangle+\frac{4}{5}|V\rangle$ - пример суперпозиции, реализующей фотон с линейной поляризацией

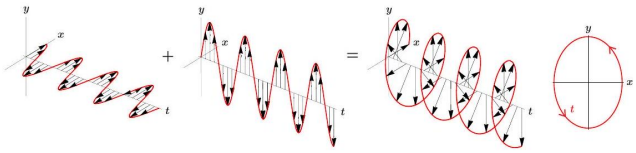


Рис. 4. Состояние $\frac{3}{5}|H\rangle+\frac{4}{5}$ e^{i \pi / 2}|V\rangle$ - пример суперпозиции, реализующей фотон с правой эллиптической поляризацией

Умножение вектора $|V\rangle$ на число $|c_2|\, e^{i\varphi_2}$ означает, что амплитуда колебания вдоль оси y умножается на $|c_2|$, а сама волна сдвинута по фазе на φ_2 (рис. 4 и 5).

Так, если $\varphi_2 - \varphi_1 \in (0, \pi)$, то с увеличением времени конец вектора $\mathbf{E}$ движется против часовой стрелки по эллипсу в плоскости xy (по кратчайшему повороту от x к y). Такое состояние называют состоянием с правой эллиптической поляризацией [6, 7], поскольку это соответствует завинчиванию буравчика вдоль оси z и положительному моменту количества движения относительно направления распространения (рис. 6а).

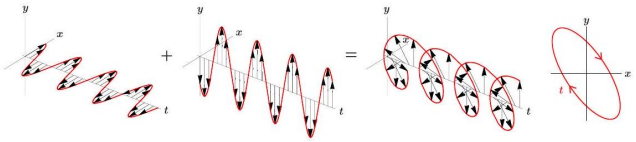


Рис. 5. Состояние $\frac{3}{5}|H\rangle+\frac{4}{5} e^{i 5 \pi / 4}|V\rangle$ - пример суперпозиции, реализующей фотон с левой эллиптической поляризацией

Если $\varphi_2 - \varphi_1 \in (\pi, 2\pi)$, то с увеличением времени конец вектора $\mathbf{E}$ движется по часовой стрелке по эллипсу в плоскости xy (по кратчайшему повороту от y к x). Такое состояние называют состоянием с левой эллиптической поляризацией 6, 7, поскольку это соответствует выкручиванию буравчика из оси z и отрицательному моменту количества движения относительно направления распространения (рис. 6р).

Если $|c_1| = |c_2|$ и $\varphi_2 - \varphi_1 = \pi/2$, то имеем фотон с правой круговой поляризацией, вектор такого состояния $|\circlearrowleft\rangle = \frac{1}{\sqrt{2}}(|H\rangle + i|V\rangle)$.

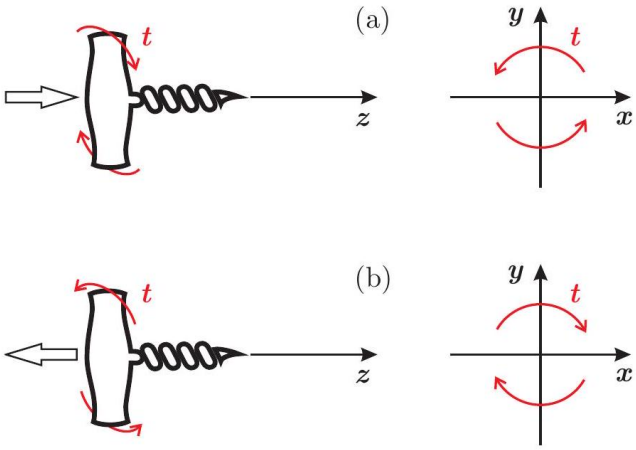


Рис. 6. (a) Правая поляризация. (b) Левая поляризация

Если $|c_1| = |c_2|$ и $\varphi_2 - \varphi_1 = 3\pi/2$, то имеем дело с левой круговой поляризацией, вектор такого состояния $|\circlearrowright\rangle = \frac{1}{\sqrt{2}}(|H\rangle - i|V\rangle)$.

Совершенно понятно, что складывать можно не только колебания в горизонтальной и вертикальной плоскостях. Так, например, складывая с равными по модулю коэффициентами состояния $|\circlearrowleft\rangle$ и $|\circlearrowright\rangle$, будем получать фотоны с линейной поляризацией. Сумма произвольных состояний также будет допустимым состоянием.

Если окажется, что $|c_1|^2 + |c_2|^2 \neq 1$, то нужно будет заменить $c_1 \to c_1/\sqrt{|c_1|^2 + |c_2|^2}$ и $c_2 \to c_2/\sqrt{|c_1|^2 + |c_2|^2}$. Как мы увидим в дальнейшем, сумма $|c_1|^2 + |c_2|^2$ имеет смысл «количества» фотонов и должна равняться единице, если мы знаем, что имеем дело с одним фотоном. Если же фотон мог где-то поглотиться и мы не знаем, поглотился ли он или нет, то сумма $|c_1|^2 + |c_2|^2$ может быть меньше единицы, и вероятность поглощения есть $1 - \left(|c_1|^2 + |c_2|^2\right)$.

Мы увидели, что если отвлечься от условия $|c_1|^2 + |c_2|^2 = 1$ и отождествить состояния, отличающиеся лишь глобальным фазовым множителем, т.е. отождествить состояния $|\psi\rangle$ и $c|\psi\rangle, c \in \mathbb{C}, c \neq 0$, то пространство векторов состояний будет линейным. Правило суперпозиции состояний тогда просто отражение линейности этого пространства. Следующий раздел посвящён краткому повторению соответствующей

главы линейной алгебры.

5.0.4 4. A Unitary Space

Рассмотренные нами векторы $|\psi\rangle$ - элементы унитарного пространства $\mathbb{C}^2$.

Определение 1. Унитарное пространство - комплексное линейное пространство векторов $|\psi\rangle$, в котором каждой упорядоченной паре $|\varphi\rangle$ и $|\psi\rangle$ поставлено в соответствие комплексное число $(|\varphi\rangle, |\psi\rangle)$, обозначаемое кратко $\langle\varphi \mid \psi\rangle$ и называемое их скалярным произведением, так, что выполнены аксиомы:

1. $\langle\varphi \mid \psi\rangle = (\langle\psi \mid \varphi\rangle)^*$;
2. $(|\varphi\rangle, a\,|\psi_1\rangle + b\,|\psi_2\rangle) = a\,\langle\varphi \mid \psi_1\rangle + b\,\langle\varphi \mid \psi_2\rangle$ для любых $a, b \in \mathbb{C}$;
3. $\langle\psi \mid \psi\rangle$ вещественно и $\langle\psi \mid \psi\rangle \geqslant 0$, причём $\langle\psi \mid \psi\rangle = 0 \Leftrightarrow |\psi\rangle = 0$ (нулевой элемент пространства).

Из аксиом 1 и 2 следует, что скалярное произведение линейно по второму аргументу и антилинейно по первому, т.е.

$$(a\,|\varphi_1\rangle + b\,|\varphi_2\rangle\,, |\psi\rangle) = a^*\,\langle\varphi_1 \mid \psi\rangle + b^*\,\langle\varphi_2 \mid \psi\rangle\,, \quad \forall a, b \in \mathbb{C}. \tag{7}$$

Мы будем пользоваться конкретной реализацией скалярного произведения, которое легко понять в обозначениях Дирака: каждому вектору-столбцу $|\psi\rangle$ поставим в соответствие вектор-строку $\langle\psi|$ по следующему правилу:

$$|\psi\rangle = \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} \quad \longrightarrow \quad \langle\psi| = \begin{pmatrix} c_1^* & c_2^* \end{pmatrix} = (|\psi\rangle)^\dagger. \tag{8}$$

В последнем равенстве мы использовали операцию эрмитового сопряжения матриц $\dagger = \top* = *\top$, которая осуществляет транспонирование и комплексное сопряжение.

Определение 2. Матрица $A^\dagger = A^{\top *}$ размерности $n \times m$ называется эрмитово сопряженной к матрице A размера $m \times n$:

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}^\dagger = \begin{pmatrix} a_{11}^* & \cdots & a_{m1}^* \\ \vdots & \ddots & \vdots \\ a_{1n}^* & \cdots & a_{mn}^* \end{pmatrix}. \tag{9}$$

Тогда легко реализовать скалярное произведение векторов $|\varphi\rangle = \binom{d_1}{d_1}$ и $|\psi\rangle = \binom{c_1}{c_2}$ как произведение строки и столбца:

$$\underbrace{\langle\varphi \mid \psi\rangle}_{\text{bracket}} = \underbrace{\langle\varphi|}_{\text{bra}}\,\underbrace{|\psi\rangle}_{\text{ket}} = \begin{pmatrix} d_1^* & d_2^* \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = d_1^* c_1 + d_2^* c_2. \tag{10}$$

По понятной причине векторы-строки $\langle\cdot|$ принято называть бравекторами, а векторы-столбцы $|\cdot\rangle$ - кет-векторами.

Очевидно, что введённое таким образом скалярное произведение удовлетворяет аксиомам 1-3. В частности, норма вектора

$$\langle\psi \mid \psi\rangle = |c_1|^2 + |c_2|^2\,. \tag{11}$$

Пусть $|\chi\rangle = A|\psi\rangle$, где A - квадратная матрица с элементами a_{ij} (для наших примеров матрица размера 2×2). Тогда

$$\langle\varphi \mid \chi\rangle = (|\varphi\rangle, A|\psi\rangle) = \langle\varphi|A|\psi\rangle = \sum_{ij} d_i^* a_{ij} c_j = \left(\sum_{ji} c_j^* a_{ij}^* d_i\right)^* =$$
$$= \left(|\psi\rangle, A^\dagger|\varphi\rangle\right)^* = \left(A^\dagger|\varphi\rangle, |\psi\rangle\right) \qquad (12)$$

т.е. $(|\varphi\rangle, A|\psi\rangle) = \left(A^\dagger|\varphi\rangle, |\psi\rangle\right)$ или кратко $\langle\varphi \mid A\psi\rangle = \left\langle A^\dagger\varphi \mid \psi\right\rangle$. Из равенства (12) сразу следует, что $(\hat{A}\hat{B}\ldots\hat{F})^\dagger = \hat{F}^\dagger\ldots\hat{B}^\dagger\hat{A}^\dagger$. В частности, $(A|f\rangle)^\dagger = \langle f|A^\dagger$.

Введём ещё два определения.

Определение 3. Квадратная матрица A называется эрмитовой, если $A = A^\dagger$.

Определение 4. Невырожденная квадратная матрица U называется унитарной, если $U^\dagger U = UU^\dagger = I$, где I - единичная матрица, т.е. $U^{-1} = U^\dagger$.

5.0.5 5. Measurements and Observables

Раздел квантовых измерений традиционно в недостаточной мере излагается в стандартных курсах квантовой механики. Отчасти это связано с тем, что в середине XX века возможности эксперимента не позволяли работать с одиночными квантовыми системами, опыты проводились с макроскопическими ансамблями, где главное значение имеют средние значения, а не результаты отдельных наблюдений. Тем не

менее в связи с продолжающейся миниатюризацией в микро- и наноэлектронике, развитием техники низких температур, созданием высокодобротных резонаторов для электромагнитного поля открылись новые возможности для манипулирования и проведения измерений над отдельными квантовыми системами. Квантовые поляризационные состояния фотонов начали использовать одними из первых, что позволило продемонстрировать с их помощью ряд интересных квантовых эффектов.

5.1. Поляроид

Если на пути фотона поставить идеальный фотодетектор, то он его зарегистрирует с вероятностью 1 («щелчок», рис. 7). Если же фотона нет, щелчка не будет.

Рис. 7. Фотон поглощается идеальным детектором

Проведем аналогичный опыт, но на пути фотона поставим поляроид. Для макроскопической электромагнитной волны поляроид, ориентированный вдоль некоторого направления, на выходе выдает компоненту волны с поляризацией вдоль этого направления, а перпендикулярную компоненту поглощает.

Опыт показывает, что одиночный фотон (в определённом состоянии $|\psi\rangle$) может как пройти через поляроид и вызвать щелчок детектора, так и поглотиться в поляроиде и не быть зафиксированным

детектором. Причём заранее невозможно предсказать, какой вариант реализуется. Результат носит принципиальный вероятностный характер (рис. 8).

Единственными случаями, когда результат можно предсказать, являются случаи линейной поляризации вдоль и поперёк оси поляроида: в первом случае фотон детектируется с вероятностью 1 , во втором с вероятностью 0 .

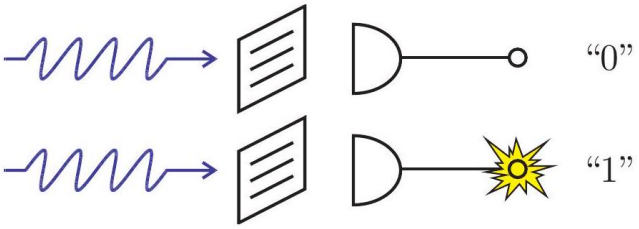


Рис. 8. Вероятностный характер срабатывания детектора для фиксированного состояния фотона

Дело в том, что поляроид проецирует состояния и может выдавать на выходе фотоны только с поляризацией вдоль этого направления. Например, если поляроид ориентирован горизонтально, то на выходе из него все пролетающие фотоны находятся в состоянии $|H\rangle$ (рис. 9).

Действие такого поляроида задаётся проектором

$$P = |H\rangle\langle H| = \begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}1 & 0\end{pmatrix} = \begin{pmatrix}1 & 0\\0 & 0\end{pmatrix}. \tag{13}$$

Подействуем этим проектором на произвольное состояние фотона $|\psi\rangle = c_1|H\rangle + c_2|V\rangle$:

$$P|\psi\rangle = |H\rangle\langle H||\psi\rangle = |H\rangle \underbrace{\langle H \mid \psi\rangle}_{\text{число}} = \langle H \mid \psi\rangle|H\rangle = c_1|H\rangle = \begin{pmatrix}c_1\\0\end{pmatrix}. \tag{14}$$

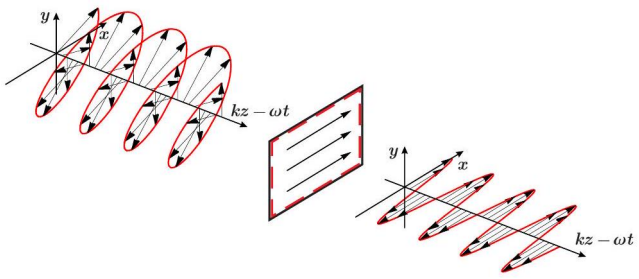


Рис. 9. Действие поляроида, ориентированного в горизонтальном направлении. Фотон либо поглощается поляроидом, либо проходит через него с горизонтальной поляризацией

Мы видим, что норма вектора $P|\psi\rangle$ равна $|c_1|^2 \leqslant 1$. Это указывает на поглощение фотона поляроидом. Действительно, опыт показывает, что вероятность зафиксировать фотон детектором в точности

равна $|c_1|^2$. С другой стороны, эта вероятность есть не что иное, как $|\langle H \mid \psi\rangle|^2$. Вероятность поглощения равна $1 - |c_1|^2 = |c_2|^2 = |\langle V \mid \psi\rangle|^2$.

Для прояснения связи физики и математики вспомним математическую задачу поиска собственных векторов и собственных значений матрицы. Для заданной матрицы A требуется найти числа λ и ненулевые векторы $|f\rangle$ такие, что

$$A|f\rangle = \lambda|f\rangle. \tag{15}$$

Поиск собственных значений заключается в решении уравнения $\det(A - \lambda I) = 0$, а затем решения системы уравнений $(A - \lambda I)|f\rangle = 0$.

Матрица P эрмитова, её собственные значения равны 1 и 0 , соответствующие им собственные векторы - это векторы $|H\rangle$ и $|V\rangle$.

Заметим, что собственные значения матрицы (13) равны 1 и 0 . Это можно интерпретировать следующим образом. Физической наблюдаемой «прохождение фотона» приписаны два значения: значение « 1 », если фотон задетектирован приёмником, и значение «0», если фотон не задетектирован (рис. 8). В единичном акте измерения с одним налетающим фотоном мы получаем одно значение: либо значение « 1 », либо значение « 0 ». Вероятность исхода « 1 » равна $|\langle H \mid \psi\rangle|^2 = |\langle \psi \mid H\rangle|^2$, т.е. квадрату модуля скалярного произведения вектора состояния фотона $|\psi\rangle$ и собственного вектора P, отвечающего собственному значению 1. Аналогично, вероятность исхода «0» равна $|\langle V \mid \psi\rangle|^2 = |\langle \psi \mid V\rangle|^2$, т.е. квадрату модуля скалярного произведения вектора состояния фотона $|\psi\rangle$ и собственного вектора P, отвечающего собственному значению 0 .

Среднее значение физической наблюдаемой «прохождение фотона» есть математическое ожидание:

$$1 \cdot (\text{ вероятность исхода « 1}) + 0 \cdot (\text{ вероятность исхода « 0}) =$$
$$= 1 \cdot |c_1|^2 + 0 \cdot |c_2|^2 = \begin{pmatrix} c_1^* & c_2^* \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \langle\psi|P|\psi\rangle \equiv \langle P\rangle.$$

Запись $\langle P\rangle$ означает среднее значение наблюдаемой, где усреднение ведётся по результатам измерений для фиксированного состояния фотона $|\psi\rangle$ (много фотонов, каждый из которых находится в состоянии $|\psi\rangle$, пропускаем через поляроид и смотрим, щёлкнул ли детектор). Такие средние называют средними по состоянию $|\psi\rangle$, что и подразумевает запись $\langle P\rangle \equiv \langle\psi|P|\psi\rangle$. Саму измеряемую величину «прохождение фотона» тоже можно обозначить буквой $P_{\text{физ.вел.}} = \{1, 0\}$, которая может принимать два значения. Тогда

$$\langle P_{\text{физ.вел.}} \rangle = \langle\psi|P|\psi\rangle. \tag{16}$$

5.2. Двулучепреломляющий кристалл

Рассмотрим более интересный случай измерения с двулучепреломляющим кристаллом (рис. 10). При попадании одиночного фотона на двулучепреломляющий кристалл компонента, поляризованная горизонтально, не отклоняется, а компонента, поляризованная вертикально, отклоняется от первоначального направления распространения луча (пунктирными линиями показаны фронты элементарных волн). Поставив два детектора, в каждом единичном акте мы будем наблюдать экспериментально срабатывание лишь одного из детекторов. Можно считать, что до попадания в детектор фотон находится в обоих лучах одновременно: u в верхнем, u в нижнем (принцип суперпозиции). Однако, будучи частицей, фотон может быть зарегистрирован только в одном детекторе - либо в верхнем, либо в нижнем, т.е. происходит коллапс состояния.

Срабатыванию верхнего детектора припишем значение « $+1$ », а срабатыванию нижнего - «-1». Обозначим соответствующую физическую величину $Z_{\text{физ.вел.}}$, тогда для состояния $|\psi\rangle = \binom{c_1}{c_2}$ получим

$$\langle Z_{\text{физ.вел.}} \rangle = (+1) \cdot |c_1|^2 + (-1) \cdot |c_2|^2 =$$
$$= \begin{pmatrix} c_1^* & c_2^* \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \langle\psi|\sigma_3|\psi\rangle, \tag{17}$$

где $\sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ - матрица, отвечающая физической наблюдаемой $Z_{\text{физ.вел.}}$. Видно, что собственные значения σ_3 - числа $+1$ и -1 , а отвечающие им собственные векторы -

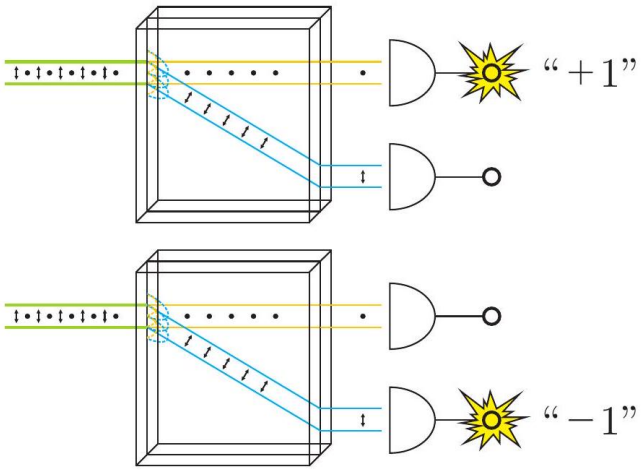


Рис. 10. Схема измерения параметра Стокса $\langle\psi| \sigma_{3}|\psi\rangle$

$|H\rangle$ и $|V\rangle$.

Величину $\langle\psi|\sigma_3|\psi\rangle = |c_1|^2 - |c_2|^2$ также называют 3-м параметром Стокса. Схема на рис. 10 показывает, как этот параметр можно измерить экспериментально, суммируя количество срабатываний верхнего (N_+) и нижнего (N_-) детекторов и вычисляя отношение ($N_+ - -N_-$) / ($N_+ + N_-$)при многократном отправлении на двулучепреломляющий кристалл идентичных фотонов в состоянии $|\psi\rangle$.

5.3. Поворот плоскости поляризации

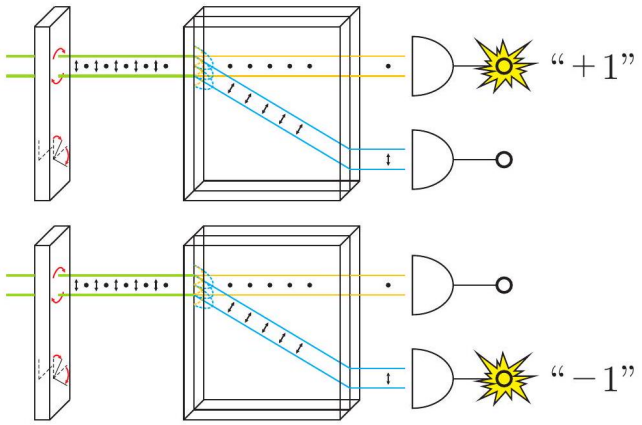


Рис. 11. Схема измерения параметра Стокса $\langle\psi| \sigma_{1}|\psi\rangle$

Видоизменим эксперимент, поставив перед двулучепреломляющим кристаллом пластинку, в которой вследствие эффекта Фарадея плоскость поляризации поворачивается на угол $-45°$, рис. 11. Такой по-

ворот плоскости поляризации отвечает обычному повороту плоскости Oxy и задаётся унитарной матрицей $U = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$. Тогда

$$|\psi\rangle \longrightarrow |\varphi\rangle = U|\psi\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} c_1 + c_2 \\ -c_1 + c_2 \end{pmatrix}. \tag{18}$$

Получим новую физическую величину $X_{\text{физ.вел.}}$, среднее значение которой равно

$$\langle X_{\text{физ.вел.}}\rangle = \frac{1}{2}\,|c_1+c_2|^2 - \frac{1}{2}\,|-c_1+c_2|^2 = \langle\varphi|\sigma_3|\varphi\rangle = \langle\psi|U^\dagger\sigma_3 U|\psi\rangle. \tag{19}$$

Приходим к выводу, что среднее значение $\langle X_{\text{физ.вел.}}\rangle$ равно $\langle\psi|\sigma_1|\psi\rangle$, где $\sigma_1 = U^\dagger\sigma_3 U = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ -1 & 1\end{pmatrix} = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$.

Матрица σ_1 эрмитова, её собственные значения равны ± 1, а собственные векторы равны $\frac{1}{\sqrt{2}}\binom{1}{\pm 1}$ соответственно.

Если бы фотон изначально находился в состоянии $\frac{1}{\sqrt{2}}\binom{1}{1}$, то при повороте плоскости поляризации на $-45°$ он бы превратился в фотон с горизонтальной поляризацией (вектор $|H\rangle = \binom{1}{0}$) и с определённостью попал бы в верхний детектор, и мы бы с определённостью получили значение « $+1$ ».

Если бы фотон изначально находился в состоянии $\frac{1}{\sqrt{2}}\binom{1}{-1}$, то при повороте плоскости поляризации на $-45°$ он бы превратился в фотон с вертикальной поляризацией (вектор $-|V\rangle = \binom{0}{-1}$) и с определённостью попал бы в нижний детектор, и мы бы с определённостью получили значение «-1».

Этот пример ещё раз показывает, что каждой измеряемой физической величине можно поставить в соответствие матрицу, собственные векторы которой определяют такие состояния, для которых исходы измерения принимают определённое значение.

Величину $\langle\psi|\sigma_1|\psi\rangle = c_2^* c_1 + c_1^* c_2 = 2\,\mathrm{Re}\,(c_1^* c_2)$ также называют 1 -м параметром Стокса. Схема на рис. 11 показывает, как этот параметр можно измерить экспериментально.

5.0.6 5.4. Phase Shift

Рассмотрим, наконец, случай, когда перед двулучепреломляющим кристаллом и пластинкой, вращающей плоскость поляризации на угол $-45°$, установлена так называемая пластинка $\lambda/4$, которая создаёт между горизонтальной и вертикальной компонентами поляризации разность фаз $\pi/2$ (из-за разных скоростей распространения волн, поляризованных горизонтально и вертикально). Действие такой пластинки задаётся унитарной матрицей:

$$W = \begin{pmatrix}i & 0\\ 0 & 1\end{pmatrix}, \quad |\psi\rangle \longrightarrow |\chi\rangle = W|\psi\rangle = \begin{pmatrix}i & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}c_1\\ c_2\end{pmatrix} = \begin{pmatrix}ic_1\\ c_2\end{pmatrix}. \tag{21}$$

Получим новую физическую величину $Y_{\text{физ.вел.}}$, среднее значение которой равно

$$\langle Y_{\text{физ.вел.}}\rangle = \langle\chi|\sigma_1|\chi\rangle = \langle\psi|W^\dagger\sigma_1 W|\psi\rangle. \tag{22}$$

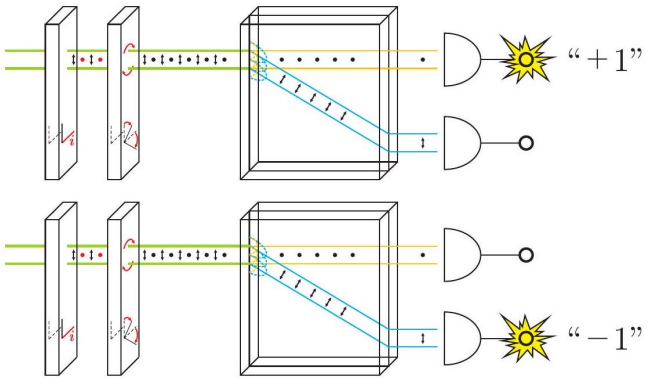


Рис. 12. Схема измерения параметра Стокса $\langle\psi| \sigma_{2}|\psi\rangle$

Приходим к выводу, что среднее значение $\langle Y_{\text{физ.вел.}} \rangle$ равно $\langle\psi|\sigma_2|\psi\rangle$, где

$$\sigma_2 = W^\dagger \sigma_1 W = \begin{pmatrix} -i & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}. \tag{23}$$

Матрица σ_2 эрмитова, её собственные значения равны ± 1, а собственные векторы равны $\frac{1}{\sqrt{2}}\binom{1}{\pm i}$ соответственно.

Если бы фотон изначально находился в состоянии с правой круговой поляризацией $|\circlearrowright\rangle = \frac{1}{\sqrt{2}}\binom{1}{i}$, то после сдвига фаз он бы превратился в фотон с линейной поляризацией $\frac{i}{\sqrt{2}}\binom{1}{1}$ и в итоге с определённостью попал бы в верхний детектор, и мы бы с определённостью получили значение « $+1$ ».

Если бы фотон изначально находился в состоянии с левой круговой поляризацией $|\circlearrowleft\rangle = \frac{1}{\sqrt{2}}\binom{1}{-i}$, то после сдвига фаз он бы превратился в фотон с линейной поляризацией $\frac{i}{\sqrt{2}}\binom{1}{-1}$ и в итоге с определённостью попал бы в нижний детектор, и мы бы с определённостью получили значение « -1 ».

Величину $\langle\psi|\sigma_2|\psi\rangle = i\left(c_2^* c_1 - c_1^* c_2\right) = 2\,\mathrm{Im}\left(c_1^* c_2\right)$ также называют 2 -м параметром Стокса. Схема на рис. 12 показывает, как этот параметр можно измерить экспериментально.

5.0.7 6. The Poincare Sphere

Для начала покажем, что физические свойства квантового состояния $|\psi\rangle = c_1|H\rangle + c_2|V\rangle$ одиночного фотона определяются двумя вещественными параметрами. Несмотря на то, что задание комплексных чисел c_1 и c_2 эквивалентно заданию 4 -х вещественных параметров, вопервых, общий фазовый множитель не изменяет физических свойств состояния, во-вторых, имеется условие нормировки $|c_1|^2 + |c_2|^2 = 1$. Таким образом, состояние $|\psi\rangle$ можно описать двумя действительными параметрами, в частности углами на сфере $\theta \in [0, \pi]$ и $\varphi \in [0, 2\pi]$:

$$|\psi\rangle = \begin{pmatrix} \cos\frac{\theta}{2} e^{-i\varphi/2} \\ \sin\frac{\theta}{2} e^{i\varphi/2} \end{pmatrix} \tag{24}$$

При такой параметризации

$$s_x := \langle\psi|\sigma_x|\psi\rangle = \sin\theta\cos\varphi \tag{25}$$
$$s_y := \langle\psi|\sigma_y|\psi\rangle = \sin\theta\sin\varphi \tag{26}$$
$$s_z := \langle\psi|\sigma_z|\psi\rangle = \cos\theta \tag{27}$$

Величины s_x, s_y, s_z называются параметрами Стокса и полностью характеризуют поляризационное квантовое состояние одиночного фотона $|\psi\rangle$. Заметим, что состояние (24) является собственным для оператора $\mathbf{s}\cdot\hat{\boldsymbol{\sigma}} = s_x\hat{\sigma}_x + s_y\hat{\sigma}_y + s_z\hat{\sigma}_z$.

Таким образом, множеству физических состояний $|\psi\rangle$ можно поставить в соответствие сферу Пуанкаре (см. рис. 13). Линейной поляризации соответствует сечение сферы плоскостью Oxz. Правой круговой поляризации соответствует точка $(0, 1, 0)$, левой круговой поляризации - точка $(\ 0, -1, 0\ )$.

5.0.8 7. The Density Matrix of the Ensemble

Рассмотренные выше понятия были сформулированы для одиночных фотонов, описываемых векторами состояния $|\psi\rangle$, называемых так-

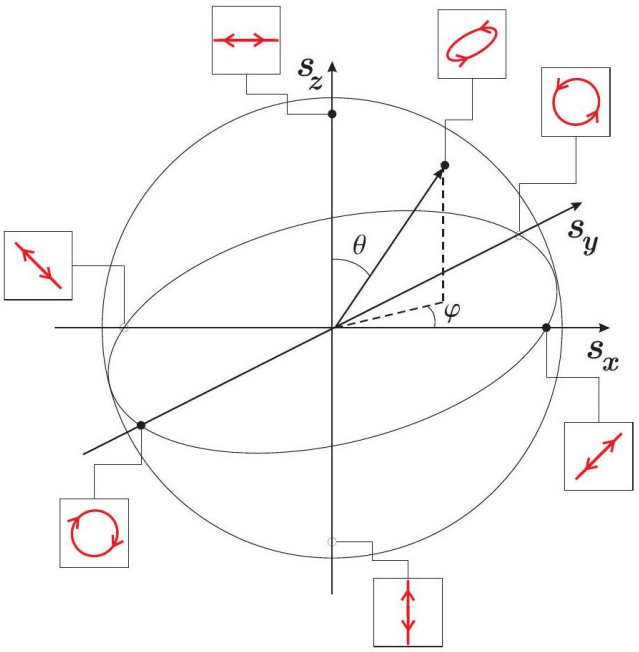


Рис. 13. Сфера Пуанкаре

же чистыми состояниями. Рассмотрим теперь ансамбль чистых состояний $\{p_i, |\psi_i\rangle\}$, в котором каждое состояние $|\psi_i\rangle$ встречается с вероятностью p_i, причём $\sum_i p_i = 1$. Тогда среднее значение некоторой физической величины $\hat{A}$ по такому ансамблю будет определяться формулой

$$\langle \hat{A} \rangle = \sum_i p_i \langle \psi_i | \hat{A} | \psi_i \rangle = \mathrm{tr}(\hat{A}\hat{\varrho}), \tag{28}$$

где $\hat{\varrho} = \sum_i p_i |\psi_i\rangle \langle \psi_i|$ - оператор плотности, $\mathrm{tr}\,\hat{M} = \sum_i \langle i|\hat{M}|i\rangle = \sum_i M_{ii}$ - след оператора, вычисляемый как сумма диагональных элементов матрицы оператора, записанного в ортонормированном базисе $\{|i\rangle\}$.

Матрица плотности ϱ с элементами $\varrho_{ij} = \langle i|\hat{\varrho}|j\rangle$ обладает следующими свойствами: 1) эрмитовость $\varrho^\dagger = \varrho$; 2) неотрицательная определённость $\varrho \geqslant 0$; 3) единичный след $\mathrm{tr}\,\varrho = 1$. Действительно,
1)

$$\hat{\varrho}^\dagger = \sum_i p_i \left(|\psi_i\rangle \langle \psi_i|\right)^\dagger = \sum_i p_i |\psi_i\rangle \langle \psi_i| = \hat{\varrho}; \tag{29}$$

2.

$$\langle \chi|\hat{\varrho}|\chi\rangle = \sum_i p_i \langle \chi \mid \psi_i\rangle \langle \psi_i \mid \chi\rangle = \sum_i p_i |\langle \chi \mid \psi_i\rangle|^2 \geqslant 0, \quad \forall |\chi\rangle; \tag{30}$$

$$\mathrm{tr}\,\hat{\varrho} = \sum_i p_i \,\mathrm{tr}\left(|\psi_i\rangle \langle \psi_i|\right) = \sum_i p_i \langle \psi_i \mid \psi_i\rangle = \sum_i p_i = 1. \tag{3))}$$

Обратно, пусть имеется оператор $\hat{\varrho}$, удовлетворяющий свойствам (29) - (31), тогда найдутся вероятности p_i и состояния $|\psi_i\rangle$ такие, что $\hat{\varrho} = \sum_i p_i |\psi_i\rangle \langle \psi_i|$. Заметим, что в общем случае представление суммой $\hat{\varrho} = \sum_i p_i |\psi_i\rangle \langle \psi_i|$ не единственно. Один из способов заключается в том, чтобы в качестве p_i взять собственные значения ϱ, а в качестве $|\psi_i\rangle$ соответствующие им ортонормированные собственные векторы.

Мы приходим к выводу, что статистические свойства ансамбля одиночных фотонов полностью определяются оператором плотности. В этом случае поляризационная матрица плотности имеет вид

$$\varrho = \begin{pmatrix} \varrho_{HH} & \varrho_{HV} \\ \varrho_{VH} & \varrho_{VV} \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1+s_3 & s_1 - is_2 \\ s_1 + is_2 & 1-s_3 \end{pmatrix}, \tag{32}$$

где $s_i = \langle \sigma_i \rangle = \mathrm{tr}\,(\varrho \sigma_i)$ - параметры Стокса в общем случае.
Условие $\varrho \geqslant 0$ эквивалентно условию $s_1^2 + s_2^2 + s_3^2 \leqslant 1$, т.е. матрица плотности задаётся точкой внутри шара на рис. 13. Граница шара (сфера Пуанкаре) соответствует так называемым чистым состояниям $\hat{\varrho} = |\psi\rangle\langle\psi|$, а внутренние точки шара - смешанным состояниям $\hat{\varrho} \neq |\psi\rangle\langle\psi|$. Нетрудно заметить, что состояние является чистым тогда и только тогда, когда $\mathrm{tr}\,(\varrho^2) = 1$.

5.0.9 8. Partially Polarized Light

Смешанные состояния соответствуют частично поляризованному свету. В классической теории поля такая ситуация возникает для немонохроматической электромагнитной волны. Напряжённость электрического поля в некоторой точке пространства: $\mathbf{E} = \mathbf{E}_0(t) e^{-i\omega t}$, где $\omega-$ средняя частота излучения. Амплитуда $\mathbf{E}_0(t) \in \mathbb{C}^2$ медленно меняется со временем на временах ω^{-1}, если волна почти монохроматическая, т.е. $\Delta\omega \ll \omega$. Зависимость $\mathbf{E}_0(t)$ показывает, что форма эллиптической поляризации меняется со временем, причём характерное время изменения формы эллипса $-(\Delta\omega)^{-1}$. Средняя интенсивность волны определяется выражением $J = \overline{\mathbf{E}\mathbf{E}^*} = \overline{\mathbf{E}_0\mathbf{E}_0^*}$, где черта сверху означает усреднение по времени $T \gg (\Delta\omega)^{-1}$. Усреднённые по времени свойства поляризации описываются тензором

$$\rho_{\alpha\beta} = \frac{1}{J}\overline{\mathbf{E}_\alpha \mathbf{E}_\beta^*} = \frac{1}{J}\overline{\mathbf{E}_{0\alpha}\mathbf{E}_{0\beta}^*}, \tag{33}$$

называемым поляризационным тензором классического электромагнитного излучения [8]. Индексы $\alpha, \beta = 1, 2$ обозначают направления в пространстве, ортогональные направлению распространения волны. Заметьте, что $\sum_\alpha \rho_{\alpha\alpha} = 1$.

Связь классического и квантового описания сводится к тому, что усреднение по времени для классической электромагнитной волны эквивалентно усреднению по ансамблю для квантовых состояний фотонов, т.е. введённая в квантовой теории матрица плотности $\varrho_{\alpha\beta}$ совпадает с поляризационным тензором $\rho_{\alpha\beta}$. Введённые ранее параметры Стокса определяют степень поляризации: $P = \sqrt{s_1^2 + s_2^2 + s_3^2}$.

Для неполяризованного света $\varrho = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ и $P = 0$. Неполяризованный свет может быть представлен как равновероятная смесь состояний $|H\rangle$ и $|V\rangle$ или равновероятная смесь любых других ортогональных состояний, например $|\circlearrowleft\rangle$ и $|\circlearrowright\rangle$, или равновероятная смесь всех состояний на сфере Пуанкаре.

Если разброс частот $\Delta\omega = 0$, то классическое описание разрешает лишь поляризационные тензоры вида $\rho_{\alpha\beta} = \frac{1}{J}\mathbf{E}_{0\alpha}\mathbf{E}_{0\beta}^*$, т.е. такие, для которых $\det\rho = 0$ и степень поляризации $P = 1$. Неполяризованный свет можно описать классически только статистически, т.е. как серию волн, поляризации которых различны и никак не коррелированы между собой. Таким образом, само существование неполяризованного света указывает на его квантовую природу [9]. В квантовом описании фотон может с разной вероятностью находиться в различных состояниях поляризации с одной и той же частотой.

5.0.10 9. Quantum Cryptography

Рассмотрим принцип работы простейшей квантовой криптографической схемы BB84 (названной так по фамилиям авторов и году публикации [2]). Протокол предназначен для секретной передачи классической информации, закодированной бинарным образом, т.е. нулями и единицами.

На передающем устройстве A установлен однофотонный источник, приготавливающий состояния $|H\rangle, |V\rangle, |\nearrow\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle), |\swarrow\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)$. Состояния $|H\rangle$ и $|V\rangle$ образуют 1-й ортонормированный базис, состояния $|\nearrow\rangle$ и $|\swarrow\rangle$ образуют 2 -й ортонормированный базис. Таким образом, состояния можно переобозначить следующим образом: $|H\rangle = |0+\rangle, |V\rangle = |1+\rangle, |\nearrow\rangle = |0\times\rangle, |\swarrow\rangle = |1\times\rangle$, где первый символ соответствует передаваемому биту (0 или 1), а второй используемому базису (+ или ×). На передающем устройстве равновероятно выбирается одно из $4 - x$ состояний и отправляется адресату. Для каждого приходящего фотона адресат на приемном конце B использует либо схему, показанную на рис. 10, либо схему, показанную на рис. 11 (равновероятно). Схема на рис. 10 однозначно различает состояния $|H\rangle$ и $|V\rangle$, поэтому обозначим её «+». Схема на рис. 11 однозначно различает состояния $|\nearrow\rangle$ и $|\swarrow\rangle$, поэтому обозначим её « × ». Щелчок верхнего детектора (0) или нижнего детектора (1) для каждой из схем фиксируется и записывается как результат измерения в выбранном базисе.

Рассмотрим возможный вариант измерений:

состояние A	0×	0+	1+	1+	1×	0×	1+	0×	0+	1×
базис B	+	+	×	+	×	+	+	×	×	+
измерение B	1	0	1	1	1	0	1	0	1	0
совп. баз. A и B	нет	да	нет	да	да	нет	да	да	нет	нет
бит A		0		1	1		1	0		
бит B		0		1	1		1	0		

С вероятностью $\frac{1}{2}$ на передающем и принимающем концах выберут разные базисы (+ и ×) и результат измерения на конце B с вероятностью $\frac{1}{2}$ будет 0 или 1 . Если же базисы на передающем и принимающем концах совпадают, то с вероятностью 1 на конце B зарегистрируется именно тот исход (0 или 1), который был использован на передающем конце. Сверка базисов между A и B производится по открытому каналу связи (телефону), однако результат измерения не сообщается! В случае совпадения базисов A знает переданный бит, B знает результат

измерения, и они должны совпадать! Таким способом можно осуществить передачу ключа.

Допустим, что подслушиватель E внедряется в квантовую линию передачи фотонов и пытается измерить их до того, как они будут зарегистрированы на принимающем конце. Для получения хоть какойнибудь информации подслушиватель E должен измерять фотоны, а новые приготовленные фотоны отправлять к принимающему концу. Если подслушиватель E угадывает базис A, то он может оставаться незамеченным. Вероятность угадывания равна $\frac{1}{2}$. При неправильном угадывании испущенный подслушивателем E фотон будет отличаться от фотона, испущенного A, и с вероятностью $\frac{1}{2}$ приведёт к неправильному исходу даже при совпадении базисов A и B :

состояние A	$0\times$	$0+$	$1+$	$1+$	$1\times$	$0\times$	$1+$	$0\times$	$0+$	$1\times$
базис E	$\times$	$+$	$\times$	$+$	$\times$	$+$	$\times$	$+$	$\times$	$+$
базис B	$+$	$+$	$\times$	$+$	$\times$	$+$	$+$	$\times$	$\times$	$+$
измерение B	1	0	1	1	1	0	1	1	1	0
совп. баз. A и B	нет	да	нет	да	да	нет	да	да	нет	нет
бит A		0		1	1		1	0		
бит B		0		1	1		1	1		

Несовпадение показано квадратной рамкой. Таким образом, A и B по незащищенному каналу связи открывают базисы измерений, и для совпадающих базисов проверяют на совпадение часть результатов измерений B и приготовлений A. Обнаружение ошибки в этой части означает подслушивание. Вероятность ошибки при подслушивании равна 25%. Таким образом, квантово-механический принцип суперпозиции позволяет обеспечить секретную коммуникацию.

На практике ошибки могут возникать не только в результате подслушивания, но и вследствие шумов. Поэтому устанавливается некоторый порог ошибок ($p_{\text{cut}} < 25\%$), в пределах которого связь является секретной и допускает процедуру исправления.

5.0.11 10. Two-Photon Entangled States

Рассмотрим поляризационные степени свободы системы, составленной из двух фотонов, и пренебрежем пространственно-частотными характеристиками электромагнитного поля. Базисными векторами составной системы являются состояния $H_1H_2, H_1V_2, V_1H_2, V_1V_2$, т.е. мы

имеем дело с пространством состояний $\mathbb{C}^4$. Определим тензорное произведение векторов $|\psi\rangle = \begin{pmatrix} c_H & c_V \end{pmatrix}^\top$ и $|\chi\rangle = \begin{pmatrix} d_H & d_V \end{pmatrix}^\top$ по правилу

$$|\psi\rangle \otimes |\chi\rangle = \begin{pmatrix} c_H \\ c_V \end{pmatrix} \otimes \begin{pmatrix} d_H \\ d_V \end{pmatrix} = \begin{pmatrix} c_H d_H \\ c_H d_V \\ c_V d_H \\ c_V d_V \end{pmatrix} \tag{34}$$

и обобщим его на матрицы

$$(A \otimes B)_{ik,jl} = A_{ij} B_{kl}, \tag{35}$$

где ik и jl - мультииндексы.

Если оператор $\hat{A}$ действует только на степени свободы 1 -го фотона (оператор действует в $\mathbb{C}^2$), то в пространстве состояний составной системы этому оператору нужно поставить в соответствие оператор $\hat{A} \otimes \hat{I}$, где $\hat{I}$ - тождественный оператор. Аналогично, если оператор $\hat{B}$ действует только на степени свободы 2 -го фотона, то в пространстве состояний составной системы этому оператору нужно поставить в соответствие оператор $\hat{I} \otimes \hat{B}$.

Математическое свойство

$$(\hat{A} \otimes \hat{B})|\psi\rangle \otimes |\chi\rangle = \hat{A}|\psi\rangle \otimes \hat{B}|\chi\rangle \tag{36}$$

показывает действие локальных операторов $\hat{A} \otimes \hat{B}$ на факторизованные состояния $|\psi\rangle \otimes |\chi\rangle$. С точки зрения физики это соответствует описанию невзаимодействующих подсистем.

Для краткости записи знак тензорного произведения часто опускают, например: $|H\rangle|H\rangle = |H\rangle \otimes |H\rangle$.

Согласно квантово-механическому принципу суперпозиции произвольное чистое двухфотонное поляризационное состояние задаётся вектором

$$|\Psi\rangle = c_1|H\rangle|H\rangle + c_2|H\rangle|V\rangle + c_3|V\rangle|H\rangle + c_4|V\rangle|V\rangle, \tag{37}$$

где $c_i \in \mathbb{C}, \sum_{i=1}^{4} |c_i|^2 = 1$.
В общем случае $|\Psi\rangle \neq |\psi\rangle|\chi\rangle$ ни для каких $|\psi\rangle$ и $|\chi\rangle$. В этом случае говорят, что состояние $|\Psi\rangle$ является перепутанным (также используют термины запутанный, сцепленный, зацепленный). Примером перепутанного состояния является состояние $|\Psi\rangle = \frac{1}{\sqrt{2}}(|H\rangle|V\rangle + |V\rangle|H\rangle)$.

Смешанное двухфотонное поляризационное состояние задаётся матрицей плотности

$$\varrho = \begin{pmatrix} \varrho_{HH,HH} & \varrho_{HH,HV} & \varrho_{HH,VH} & \varrho_{HH,VV} \\ \varrho_{HV,HH} & \varrho_{HV,HV} & \varrho_{HV,VH} & \varrho_{HV,VV} \\ \varrho_{VH,HH} & \varrho_{VH,HV} & \varrho_{VH,VH} & \varrho_{VH,VV} \\ \varrho_{VV,HH} & \varrho_{VV,HV} & \varrho_{VV,VH} & \varrho_{VV,VV} \end{pmatrix}. \tag{38}$$

Оператор плотности первой подсистемы определяется выражением

$$\hat{\varrho}_1 = \sum_i \hat{I} \otimes \langle i| \cdot \hat{\varrho} \cdot \hat{I} \otimes |i\rangle =: \mathrm{tr}_2\, \hat{\varrho} \tag{39}$$

где суммирование ведётся по ортонормированному базису второй подсистемы. Процедура редукции матрицы плотности на подсистему взятие частичного следа по другим подсистемам. Аналогично, оператор плотности второй подсистемы определяется выражением

$$\hat{\varrho}_2 = \sum_i \langle i| \otimes \hat{I} \cdot \hat{\varrho} \cdot |i\rangle \otimes \hat{I} =: \mathrm{tr}_1\, \hat{\varrho} \tag{40}$$

Нетрудно убедиться, что среднее значение $\langle \hat{A} \otimes \hat{I} \rangle = \mathrm{tr}\left(\hat{A}\varrho_1\right)$, а среднее значение $\langle \hat{I} \otimes \hat{B} \rangle = \mathrm{tr}\left(\hat{B}\varrho_2\right)$. Таким образом, среднее значение локального оператора определяется редуцированной матрицей плотности подсистемы.

Смешанное состояние ϱ называют перепутанным, если его невозможно представить в виде выпуклой суммы факторизованных состояний, т.е. $\varrho \neq \sum_i p_i\, |\psi_i\rangle\langle\psi_i| \otimes |\chi_i\rangle\langle\chi_i|$.

Для матриц 4×4 справедлив простой критерий перепутанности: матрица плотности ϱ отвечает перепутанному состоянию тогда и только тогда, когда её частичное транспонирование

$$\varrho^{\Gamma} = \begin{pmatrix} \varrho_{HH,HH} & \varrho_{HV,HH} & \varrho_{HH,VH} & \varrho_{HV,VH} \\ \varrho_{HH,HV} & \varrho_{HV,HV} & \varrho_{HH,VV} & \varrho_{HV,VV} \\ \varrho_{VH,HH} & \varrho_{VV,HH} & \varrho_{VH,VH} & \varrho_{VV,VH} \\ \varrho_{VH,HV} & \varrho_{VV,HV} & \varrho_{VH,VV} & \varrho_{VV,VV} \end{pmatrix} \not\geqslant 0, \tag{41}$$

т.е. ϱ^{Γ} имеет отрицательные собственные значения 10, 11. Геометрические свойства перепутанных матриц плотности рассмотрены в 12 .

Существует несколько способов приготовления перепутанных двухфотонных состояний. Одним из наиболее распространенных является спонтанное параметрическое рассеяние на нелинейных кристаллах с синхронизмом типа II, где два рассеянных фотона в паре всегда поляризованы ортогонально, и принципиально нет никакой возможности различить состояния $|H\rangle|V\rangle$ и $|V\rangle|H\rangle$, т.е. реализуется квантовое состояние $\frac{1}{\sqrt{2}}(|H\rangle|V\rangle + |V\rangle|H\rangle)$ [13.

5.0.12 11. Ultra-Dense Coding

В данном разделе показывается, что квантовая перепутанность является ресурсом для передачи информации. Допустим, что в лабораториях A и B имеются по одному фотону, причём двухфотонное состояние $|\Psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|H\rangle|V\rangle + |V\rangle|H\rangle)$ является перепутанным. Для передачи информации из A в B можно воспользоваться алфавитом из 4 -х элементов ($0, 1, 2, 3$) и следующим кодированием:

для передачи «0» просто переправить фотон из A в B;
для передачи « 1 » повернуть плоскость поляризации фотона в лаборатории A на угол $\pi/2$, затем переправить фотон из A в B;

для передачи « 2 $\gg$ создать сдвиг фаз π между вертикальной и горизонтальной поляризациями фотона в лаборатории A, затем переправить фотон из A в B;

для передачи « 3 $\gg$ в лаборатории A повернуть плоскость поляризации фотона на угол $\pi/2$, создать сдвиг фаз π между вертикальной и горизонтальной поляризациями фотона, затем переправить фотон из A в B.

В результате таких локальных операций и пересылки одного фотона из A в B на приёмном устройстве в лаборатории B окажутся следующие состояния соответственно:

$$|\Psi_+\rangle = \frac{1}{\sqrt{2}}(|H\rangle|V\rangle + |V\rangle|H\rangle), \tag{42}$$

$$|\Phi_+\rangle = \frac{1}{\sqrt{2}}(|V\rangle|V\rangle + |H\rangle|H\rangle), \tag{43}$$

$$|\Psi_-\rangle = \frac{1}{\sqrt{2}}(|H\rangle|V\rangle - |V\rangle|H\rangle), \tag{44}$$

$$|\Phi_-\rangle = \frac{1}{\sqrt{2}}(|H\rangle|H\rangle - |V\rangle|V\rangle). \tag{45}$$

Эти четыре состояния являются взаимно ортогональными и образуют базис Белла в $\mathbb{C}^4$. В силу ортогональности эти состояния однозначно различаются в лаборатории B. Схема однозначного различения поляризационных состояний Белла представлена в работе [14 и изложена в следующем разделе. Таким образом, пересылая один фотон, можно передавать 4 буквы алфавита, т.е. 2 бита информации. Без применения перепутанного состояния при пересылке одного фотона можно передать лишь 1 бит информации (две ортогональные поляризации). Использование перепутанного состояния (между отправителем и приемником) позволяет получить выигрыш в 2 раза, т.е. перепутанные состояния повышают плотность кодирования информации.

5.0.13 12. Measurement in the Bell State Basis

Измерить поляризационное двухфотонное состояние в базисе Белла - реализовать проекторы $|\Phi_\pm\rangle\langle\Phi_\pm|, |\Psi_\pm\rangle\langle\Psi_\pm|$, сумма которых равна I (проекторнозначная мера). Другими словами, необходимо реализовать эксперимент, в котором можно достоверно различить 4 состояния: $|\Phi_+\rangle, |\Phi_-\rangle, |\Psi_+\rangle, |\Psi_-\rangle$. Задача различения этих состояний не является простой с экспериментальной точки зрения, и первоначальные варианты обладали низкой эффективностью [13]. Эффективная схема была предложена в работе [14, схема установки представлена на рис. 14

Входное состояние попадает на делитель пучка с равными коэффициентами прохождения и отражения (BS), действие которого определяется преобразованием $\binom{\hat{a}^\dagger_\uparrow}{\hat{a}^\dagger_\downarrow} \to \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}\binom{\hat{a}^\dagger_\uparrow}{\hat{a}^\dagger_\downarrow}$ для операторов рождения фотонов в верхней (↑) и нижней (↓) частях схемы,

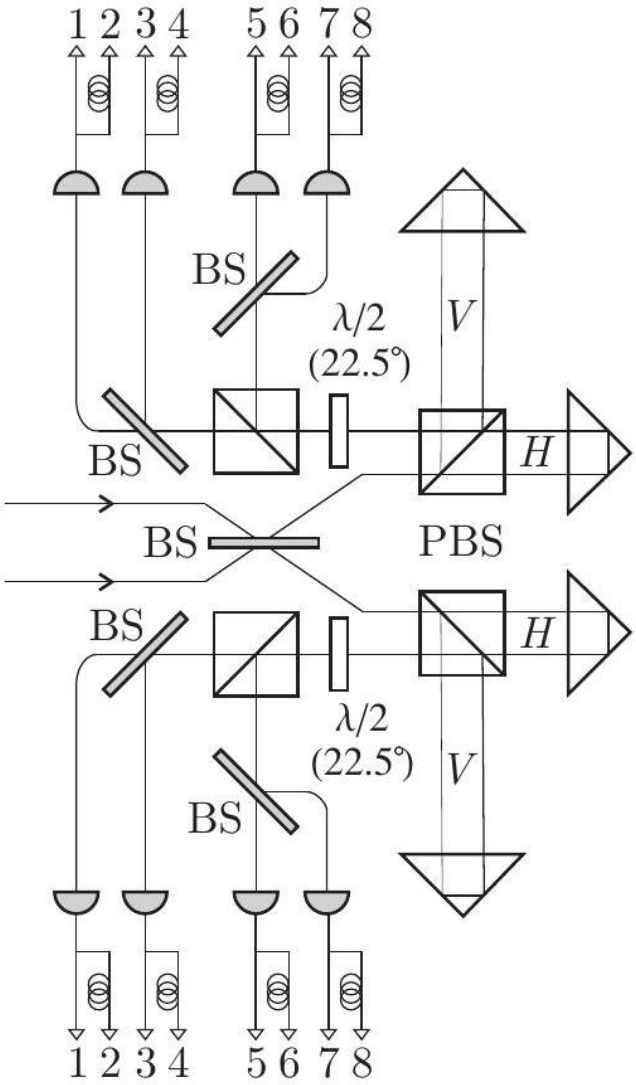


Рис. 14. Схема измерений в базисе поляризационных состояний Белла

в результате чего

$$|H\rangle_\uparrow|H\rangle_\downarrow \to \frac{1}{\sqrt{2}}\left(|H\rangle_\uparrow|H\rangle_\uparrow + |H\rangle_\downarrow|H\rangle_\downarrow\right) \tag{46}$$

$$|H\rangle_\uparrow|V\rangle_\downarrow \to \frac{1}{2}\left(-|H\rangle_\uparrow|V\rangle_\uparrow + |H\rangle_\uparrow|V\rangle_\downarrow - |H\rangle_\downarrow|V\rangle_\uparrow + |H\rangle_\downarrow|H\rangle_\downarrow\right) \tag{47}$$

$$|V\rangle_\uparrow|H\rangle_\downarrow \to \frac{1}{2}\left(-|H\rangle_\uparrow|V\rangle_\uparrow - |H\rangle_\uparrow|V\rangle_\downarrow + |H\rangle_\downarrow|V\rangle_\uparrow + |H\rangle_\downarrow|H\rangle_\downarrow\right) \tag{48}$$

$$|V\rangle_\uparrow|V\rangle_\downarrow \to \frac{1}{\sqrt{2}}\left(|V\rangle_\uparrow|V\rangle_\uparrow + |V\rangle_\downarrow|V\rangle_\downarrow\right) \tag{49}$$

Состояния Белла с точностью до общего фазового множителя преобразуются следующим образом:

$$|\Phi_+\rangle \to \frac{1}{2}\left(|H\rangle_\uparrow|H\rangle_\uparrow + |H\rangle_\downarrow|H\rangle_\downarrow + |V\rangle_\uparrow|V\rangle_\uparrow + |V\rangle_\downarrow|V\rangle_\downarrow\right), \tag{50}$$

$$|\Phi_-\rangle \to \frac{1}{2}\left(|H\rangle_\uparrow|H\rangle_\uparrow + |H\rangle_\downarrow|H\rangle_\downarrow - |V\rangle_\uparrow|V\rangle_\uparrow - |V\rangle_\downarrow|V\rangle_\downarrow\right), \tag{51}$$

$$|\Psi_+\rangle \to \frac{1}{\sqrt{2}}\left(-|H\rangle_\uparrow|V\rangle_\uparrow + |H\rangle_\downarrow|V\rangle_\downarrow\right), \tag{52}$$

$$|\Psi_-\rangle \to \frac{1}{\sqrt{2}}\left(|H\rangle_\uparrow|V\rangle_\downarrow - |H\rangle_\downarrow|V\rangle_\uparrow\right). \tag{53}$$

Из последней формулы видно, что один детектор в верхней части схемы и один детектор в нижней части схемы могут сработать одновременно только для состояния $|\Psi_-\rangle$(критерий детектирования $|\Psi_-\rangle$).

После прохождения через первый поляризационный делитель пучка (PBS) вертикально и горизонтально поляризованные компоненты становятся разнесёнными во времени, появляется дополнительная степень свободы - время f для быстрого фотона, s для медленного.

$$|\Phi_+\rangle \to \frac{1}{2}\left(|H\rangle_{\uparrow f}|H\rangle_{\uparrow f} + |H\rangle_{\downarrow f}|H\rangle_{\downarrow f} + |V\rangle_{\uparrow s}|V\rangle_{\uparrow s} + |V\rangle_{\downarrow s}|V\rangle_{\downarrow s}\right), \tag{54}$$

$$|\Phi_-\rangle \to \frac{1}{2}\left(|H\rangle_{\uparrow f}|H\rangle_{\uparrow f} + |H\rangle_{\downarrow f}|H\rangle_{\downarrow f} - |V\rangle_{\uparrow s}|V\rangle_{\uparrow s} - |V\rangle_{\downarrow s}|V\rangle_{\downarrow s}\right), \tag{55}$$

$$|\Psi_+\rangle \to \frac{1}{\sqrt{2}}\left(-|H\rangle_{\uparrow f}|V\rangle_{\uparrow s} + |H\rangle_{\downarrow f}|V\rangle_{\downarrow s}\right). \tag{56}$$

Видно, что $|\Psi_+\rangle$преобразуется таким образом, что один фотон будет регистрироваться раньше, а другой позже. Экспериментально на схеме рис. 14 будет зафиксировано одно из совпадений событий: 1 и 4 , 1 и 6,1 и 8,3 и 6,3 и 8,5 и 8,2 и 3,2 и 5,2 и 7,4 и 5,4 и 7,6 и 7 (в верхней или нижней части установки).

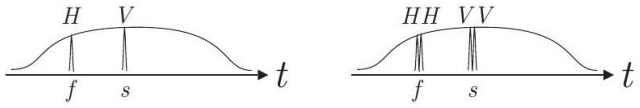


Рис. 15. Слева: состояние $|H\rangle_{f}|V\rangle_{s}=\int f(t)|H\rangle_{t}|V\rangle_{t+s-f}\, dt$. Справа: состояние $\frac{1}{\sqrt{2}}\left(|H\rangle_f|H\rangle_f + |V\rangle_s|V\rangle_s\right) = \frac{1}{\sqrt{2}}\int f(t)\left(|H\rangle_t|H\rangle_t + |V\rangle_{t+s-f}|V\rangle_{t+s-f}\right)dt \approx\approx \frac{1}{\sqrt{2}}\int f(t)\left(|H\rangle_t|H\rangle_t + |V\rangle_t|V\rangle_t\right)dt$

Для различения состояний $|\Phi_+\rangle$и $|\Phi_-\rangle$нужно отметить, что поскольку волновая функция перепутанной пары фотонов имеет характерный разброс по времени создания в пределах времени когерентности импульсного лазера (17 нс), что превышает время $s - f = 3$ нс, то для пары фотонов с волновыми функциями $\frac{1}{\sqrt{2}}\left(|H\rangle_{\uparrow f}|H\rangle_{\uparrow f} \pm |V\rangle_{\uparrow s}|V\rangle_{\uparrow s}\right)$ волновые пакеты $|H\rangle_{\uparrow f}|H\rangle_{\uparrow f}$ и $|V\rangle_{\uparrow s}|V\rangle_{\uparrow s}$ полностью перекрываются, и поэтому задержка не влияет на когерентность (рис. 15). Состояния можно переписать в виде

$$|\Phi_+\rangle \to \frac{1}{2}\left(|/\rangle_\uparrow|/\rangle_\uparrow + |/\rangle_\downarrow|/\rangle_\downarrow + |\backslash\rangle_\uparrow|\backslash\rangle_\uparrow + |\backslash\rangle_\downarrow|\backslash\rangle_\downarrow\right), \tag{57}$$

$$|\Phi_-\rangle \to \frac{1}{2}\left(|/\rangle_\uparrow|\backslash\rangle_\uparrow + |/\rangle_\downarrow|\backslash\rangle_\downarrow + |\backslash\rangle_\uparrow|/\rangle_\uparrow + |\backslash\rangle_\downarrow|/\rangle_\downarrow\right), \tag{58}$$

где $|/\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$ и $|\backslash\rangle =\!\!\rightarrow (|H\rangle - |V\rangle)/\sqrt{2}$. При пропускании света через полуволновую пластинку ($\lambda/2$), повернутую на угол 225°, осуществляется преобразование состояний $|/\rangle \to |H\rangle, |\backslash\rangle \to |V\rangle$, т.е.

$$|\Phi_+\rangle \to \frac{1}{2}\left(|H\rangle_\uparrow|H\rangle_\uparrow + |H\rangle_\downarrow|H\rangle_\downarrow + |V\rangle_\uparrow|V\rangle_\uparrow + |V\rangle_\downarrow|V\rangle_\downarrow\right), \tag{59}$$

$$|\Phi_-\rangle \to \frac{1}{2}\left(|H\rangle_\uparrow|V\rangle_\uparrow + |H\rangle_\downarrow|V\rangle_\downarrow + |V\rangle_\uparrow|H\rangle_\uparrow + |V\rangle_\downarrow|H\rangle_\downarrow\right). \tag{60}$$

После прохождения заключительного поляризационного делителя пучка (PBS) фотоны летят в одном направлении для состояния $|\Phi_+\rangle$ и в разных направлениях для состояния $|\Phi_-\rangle$. Таким образом, одновременные события 1 и 3(2 и 4), 5 и 7(6 и 8) или наблюдение только одного из событий $1, 2, 3, 4, 5, 6, 7, 8$ (в верхней или нижней части установки) означают, что исходное состояние было состоянием $|\Phi_+\rangle$. Одновременные наблюдения событий 1 и 5(2 и 6), 1 и 7(2 и 8), 3 и 5 (4 и 6), 3 и 7 (4 и 8) в верхней или нижней части установки означают, что исходное состояние было состоянием $|\Phi_-\rangle$.

Таким образом, по наблюдению исходов можно однозначно произвести измерение в базисе состояний Белла.

5.0.14 13. Quantum Teleportation

Рассмотрим процедуру передачи неизвестного квантового состояния $|\psi\rangle = c_1|H\rangle + c_2|V\rangle$ с произвольными c_1, c_2 между удалёнными лабораториями (рис. 16). Сразу отметим, что передаётся не материя, а именно квантовое состояние. Другими словами, не происходит передачи энергии. В удалённой лаборатории лишь воссоздаётся квантовое состояние $|\psi\rangle$ в уже имеющемся в этой лаборатории фотоне.

Ресурсом для квантовой телепортации является квантовая перепутанность между лабораториями. Допустим, в лабораториях A и B имеется по одному фотону, которые являются частями двухфотонного состояния $|\Psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|H\rangle_A|V\rangle_B + |V\rangle_A|H\rangle_B)$. Дополнительно в лаборатории имеется состояние $|\psi\rangle_A = c_1|H\rangle + c_2|V\rangle$, которое и требуется воссоздать в лаборатории B. Начальное состояние всей трёхфотонной системы

$$|\psi\rangle_A|\Psi\rangle_{AB} = \frac{1}{\sqrt{2}}\left(c_1|H\rangle|H\rangle|V\rangle + c_2|V\rangle|H\rangle|V\rangle + c_1|H\rangle|V\rangle|H\rangle + c_2|V\rangle|V\rangle|H\rangle\right). \tag{61}$$

К первым двум фотонам, находящимся в лаборатории A, применяют измерение в базисе состояний Белла. Поскольку

$$\begin{aligned}|\psi\rangle_A|\Psi\rangle_{AB} = &|\Phi_+\rangle\left(c_1|V\rangle + c_2|H\rangle\right) + |\Phi_-\rangle\left(c_1|V\rangle - c_2|H\rangle\right) + \\ &+ |\Psi_+\rangle\left(c_1|H\rangle + c_2|V\rangle\right) + |\Psi_-\rangle\left(c_1|H\rangle - c_2|V\rangle\right),\end{aligned} \tag{62}$$

то при наблюдении конкретного исхода ($\Phi_+, \Phi_-, \Psi_+, \Psi_-$) квантовое состояние 3 -го фотона становится определённым: $\Psi_+ \longleftrightarrow c_1|H\rangle + c_2|V\rangle$, $\Phi_+ \longleftrightarrow c_1|V\rangle + c_2|H\rangle, \Psi_- \longleftrightarrow -c_1|H\rangle + c_2|V\rangle, \Phi_- \longleftrightarrow -c_1|V\rangle + c_2|H\rangle$.

Результат измерения в лаборатории A передаётся по классическому каналу связи (телефону) в лабораторию B. В зависимости от полученного сообщения в лаборатории B применяют одну из унитарных операций U, описанных в разделе 5 .

$$\begin{array}{ll}\Psi_+ \longrightarrow I, & c_1|H\rangle + c_2|V\rangle \longrightarrow c_1|H\rangle + c_2|V\rangle,\\ \Phi_+ \longrightarrow \sigma_x, & c_1|V\rangle + c_2|H\rangle \longrightarrow c_1|H\rangle + c_2|V\rangle,\\ \Psi_- \longrightarrow \sigma_z, & -c_1|H\rangle + c_2|V\rangle \longrightarrow c_1|H\rangle + c_2|V\rangle,\\ \Phi_- \longrightarrow i\sigma_y, & -c_1|V\rangle + c_2|H\rangle \longrightarrow c_1|H\rangle + c_2|V\rangle.\end{array}$$

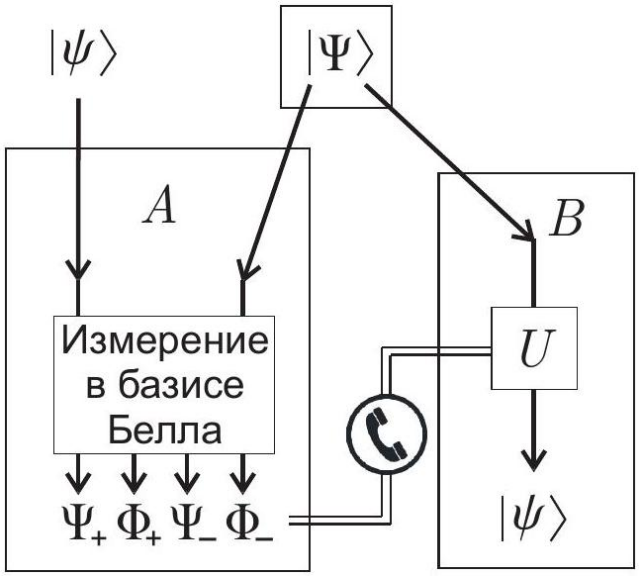


Рис. 16. Схема квантовой телепортации неизвестного состояния $|\psi\rangle$

В итоге состояние 3 -го кубита в любом случае преобразуется к виду $c_1|H\rangle+c_2|V\rangle = |\psi\rangle$, т.е. в лаборатории B осуществляется восстановление произвольного квантового состояния 1 -го кубита, изначально находившегося в A. Протокол «телепортации» напрямую связан с передачей классической информации, поэтому противоречий с теорией относительности нет. Также отметим, что 3 -й фотон не берётся из ниоткуда, он уже представлен в лаборатории B как часть перепутанного состояния.

5.0.15 14. Polarization of an Arbitrary Multiphoton State

Рассмотрим горизонтально поляризованную плоскую электромагнитную волну с заданным волновым вектором $\mathbf{k}$, т.е. фиксированную моду излучения. В предыдущих разделах рассматривались ситуации, когда в одной моде излучения находился один фотон или не находился вовсе. На самом деле фотоны являются бозонами, поэтому в фиксированной моде излучения может находиться $n_H = 0, 1, 2, \ldots$ тождественных фотонов (любое неотрицательное число). Многофотонные квантовые состояния удобно описывать в представлении чисел заполнения, где базисными векторами являются состояния $|n_H\rangle$ с заданным числом фотонов, причём состояния с различным числом частиц ортогональны: $\langle n_H \mid k_H\rangle = \delta_{nk}$. Произвольное многофотонное состояние в фиксированной моде с горизонтальной поляризацией записывается в виде $|\psi\rangle = \sum_n c_n |n_H\rangle \in l_2(Z_+)$. Произвольное состояние в моде с вертикальной поляризацией записывается в виде $|\varphi\rangle = \sum_m c_m |m_V\rangle \in l_2(Z_+)$, где
$|m_V\rangle$ - состояние с m вертикально поляризованными фотонами. Заметим, что $|\psi\rangle$ и $|\varphi\rangle$ - элементы разных пространств. Двухмодовое пространство состояний состоит из векторов

$$|\Psi\rangle = \sum_{n,m} c_{nm} |n_H, m_V\rangle , \tag{63}$$

представляющих собой линейную комбинацию векторов с определённым числом фотонов в каждой из мод, $|\Psi\rangle \in l_2(Z_+ \times Z_+)$. В частном случае однофотонного состояния имеем $c_1|1,0\rangle + c_2|0,1\rangle$, т.е. такое физическое состояние, которое ранее обозначалось $c_1|H\rangle + c_2|V\rangle$. Состояние без фотонов $|0,0\rangle$ называют вакуумным.

Введём оператор уничтожения $\hat{a}_i$ и оператор рождения $\hat{a}_i^\dagger$ фотонов в i-й моде согласно правилу [15]

$$\hat{a}_i \left|\ldots n_i \ldots\right\rangle = \sqrt{n_i}\left|\ldots n_i - 1 \ldots\right\rangle, \tag{64}$$

$$\hat{a}_i^\dagger \left|\ldots n_i \ldots\right\rangle = \sqrt{n_i + 1}\left|\ldots n_i + 1 \ldots\right\rangle. \tag{65}$$

Обобщением введённых ранее операторов Стокса на случай произвольного многофотонного состояния являются эрмитовы операторы

$$\hat{S}_1 = \hat{a}_H \hat{a}_V^\dagger + \hat{a}_H^\dagger \hat{a}_V, \tag{66}$$

$$\hat{S}_2 = i\left(\hat{a}_H \hat{a}_V^\dagger - \hat{a}_H^\dagger \hat{a}_V\right), \tag{67}$$

$$\hat{S}_3 = \hat{a}_H^\dagger \hat{a}_H - \hat{a}_V^\dagger \hat{a}_V. \tag{68}$$

Дополнительно также вводят оператор $\hat{S}_0 = \hat{a}_H^\dagger \hat{a}_H + \hat{a}_V^\dagger \hat{a}_V$, который представляет собой оператор числа фотонов. Заметьте, что сужение оператора $\hat{S}_0$ на подпространство однофотонных состояний $c_1|1,0\rangle + +c_2|0,1\rangle$ есть единичный оператор. Из коммутатора $\left[\hat{a}_\alpha, \hat{a}_\beta^\dagger\right] = \delta_{\alpha\beta}$ следует, что $\left[\hat{S}_\alpha, \hat{S}_\beta\right] = 2i\varepsilon_{\alpha\beta\gamma}\hat{S}_\gamma$, т.е. операторы Стокса удовлетворяют тем же самым коммутационным соотношениям, что и матрицы Паули.

Рассмотрим двухфотонные состояния $|\Psi\rangle = \frac{1}{\sqrt{2}}(|2,0\rangle + |0,2\rangle)$ и $|\Phi\rangle = |1,1\rangle$. Заметим, что $\langle\Psi|\hat{S}_i|\Psi\rangle = \langle\Phi|\hat{S}_i|\Phi\rangle$ для всех $i = 0,1,2,3$, т.е. состояния $|\Psi\rangle$ и $|\Phi\rangle$ невозможно различить в обычных поляризационных экспериментах, рассмотренных ранее! Этот пример показывает, что одним и тем же параметрам Стокса могут отвечать различные многофотонные поляризационные состояния. Заметим, однако, что в рассмотренном примере состояния $|\Psi\rangle$ и $|\Phi\rangle$ ортогональны друг другу, и их можно однозначно различить с помощью другого эксперимента, основанного на интерференции фотонов. Полное восстановление (томография) многофотонных поляризационных состояний рассмотрено в работе [16].

5.0.16 15. Quantum Channels

Рассмотрим взаимодействие квантовой системы с окружением. Начальное состояние системы задаётся оператором плотности ϱ, начальное состояние окружения - оператором плотности ξ. Начальное состояние системы и окружения - оператор плотности $\varrho \otimes \xi$. Гамильтониан системы и окружения $\hat{H} = \hat{H}_{\text{sys}} \otimes \hat{I} + \hat{I} \otimes \hat{H}_{\text{env}} + \hat{H}_{\text{int}}$ состоит из гамильтониана системы $\hat{H}_{\text{sys}}$, гамильтониана окружения $\hat{H}_{\text{env}}$ и гамильтониана взаимодействия системы с окружением $\hat{H}_{\text{int}}$. Для простоты предположим, что $\hat{H}$ не зависит от времени, а система взаимодействует с окружением в течение конечного времени t, тогда оператор эволюции $\hat{U} = \exp\left(-i\hat{H}t/\hbar\right)$. Состояние системы и окружения после взаимодействия есть $\hat{U}(\varrho \otimes \xi)\hat{U}^\dagger$ и является перепутанным в общем случае. Если мы интересуемся только состоянием системы после взаимодействия, то оно получается взятием частичного следа по окружению. В результате реализуется следующее отображение оператора плотности системы:

$$\varrho \longrightarrow \Phi[\varrho] = \text{tr}_{\text{env}}\left[\hat{U}(\varrho \otimes \xi)\hat{U}^\dagger\right] \tag{69}$$

С математической точки зрения Φ - линейное вполне положительное отображение, сохраняющее след (CPT), называемое квантовым каналом 5, 17. Из теоремы

Стайнспринга следует, что для любого CPT-отображения Φ найдутся ξ и $\hat{U}$ такие, что верно (69).

Примером квантового канала является дефазировка. В качестве системы рассмотрим поляризационные степени свободы одиночного фотона, т.е. матрицу плотности $\varrho = \begin{pmatrix} \varrho_{HH} & \varrho_{HV} \\ \varrho_{VH} & \varrho_{VV} \end{pmatrix}$. В качестве окружения рассмотрим пространственные моды электромагнитного поля с частотами ω. Базисные состояния пространственных мод обозначим $|\omega\rangle$, тогда $\langle \omega \mid \omega' \rangle = \delta_{\omega\omega'}$. Начальное состояние системы и окружения - оператор $\varrho \otimes |\chi\rangle\langle\chi|$, где $|\chi\rangle = \int d\omega f(\omega)|\omega\rangle$. Функция $f(\omega)$ - амплитуда вероятности обнаружить фотон в моде с частотой ω, поэтому $\int d\omega |f(\omega)|^2 = 1$. В результате двулучепреломления при прохождении расстояния z в среде между состояниями $|H\rangle$ и $|V\rangle$ возникает набег фаз $\omega\,(n_H - n_V)\,z/c$, где n_H и n_V - показатели преломления для горизонтально и вертикально поляризованных волн. Изменение квантового состояния при распространении фотона в пространстве соответствует эволюции во времени $t = z/c$ с эффективным гамильтонианом

$$\hat{H} = \int d\omega \hbar\omega \left(n_H |H\rangle\langle H| + n_V |V\rangle\langle V|\right) \otimes |\omega\rangle\langle\omega| \tag{70}$$

Подставляя оператор эволюции

$$\hat{U} = \int d\omega \left[\exp\left(-i n_H \omega t\right) |H\rangle\langle H| + \exp\left(-i n_V \omega t\right) |V\rangle\langle V|\right] \otimes |\omega\rangle\langle\omega| \tag{71}$$

в уравнение (69), получаем

$$\Phi[\varrho] = \begin{pmatrix} \varrho_{HH} & G^*(t)\varrho_{HV} \\ G(t)\varrho_{VH} & \varrho_{VV} \end{pmatrix}, \tag{72}$$

где $G(t) = \int d\omega |f(\omega)|^2 e^{i(n_H - n_V)\omega t}$ - функция декогеренции. Заметим, что $G(t) \to 0$ при $t \to \infty$, поэтому на больших временах матрица плотности становится диагональной, т.е. происходит дефазировка. Действие канала (72) сводится к сжатию сферы Пуанкаре вдоль направлений s_x и s_y с коэффициентом $|G(t)|$ и повороту вокруг оси s_z на угол $\arg G(t)$.

Отметим важный случай деполяризующего канала, реализующегося для поляризационных степеней свободы в многомодовом волокне вследствие перекачки энергии между модами с разными поляризациями 18 :

$$\Phi[\varrho] = q\varrho + \mathrm{tr}[\varrho]\frac{1}{2}I \tag{73}$$

где $q \in [0, 1]$ - параметр деполяризации. Действие канала (73) сводится к сжатию сферы Пуанкаре во всех направлениях с коэффициентом q. Действие дефазирующих и деполяризующих локальных каналов вида $\Phi \otimes \Phi$ на перепутанные состояния изучено в работе 19 .

6 Lectures on Mathematical Fundamentals of QM by Amosov

Introduction

Квантовой механике посвящено обширное количество учебников и монографий. Тем не менее они часто построены по принципу или изложению: физика для физиков или математика для математиков.

Доказательство А.С.Холево и независимо Б. Шумахером и М. Вестморелендом квантовой теоремы кодирования в 1996 г. привело к бурному развитию новой дисциплины - квантовой теории вероятностей, требующей особого синтетического взгляда, неразрывно связывающего математику и физику.

Прекрасные книги А.С.Холево, вышедшие и переизданные в последние годы, конечно, заслужили всеобщее признание среди профессионалов, занимающихся квантовой теорией вероятностей. Между тем в них были опущены некоторые важные части теории, касающиеся, например, действия преобразования Фурье на канонические наблюдаемые, квантовой томографии и квантовых случайных процессов в пространстве Фока.

В предлагаемых лекциях, тоже не претендующих на полноту, восполнены эти пробелы. Изложение построено, начиная с азов теории, восходящей к пионерским работам Дж. фон Неймана.

Автор выражает благодарность Ивану Сергееву, студенту ФОПФ МФТИ, за составление электронного конспекта, который лег в основу этой книги.

List of Designations

$\mathfrak{A}$ - множество наблюдаемых
$\mathfrak{S}$ - множество состояний
P_A^ρ - распределение вероятностей на прямой, отвечающее $A \in \mathfrak{A}, \rho \in \mathfrak{S}$
$\mathcal{B}(\mathbb{R})$ - алгебра борелевских множеств на прямой
q, p - наблюдаемые координаты и импульса
$\langle\psi|, |\psi\rangle$ - векторы бра и кет
$\langle\cdot,\cdot\rangle$ - скалярное произведение в контексте квантовой механики
$(\cdot,\cdot)$ - скалярное произведение в абстрактном гильбертовом пространстве
$\mathcal{D}(A)$ - область определения оператора A
$\mathrm{Spect}(A)$ - спектр оператора A
$\|f\|_\infty = \sup_x |f(x)|$ - равномерная норма функции f
$\|A\|$ - спектральная норма оператора A
$\mathrm{span}\,(X_j)$ - линейная оболочка элементов X_j
$F(H)$ - симметричное (бозонное) пространство Фока над одночастичным сепарабельным гильбертовым пространством H

6.1 A.1

6.1.1 1.1. Mackey 's Axioms

Знаменитый американский математик Джордж Макки прочитал в 1960 году в Гарвардском университете курс лекций по математическим основаниям квантовой механики. Эти лекции были изданы на английском языке в 1963 году, а в скором времени переведены и на русский язык 7. В книге Макки были впервые математически точно сформулированы аксиомы квантовой механики.

Имеется два множества: $\mathfrak{A}$, элементы которого называются наблюдаемыми, и $\mathfrak{S}$ - множество состояний. Для любой наблюдаемой $A \in \mathfrak{A}$ и для любого состояния $\rho \in \mathfrak{S}$ на алгебре борелевских подмножеств вещественной прямой $\mathcal{B}(\mathbb{R})$ определена функция $P_A^\rho : \mathcal{B}(\mathbb{R}) \to [0,1]$, обладающая следующими свойствами:

1. $P_A^\rho(\emptyset) = 0$;
2. $P_A^\rho(\mathbb{R}) = 1$;
3. $P_A^\rho\left(\bigcup_k B_k\right) = \sum_k P_A^\rho\left(B_k\right)$, если множества $B_j \cap B_k = \emptyset$ для любых $j \neq k$.

Величина $P_A^\rho(B)$ равна вероятности того, что наблюдаемая A примет значение из множества B , если состояние системы ρ.

Аксиома 1.1. 1) Если $P_A^\rho(B) = P_{\tilde{A}}^\rho(B)$, тогда $A = \tilde{A}$.

2) Если $P_A^\rho(B) = P_A^{\tilde{\rho}}(B)$ для всех $B \in \mathcal{B}(\mathbb{R})$ и всех $A \in \mathfrak{A}$, тогда $\rho = \tilde{\rho}$.

Аксиома 1.2. Пусть $A \in \mathfrak{A}, f : \mathbb{R} \to \mathbb{R}$ - борелевская функция, то есть $f^{-1}(B) \in \mathcal{B}(\mathbb{R}) \forall B \in \mathcal{B}(\mathbb{R})$. Тогда существует единственная наблюдаемая $A^f \in \mathfrak{A}$ такая, что $P_{A^f}^\rho(B) = P_A^\rho\left(f^{-1}(B)\right)$. Эту наблюдаемую будем обозначать $f(A)$.

Аксиома 1.3. Пусть $\rho_k \in \mathfrak{S}$ - набор состояний, $\pi_k \geq 0 : \sum_k \pi_k = 1$ дискретное распределение вероятностей. Тогда $\bar{\rho} = \sum_k \pi_k \rho_k \in \mathfrak{S}$, при этом $\forall B \in \mathcal{B}(\mathbb{R})$ вероятность $P_A^{\bar{\rho}}(B) = \sum_k \pi_k P_A^{\rho_k}(B)$. состояние $\bar{\rho}$ называется смесъю или смешанным состоянием.

Замечание 1.1 (к аксиоме 1.2). Если понимать наблюдаемые как измерения, то п. 2) аксиомы 1.1 можно переформулировать следующим образом: если все измерения для двух состояний совпадают, то эти состояния совпадают.

Замечание 1.2. В связи с аксиомой 1.2 возникают вопросы о существовании полного набора измерений и полного набора состояний. В качестве примера полного набора наблюдаемых (измерений) можно привести линейные комбинации операторов координаты и импульса, а также операторов проекции спина на всевозможные направления. Такой тематикой занимается квантовая томография [33]. Примером полного набора состояний служат когерентные состояния, широко применяющиеся в квантовой оптике, возникшей благодаря пионерским работам 30,45 .

Определение 1.1. Пусть $A \in \mathfrak{A}, f : \mathbb{R} \to \mathbb{R}$ - борелевская функция. Тогда среднее значение функции от наблюдаемой определяется по формуле

$$\langle f(A) \rangle_\rho = \int_{\mathbb{R}} f(x) dP_A^\rho(x)$$

где интегрирование ведётся по вероятностной мере P_A^ρ.

Нашей ближайшей задачей будет поиск конкретных множеств $\mathfrak{A}$ и $\mathfrak{S}$, для которых выполняются аксиомы Макки.

6.1.2 1.2. Schrodinger and Heisenberg's Approaches to Quantum Mechanics

1.2.1. Волновая механика (Шрёдингер)

Будем считать, что состояния представляют собой единичные векторы ψ гильбертова пространства $H = L^2(\mathbb{R})$.

Определим стандартные наблюдаемые - координату и импульс:

$$q : (q\psi)(x) = x\psi(x)$$
$$p : (p\psi)(x) = -i\psi'(x)$$

где функции $\psi \in S(\mathbb{R})$ принадлежат всюду плотному в H пространству Шварца $S(\mathbb{R})$, на котором корректно заданы всевозможные полиномы от q и p. Функция $\psi(x) \equiv < x, \psi >$ называется волновой функцией состояния ψ в координатном представлении.

Замечание 1.3. В квантовой механике в качестве наблюдаемых обычно используются линейные самосопряженные операторы A, для которых определены функции $f(A)$, где f как минимум может быть любым полиномом от A, так что считается, что пересечение областей

определения всех степеней $A^n, n = 1, 2, 3, \ldots$, плотно в H. Операторы координаты и импульса представляют собой канонический пример наблюдаемых, обладающих таким свойством.

По формуле Борна квадрат модуля волновой функции $|\psi(x)|^2$ представляет собой плотность распределения вероятностей наблюдаемой q в состоянии $\psi \in H$, то есть в обозначениях Макки:

$$P_q^{\psi}(B) = \int_B |\psi(x)|^2 dx \tag{1.1}$$

Следовательно, среднее значение от координаты

$$\langle f(q) \rangle_{\psi} = \int_{\mathbb{R}} f(x)|\psi(x)|^2 dx \tag{1.2}$$

Если использовать импульсное представление волновой функции

$$\psi(p) = \frac{1}{\sqrt{2\pi}} \int_{\mathbb{R}} e^{ipx} \psi(x) dx \tag{1.3}$$

тогда

$$\langle f(p) \rangle_{\psi} = \int_{\mathbb{R}} f(p)|\psi(p)|^2 dp \tag{1.4}$$

$$P_p^{\psi}(B) = \int_B |\psi(p)|^2 dp \tag{1.5}$$

Вопрос 1.1 (В. Паули [41). Однозначно ли плотности распределения вероятностей волновой функции в координатном и импульсном представлениях $|\psi(x)|^2 u|\psi(p)|^2$ задают волновую функцию ψ ?

Утверждение. Можно привести конкретные примеры, из которых следует отрицательный ответ на вопрос Паули. Волновая функция представляется в виде

$$\psi(x) = |\psi(x)|e^{i\alpha(x)} \tag{1.6}$$

Функция $\alpha(x)$ называется фазой волновой функи, Фаза волновой функции может быть выбрана произвольно, поэтому сама волновая функция не восстанавливается однозначно по плотностям вероятности.

Замечание 1.4. В представлении квантовой механики Вигнера-Мойала интегрирование ведётся по двум переменным:

$$\langle f(q,p) \rangle_{\rho} = \iint W(q,p) f(q,p) dq dp \tag{1.7}$$

Функция $W(q,p)$ называется функцией Вигнера [47]. При этом $f(q) == f(q)$, если у функции Вигнера отсутствует зависимость от p, и $f(p) = f(p)$, если отсутствует зависимость от q. Мойал показал [39, что произвольная наблюдаемая задается некоторой функцией от координаты и импульса: $f = f(q,p)$, которую естественно назвать *си* волом наблюдаемой.

1.2.2. Матричная механика (Гейзенберг)

Будем считать, что наблюдаемыми являются линейные самосопряженные операторы в гильбертовом пространстве.

Пусть H - гильбертово пространство. Обозначим $\langle \cdot, \cdot \rangle : H \times H \to \mathbb{C}$ скалярное произведение в H, то есть антилинейную по первому и линейную по второму аргументу функцию такую, что для любых $f, g, h \in H$ и $\alpha, \beta \in \mathbb{C}$ выполнены следующие равенства:

$$\langle \alpha f + \beta g, h\rangle = \bar{\alpha}\langle f, g\rangle + \bar{\beta}\langle g, h\rangle, \tag{1.8}$$

$$\overline{\langle f, g\rangle} = \langle g, f\rangle. \tag{1.9}$$

Определение 1.2. Пусть $A : H \to H, A^* : H \to H$ - некоторые операторы в H с областями определения $\mathcal{D}(A)$ и $\mathcal{D}(A^*)$ соответственно.

Оператор A^* называется сопряженным κ оператору A, если $\forall f \in\in \mathcal{D}(A) \forall g \in \mathcal{D}(A^*)$ выполнено $\langle Af, g\rangle = \langle f, A^* g\rangle$.

Оператор A называется симметричным, если $\forall f, g \in \mathcal{D}(A)$, выполнено $\langle Af, g\rangle = \langle f, Ag\rangle$

Оператор A называется самосопряженным, если A симметричный, и $\mathcal{D}(A) = \mathcal{D}(A^*)$.

Замечание 1.5. Все ограниченные симметричные операторы автоматически являются самосопряженными.

Пример 1.1. Пусть оператор A определен по формуле $(Af)(x) == -if'(x)$, и его область определения $\mathcal{D}(A) = \{f \mid f' \in L^2(\mathbb{R}_+),\ f(0) = 0\}$. Тогда сопряженный к нему оператор A^* задается формулой $(A^* f)(x) = -if'(x)$, причем его область определения $\mathcal{D}(A^*) == \{f \mid f' \in L^2(\mathbb{R}_+)\} \supsetneq \mathcal{D}(A)$. Следовательно, A - симметричный, но не самосопряженный оператор.

Пусть $\{e_n\}$ - ортонормированный базис в H. Любому оператору A в этом базисе можно сопоставить матрицу $a_{nm} = \langle e_n, Ae_m\rangle$. Предположим, что оператор A является самосопряженным, тогда его матрица будет эрмитовой $a_{nm} = \overline{a_{mn}}$. В конечномерном случае все эрмитовы матрицы имеют полный набор ортогональных собственных векторов (число векторов равно размерности пространства). Пусть у матрицы (a_{nm}), подобно конечномерному случаю, существует базис из собственных векторов. Обозначим собственные значения: $\lambda_n \in \mathbb{R}$ и нормированные собственные векторы: $f_n \in H$. Любой вектор $f \in H$ можно разложить по базису: $f_n : f = \sum_n c_n f_n$. Тогда

$$\langle A\rangle_f = \langle f, Af\rangle = \sum_n \lambda_n |c_n|^2 \tag{1.10}$$

По аналогии для функции

$$\langle F(A)\rangle_f = \sum_n F(\lambda_n) |c_n|^2. \tag{1.11}$$

Введём дискретное распределение вероятностей:

$$P_A^f(\{n\}) = |c_n|^2. \tag{1.12}$$

Тогда выражение для среднего значения A в состоянии f можно записать в виде

$$\langle F(A)\rangle_f = \sum_n F(\lambda_n) P_A^f(\{n\}). \tag{1.13}$$

6.2 A.2

6.2.1 2.1. The Relationship Between Schrodinger's and Heisenberg's Approaches

Наша цель - связать подходы Шрёдингера и Гейзенберга. Для этого мы должны построить пространство наблюдаемых $\mathfrak{A}$, пространство состояний $\mathfrak{S}$ и функцию $0 \leq P_A^\rho(B) \leq 1 \forall B \in \mathcal{B}(\mathbb{R})$ для всех $A \in \mathfrak{A}$, $\rho \in \mathfrak{S}$. Мы взяли самосопряжённые операторы $A = A^*$ в качестве наблюдаемых и единичные векторы гильбертова пространства $\psi \in H$

: $\|\psi\| = 1$ в качестве состояний. В аксиоме 1.3 Макки используются выпуклые линейные комбинации состояний, поэтому брать только единичные векторы в качестве состояний недостаточно.

Введём обозначения Дирака.

Определение 2.1. Пусть $\psi, \varphi \in H$. Тогда $|\psi\rangle\langle\varphi| f = \langle\varphi, f\rangle\psi$, где $f \in H$. В дальнейшем будем называть $|\psi\rangle\langle\varphi|$ операторами ранга один.

Следствие 2.1. $|\psi\rangle\langle\psi|$ - проектор на линейную оболочку, натянутую на вектор $\psi, \|\psi\| = 1$.

Потребуем, чтобы в число состояний входили проекторы $|\psi\rangle\langle\psi|$. Тогда из аксиомы 1.3 следует, что пространство состояний $\mathfrak{S}$ состоит из проекторов и их выпуклых комбинаций вида $\sum_j \pi_j |\psi_j\rangle \langle\psi_j|$, где $\pi_j \geq\geq 0, \sum_j \pi_j = 1$.

Таким образом, определены множества $\mathfrak{A}$ и $\mathfrak{S}$. Осталось определить вероятностную меру.

6.2.2 2.2. Functional Calculus for Self-Adjoint Operators

Пусть A - линейный (вообще говоря, неограниченный) оператор в гильбертовом пространстве H. Будем считать, что пересечение областей определения всех степеней A^n образует плотное множество в H. Нашей целью является определение функций от оператора A.

Определение 2.2. Пусть $A : H \to H$ - оператор и $P(x) = a_n x^n + + \cdots + a_0$ - полином. Тогда $P(A) = a_n A^n + \cdots + a_0$.

Замечание 2.1. Если A - ограниченный оператор, тогда и $P(A)-$ ограниченный оператор, причем можно показать, что $\|f(A)\| \leq \|f\|_\infty$. $\|A\|$, где $\|f\|_\infty = \sup_x |f(x)|$ - равномерная норма.

Определение 2.3. Говорят, что число $\lambda \in \mathbb{C}$ принадлежит спектру оператора $\lambda \in \operatorname{Spect} A$, если $\nexists (A - \lambda I)^{-1}$. Обратный оператор $(A - \lambda I)^{-1}$ существует, если уравнение $(A - \lambda I) f = g$ имеет единственное решение $f \in H$ для любой правой части $g \in H$, и не существует в обратном случае.

Замечание 2.2. В следствие теоремы Лиувилля $\operatorname{Spect} A \neq \emptyset$.

Теорема 2.1 (о полиномиальном отображении спектра). Пусть A - самосопряженный оператор. В этом случае, $\lambda \in \operatorname{Spect} A$ тогда и только тогда, когда $P(\lambda) \in \operatorname{Spect}(P(A))$.

Доказательство. Пусть $\lambda \in \operatorname{Spect} A$. Рассмотрим многочлен $F(x) == P(x) - P(\lambda)$. Заметим: $F(\lambda) = P(\lambda) - P(\lambda) = 0$, то есть $x = \lambda$ - корень многочлена $F(x)$. По теореме Безу существует многочлен $Q(x)$ такой, что $F(x) = P(x) - P(\lambda) = (x - \lambda)Q(x)$. Следовательно, оператор $F(A)$ можно представить в виде: $F(A) = P(A) - P(\lambda)I == (A - \lambda I)Q(A)$. По условию $\lambda \in \operatorname{Spect} A$, то есть $\nexists (A - \lambda I)^{-1}$. Следовательно, $\nexists (P(A) - P(\lambda)I)^{-1}$, то есть $P(\lambda) \in \operatorname{Spect}(P(A))$. Таким образом, мы доказали, что из $\lambda \in \operatorname{Spect} A$ следует $P(\lambda) \in \operatorname{Spect}(P(A))$.

Пусть $\mu \in \operatorname{Spect}(P(A))$. Рассмотрим многочлен $F(x) = P(x) - -\mu$. Разложим его на множители: $F(x) = P(x) - \mu = a \cdot \prod_j (x - \lambda_j)$. Следовательно, $F(A) = P(A) - \mu I = a \cdot \prod_j (A - \lambda_j I)$. По условию $\mu \in\in \operatorname{Spect}(P(A))$, то есть $\nexists (P(A) - \mu I)^{-1}$. Таким образом, $\nexists (A - \lambda_{j_0} I^{-1})$, то есть $\lambda_{j_0} \in \operatorname{Spect} A$ для некоторого номера j_0. Заметим $F(\lambda_{j_0}) == P(\lambda_{j_0}) - \mu = 0$. Следовательно, $\mu = P(\lambda_{j_0})$ для $\lambda_{j_0} \in \operatorname{Spect} A$. Таким образом, мы доказали, что из $\mu \in \operatorname{Spect}(P(A))$ следует $\mu = P(\lambda_{j_0})$, где $\lambda_{j_0} \in \operatorname{Spect} A$.

Определение 2.4. Спектральным радиусом ограниченного оператора A называется $r(A) = \sup_{\lambda \in \operatorname{Spect} A} |\lambda|$.

Пример 2.1. Пусть $H = L^2$ ([0,1]). Рассмотрим оператор A, определенный по формуле

$$(Af)(x) = \int_0^x f(t)dt \tag{2.1}$$

Оператор A называется оператором Вольтерры. Найдём спектр оператора Вольтерры: Spect A. Рассмотрим уравнение $(A-\lambda I)f=g$ относительно $f\in H$, где $g\in H$:

$$\int_0^x f(t)dt-\lambda f(x)=g(x) \tag{2.2}$$

Положив $x=0$ в 2.2 , имеем $-\lambda f(0)=g(0)$. Будем считать, что f и g - дифференцируемые функции. В результате дифференцирования (2.2) получим

$$f(x)-\lambda f'(x)=g'(x) \tag{2.3}$$

Решим дифференциальное уравнение (2.3) методом вариации постоянной. Решение однородного уравнения $f(x)-\lambda f'(x)=0$ - семейство функций вида $f(x)=C\cdot\exp\left(\frac{x}{\lambda}\right)$, где $C=\text{const}$. Подставим $f(x)=C(x)\cdot\exp\left(\frac{x}{\lambda}\right)$ в 2.3:

$$-\lambda\exp\left(\frac{x}{\lambda}\right)C'(x)=g'(x) \tag{2.4}$$

Решим полученное дифференциальное уравнение относительно $C(x)$:

$$C(x)=C(0)-\frac{1}{\lambda}\int_0^x\exp\left(-\frac{t}{\lambda}\right)g'(t)dt \tag{2.5}$$

Проинтегрировав по частям, получим

$$C(x)=C(0)-\frac{1}{\lambda}\left[\exp\left(-\frac{x}{\lambda}\right)g(x)-g(0)\right]-\frac{1}{\lambda^2}\int_0^x\exp\left(-\frac{t}{\lambda}\right)g(t)dt \tag{2.6}$$

Используя $-\lambda f(0)=g(0)$ и $f(x)=C(x)\cdot\exp\left(\frac{x}{\lambda}\right)$, найдём $C(0)==-\frac{1}{\lambda}g(0)$. Следовательно,

$$C(x)=-\frac{1}{\lambda}\exp\left(-\frac{x}{\lambda}\right)g(x)-\frac{1}{\lambda^2}\int_0^x\exp\left(-\frac{t}{\lambda}\right)g(t)dt \tag{2.7}$$

Таким образом, для всех $\lambda\neq 0$ мы доказали $\exists(A-\lambda I)^{-1}$. Следовательно, Spect $A=\{0\}$.

Оператор Вольтерры не является самосопряженным, сопряженный к нему оператор имеет вид

$$\left(A^*f\right)(x)=\int_x^1 f(t)dt \tag{2.8}$$

Теорема 2.2 (теорема о спектральном радиусе). Пусть $A=A^*$. Тогда $\|A\|=r(A)$.

Доказательство. Используем ряд Неймана:

$$(A-\lambda I)^{-1}=-\frac{1}{\lambda}\left(I-\frac{A}{\lambda}\right)^{-1}=-\frac{1}{\lambda}\sum_{n=0}^{\infty}\left(\frac{A}{\lambda}\right)^n. \tag{2.9}$$

Этот ряд сходится и $\exists(A-\lambda I)^{-1}$ тогда и только тогда, когда $|\lambda|>>\|A\|$. Следовательно, $r(A)\leq\|A\|$.

Заметим, что если $A\psi\neq 0$, то выполнено неравенство

$$\left|\left(A\psi,\frac{A\psi}{\|A\psi\|}\right)\right|=\frac{|(A\psi,A\psi)|}{\|A\psi\|}=\frac{\|A\psi\|^2}{\|A\psi\|}=\|A\psi\| \tag{2.10}$$

Следовательно,

$$\sup_{\|\varphi\|=1} |(A\psi,\varphi)| \geq \left|\left(A\psi, \frac{A\psi}{\|A\psi\|}\right)\right| = \|A\psi\| \tag{2.11}$$

Таким образом,

$$\|A\| = \sup_{\|\psi\|=1} \|A\psi\| \leq \sup_{\|\psi\|=\|\varphi\|=1} |(A\psi,\varphi)| \tag{2.12}$$

Заметим, что

$$\begin{gathered}(A(\psi+\varphi),\psi+\varphi) - (A(\psi-\varphi),\psi-\varphi) = \\ = (A\psi,\psi) + (A\psi,\varphi) + (A\varphi,\psi) + (A\varphi,\varphi) - \\ -[(A\psi,\psi) - (A\psi,\varphi) - (A\varphi,\psi) + (A\varphi,\varphi)] = \\ = 2(A\psi,\varphi) + 2(A\psi,\varphi) = 4(A\psi,\varphi)\end{gathered}$$

Пусть $\xi = \psi \pm \varphi \neq 0$, где $\|\psi\| = \|\varphi\| = 1$, тогда
$0 < \|\xi\|^2 = (\psi \pm \varphi, \psi \pm \varphi) = \|\psi\|^2 + \|\varphi\|^2 \pm 2\,\mathrm{Re}[(\psi,\varphi)] = 2 \pm 2\,\mathrm{Re}[(\psi,\varphi)]$.

Следовательно,

$$|(A\xi,\xi)| = \|\xi\|^2 \left|\left(A\frac{\xi}{\|\xi\|}, \frac{\xi}{\|\xi\|}\right)\right| \leq (2 \pm 2\,\mathrm{Re}[(\psi,\varphi)]) \left|\left(A\frac{\xi}{\|\xi\|}, \frac{\xi}{\|\xi\|}\right)\right| \tag{2.14}$$

Для $\xi = 0$ имеем $(A\xi,\xi) = 0$, следовательно, неравенство верно для всех $\xi \in H$. Следовательно,

$$\begin{aligned}|(A\psi,\varphi)| &= \frac{1}{4}|(A(\psi+\varphi),\psi+\varphi) - (A(\psi-\varphi),\psi-\varphi)| \leq \\ &\leq \frac{1}{4}[|(A(\psi+\varphi),\psi+\varphi)| + |(A(\psi-\varphi),\psi-\varphi)|] \leq \\ &\leq \frac{1}{2}\left[\left|\left(A\frac{\psi+\varphi}{\|\psi+\varphi\|}, \frac{\psi+\varphi}{\|\psi+\varphi\|}\right)\right| + \left|\left(A\frac{\psi-\varphi}{\|\psi-\varphi\|}, \frac{\psi-\varphi}{\|\psi-\varphi\|}\right)\right|\right].\end{aligned}$$

Таким образом,

$$\|A\| \leq \sup_{\|\psi\|=\|\varphi\|=1} |(A\psi,\varphi)| \leq \sup_{\|\eta\|=1} |(A\eta,\eta)| = r(A) \tag{2.15}$$

Откуда вытекает $\|A\| \leq r(A) \leq \|A\|$, то есть $\|A\| = r(A)$.
Из теорем 2.1 и 2.2 немедленно следует

Следствие 2.2.

$$\|P(A)\| = \sup_{\lambda\in\mathrm{Spect}(P(A))} |\lambda| = \sup_{\lambda\in\mathrm{Spect}\,A} |P(\lambda)| = \|P\|_\infty \tag{2.16}$$

Договоримся отождествлять функции f и g, если они совпадают на спектре, то есть $\|f-g\|_\infty = 0$.
Утверждение 2.1. Пусть ψ_0 - единичный циклический вектор для самосопряжённого оператора A, то есть $\|\psi_0\| = 1$, и векторы $A^n\psi_0$, $n = 0,1,2,\ldots$, порождают H. Тогда оператор A изоморфен оператору умножения на координату в некотором гильбертовом пространстве $H = L^2(\mu)$ с мерой μ.
Замечание 2.3. Для наблюдаемой координаты $A = q$ циклическим вектором является $\psi_0(x) = \frac{1}{\pi^{1/4}} \exp\left(-\frac{x^2}{2}\right)$ - волновая функция основного состояния квантового осциллятора.

Поскольку множество всех полиномов плотно в пространстве непрерывных функций $C(K)$ на любом компактном множестве K, из следствия 2.2 немедленно вытекает, что функция $f(A)$ определена для любого $f \in C(K)$ и компактного множества $K \subset \mathrm{Spect}(A)$. Рассмотрим $f \in C_c(\mathrm{Spect}\, A)$ и определим функционал

$$\ell_A^{\psi_0}(f) = (\psi_0, f(A)\psi_0) \tag{2.17}$$

Здесь и ниже мы обозначаем $C_c(X)$ пространство непрерывных функций с компактным носителем на пространстве X. Это положительный

функционал, то есть для любой неотрицательной функции $f \geq 0$ значение функционала $\ell_A^{\psi_0}(f) \geq 0$. Заметим, что $\left|\ell_A^{\psi_0}(f)\right| \leq \|f(A)\| \leq\leq \|f\|_\infty \cdot \|A\|$, то есть $\ell_A^{\psi_0}(f)$ - непрерывный функционал. Пространство X называется хаусдорфовым, если любые его две точки обладают непересекающимися окрестностями. Спектр $\mathrm{Spect}(A)$ является примером локально компактного хаусдорфова пространства, следовательно для него применима следующая теорема.

Теорема 2.3 (Рисс-Марков-Какутани [10, 42]). Любой положительный функционал на пространстве $C_c(X)$ представляется в виде

$$\ell_A^{\psi}(f) = \int_X f(x) d\mu_A^{\psi}(x) \tag{2.18}$$

где μ_A^{ψ} - некоторая мера, нормированная условием $\mu(X) = 1$.

Для случая $X = \mathrm{Spect}(A)$ теорему Рисса-Маркова-Какутани можно использовать для определения непрерывных функций от оператора A. Рассмотрим сначала случай, когда вектор ψ_0 циклический для оператора A, то есть замыкание линейной оболочки векторов $A^n\psi_0$ совпадает со всем пространством.

Теорема 2.4 (спектральная теорема). Пусть самосопряженный оператор A обладает циклическим вектором ψ_0. Тогда оператор $U : H \to\to L^2(\mu)$, заданный формулой

$$U\psi_0 = 1, \left(UA^n\psi_0\right)(x) = x^n, n = 1, 2, 3, \ldots$$

является унитарным, причём

$$UAU^* = M_x$$

где M_x - оператор умножения на x в пространстве $L^2(\mu)$.

Замечание 2.4. Мы будем называть M_x представлением оператора A в $L^2(\mu)$. Функцию $\psi_A(x) = (U\psi)(x)$ будем называть волновой функцией состояния ψ в представлении, связанном с наблюдаемой A.

Доказательство. Заметим, что

$$(UA^n\psi_0, A^m\psi_0)_{L_2(\mu)} = \int_{Spect(A)} x^{n+m} d\mu(x) = \left(\psi_0, A^{n+m}\psi_0\right)$$

и

$$(x^n, UAU^*x^m)_{L^2(\mu)} = (A^n\psi_0, AA^m\psi_0)$$

Определение 2.5. Унитарный оператор U переводит любое чистое состояние $\psi \in H$ в функцию $\psi_A(x) = (U\psi)(x), x \in \mathrm{Spect}(A)$ в пространстве $L^2(\mu)$. Функция ψ_A называется волновой функцией состояния ψ в пространстве $L^2(\mu)$, ассоциированном с наблюдаемой A.

Следствие 2.3. Для любой функции $f \in L^\infty(\mathrm{Spect}(A))$ определена функиия $f(A)$, причём выполнено неравенство

$$\|f(A)\| \leq \|f\|_\infty \|A\|.$$

Доказательство. Для начала предположим, что пространство H сепарабельное. Если $\psi_0 \in H$ не является циклическим вектором, то замыкание $H_0 \subset H$ линейной оболочки $A^n\psi_0$ является гильбертовым подпространством и $H = H_0 \oplus H_1$, причём ψ_0 является циклическим вектором для сужения $A|_{H_0}$. Аналогично для $\psi_1 \in H$ замыкание $H_2 \subset H_1$ линейной оболочки $A^n\psi_1$ определяет сужение $A|_{H_2}$, для которого ψ_1 является циклическим вектором. Повторяя процесс по индукции получаем разложение $H = \bigoplus_{n=0}^{\infty} H_{2n}$ для которого любое сужение $A|_{H_{2n}}$ обладает циклическим вектором. В случае несепарабельного гильбертова пространства H нужно использовать аксиому выбора.

В силу теоремы 2.4 любое сужение $A|_{H_{2n}} \equiv A_n = U^* M_x U$. Определим оператор $f(A_n)$ по формуле

$$f(A_n) = U^* f(M_x) U \tag{2.19}$$

где

$$(f(M_x)\xi)(x) = f(x)\xi(x) \tag{2.20}$$

$\xi \in L^2(\mu)$. Для всего оператора A положим

$$f(A) = \oplus_n f(A_n)$$

Из 2.19 и 2.20 немедленно вытекает утверждение теоремы.

Определение 2.6. Пусть $f : X \to [0,1], V \subset X, -$ открытое подмножество, $K \subset X$ - компактное подмножество. Будем писать $f \prec V$ или $V \succ f$, если $\operatorname{supp} f \subset V$. Будем писать $f \succ K$ или $K \prec f$, если $\forall x \in K$ выполнено $f(x) = 1$.

Лемма 2.1 (Урысон). Пусть X - локально компактное хаусдорфово пространство и K - компактное множество, V - открытое множество, $K \subset V$. Тогда $\exists f : X \to [0,1]$ - непрерывная на X функция такая, что $K \prec f \prec V$.

Идея доказательства теоремы 2.3 Пусть $\ell : X \to \mathbb{C}$. Определим меру $\mu(V) = \sup\{\ell(f) : f \prec V\}$ на открытых подмножествах $V \subset X$ и меру $\nu(K) = \inf\{\ell(f) : K \prec f\}$ на компактных подмножествах $K \subset\subset X$, продолжим их на всё пространство X. Если для любого борелевского множества $B \in \mathcal{B}(X)$ выполнено $\mu(B) = \nu(B)$, то определённая таким образом функция будет искомой мерой на X. Для доказательства равенства μ и ν следует воспользоваться леммой Урысона.

Теорема 2.5. Пусть $A = A^*$ - самосопряженный оператор и f функция такая, что $\operatorname{Im} f = \{0,1\}$. Тогда $f(A) = f^*(A) = f^2(A)$, то есть $f(A)$ является ортогональным проектором.

Доказательство. Из $\operatorname{Im} f = \{0,1\}$ следует, что функцию f можно представить в виде $f(x) = \chi_B(x)$, где B - множество точек, в которых функция f принимает значение 1 , то есть $f(x) = 1$ тогда и только тогда, когда $x \in B$ и в остальных точках $f(x) = 0$.

Из следствия 2.3 получаем, что $f(A)$ корректно определена. Более того, оператор $f(A)$ унитарно эквивалентен оператору $\oplus_n f(M_x^n)$, где операторы умножения на независимую переменную M_x^n действуют в пространствах $L^2(\mu_n)$. Тогда для любого $\psi_n \in L^2(\mu_n)$ имеем

$$(f(M_x^n)\psi_n)(x) = f(x)\psi_n(x) = \begin{cases} \psi_n(x), & x \in B \\ 0, & x \notin B \end{cases} \tag{2.21}$$

Легко видеть, что операторы $f(M_x^n)$ являются ортогональными проекторами. Таким образом, $f(A)$ униарно эквивалентен ортогональной сумме проекторов $f(M_x^n)$ в пространствах $L^2(\mu_n)$. $\square$

Для борелевского множества $B \subset \mathrm{Spect}(A)$ определим операторозначную функцию E по формуле $E(B) = \chi_B(A)$. По теореме 2.5 это проектор, то есть $E(B) = E^*(B) = E^2(B)$.

Теорема 2.6. Проекторозначная функиия $B \to E(B)$ обладает свойствами:

1. $E(B) = E^*(B) = E^2(B)$;
2. $E(\emptyset) = 0, E(\mathbb{R}) = I$;
3. $E\left(\bigcup_j B_j\right) = \sum_j E\left(B_j\right)$,

если множества $B_j \cap B_k = \emptyset$, а сходимость ряда понимается в смысле сильной операторной топологии и называется спектральной мерой самосопряженного оператора A.

Доказательство. В следствие теоремы 2.4 оператор A унитарно эквивалентен ортогональной сумме операторов умножения M_x^n в пространствах $L^2\left(\mu_n\right)$. В этих пространствах $\chi_B\left(M_x^n\right)$ представляет собой оператор умножения на индикаторную функцию $\chi_B(x)$ множества B.

Определение 2.7. Для пары $A \in \mathfrak{A}, \rho = |\psi\rangle\langle\psi| \in \mathfrak{S}$ положим

$$P_A^\rho(B) = \langle\psi, E(B)\psi\rangle.$$

Следствие 2.4. Возъмём произвольный набор единичных векторов $\psi_j \in H$. По аксиоме 1.3 Макки для выпуклых комбинаций

$$\rho = \sum_j \pi_j \left|\psi_j\right\rangle \left\langle\psi_j\right| = \sum_j \pi_j \rho_j \tag{2.22}$$

$\pi_j \geq 0, \sum_j \pi_j = 1$, вероятность должна вычисляться по формуле

$$P_A^\rho(B) = \sum_j \pi_j P_A^{\rho_j}(B) = \sum_j \pi_j \left\langle\psi_j, E(B)\psi_j\right\rangle. \tag{2.23}$$

Поскольку $0 \leq \langle\psi_j, E(B)\psi_j\rangle \leq 1$ и $\pi_j \geq 0, \sum_j \pi_j = 1$, формуль и (2.23) корректно определены.

Замечание 2.5 (связь подходов Шрёдингера и Гейзенберга). Пусть самосопряженный оператор A обладает циклическим вектором, как это имеет место для наблюдаемых координаты и импульса q и p, и пусть $\rho = |\psi\rangle\langle\psi|$ - чистое состояние. Рассмотрим проекторозначную меру 2.6 и представление A в пространстве $L^2(\mu)$, определённое в теореме 2.4. Тогда вероятностная мера на борелевских подмножествах $B \in \mathcal{B}(\mathbb{R})$, отвечающая паре (ρ, A), определяется формулой

$$P_A^{|\psi\rangle\langle\psi|}(B) = \langle\psi, E(B)\psi\rangle \tag{2.24}$$

при подходе Гейзенберга и формулой Борна:

$$P_A^{|\psi\rangle\langle\psi|} = \int_B \left|\psi_A(x)\right|^2 d\mu(x) \tag{2.25}$$

при подходе Шрёдингера. Функции, определённые формулами (2.24) и (2.25) совпадают в силу теоремы 2.4.

Вопрос 2.1. Верно ли, что пространство наблюдаемых $\mathfrak{A}$ состоит только из самосопряженных операторов?

Утверждение. Пространство наблюдаемых $\mathfrak{A}$ можно расширить до множества положительных операторозначных мер [13.

Вопрос 2.2 (Макки). Можно ли расширить выпуклое множество состояний $\mathfrak{S}$?

Утверждение. На этот вопрос отвечает теорема Глизона [31 - выпуклое множество состояний $\mathfrak{S}$ расширить нельзя.

6.2.3 2.3. Nuclear Operators

Мы научились строить семейство распределений вероятностей P_A^ρ для того случая, когда $A \in \mathfrak{A}$ - множеству самосопряженных операторов, а $\rho \in \mathfrak{S}$, где

$$\mathfrak{S} = \left\{ \sum_j \pi_j \left|\psi_j\right\rangle \left\langle\psi_j\right| : \pi_j \geq 0, \sum_j \pi_j = 1, \|\psi_j\| = 1 \right\}. \tag{2.26}$$

Получим абстрактное описание множества (2.26). Элементы (2.26) мы будем называть квантовыми состояниями или просто состояниями.

Определение 2.8. Оператор $\rho : H \to H$ называется компактным, если для любого ограниченного подмножества $B \subset H$ его образ $\rho(B)$ - предкомпактное множество (замыкание компактно).

Определение 2.9. Оператор $\rho : H \to H$ называется компактным, если для любой ограниченной последовательности $\{f_n\}, \|f_n\| \leq C$, существует сходящаяся подпоследовательность последовательности $\{\rho f_n\}$.

Утверждение 2.2. Определения 2.8 и 2.9 эквивалентны.

Поскольку проекторы являются самосопряженными операторами, $\mathfrak{S}$ состоит из самосопряженных операторов. Более того, проекторы - компактные операторы, так что состояния $\rho \in \mathfrak{S}$ компактны, так как являются пределом сходящейся по норме последовательности компактных операторов. Таким образом, любое состояние $\rho \in \mathfrak{S}$ является самосопряженным компактным оператором.

Теорема 2.7. Любой самосопряженный компактный оператор $\rho : H \to H$ можно представить в виде

$$\rho = \sum_j \lambda_j \left|\psi_j\right\rangle \left\langle\psi_j\right| \tag{2.27}$$

где $\langle\psi_j, \psi_k\rangle = \delta_{jk}, \rho\psi_j = \lambda_j\psi_j, ?^\circ \, |\lambda_1| \geq \cdots \geq |\lambda_n| \geq \ldots$, причём если множество $\{\lambda_n\}$ бесконечно, тогда $\lim_{n\to\infty} \lambda_n = 0$.

Доказательство. В силу теоремы 2.2 ;

$$\|\rho\| = \sup_{\lambda \in \operatorname{Spect}\rho} |\lambda| = |\lambda_1| \tag{2.28}$$

По определению нормы оператора существует последовательность $\{f_n\}$, $\|f_n\| = 1$, такая, что $\|\rho f_n\| \to \|\rho\|$ при $n \to \infty$. Последовательность $\{f_n\}$ является ограниченной, ρ - компактный оператор, следовательно существует сходящаяся подпоследовательность последовательности $\{\rho f_n\}$. Таким образом, существует собственный вектор ψ_1 оператора ρ, отвечающий собственному значению λ_1. Обозначим $H_1 = \{\mathbb{C}\psi_1\}$, $\rho_1 = \rho|_{H_1}$, и рассмотрим сужение $\rho_1^\perp = \rho|_{H \ominus H_1}$. Оператор $\rho_1^\perp$ является самосопряженным компактным оператором. Повторяя рассуждение по индукции, получаем, что $\rho = \oplus_j \rho_j$ относительно ортогонального разложения $H = \oplus_j H_j$, причём $\rho\psi_j = \lambda_j\psi_j$ для любого $\psi_j \in H_j$.

Определение 2.10. Оператор $A : H \to H$ называется положительным (обозначается $A > 0$), если для любого элемента $\psi \in H$ выполнено $(\psi, A\psi) \geq 0$.

Оператор A^*A - самосопряженный и положительный, следовательно функция $f(x) = \sqrt{x}$ непрерывна на $\operatorname{Spect}(A)$ и оператор $f\left(A^*A\right)$ корректно задан.

Определение 2.11. Модулем оператора A называется оператор $|A| = \sqrt{A^*A}$.

Определение 2.12. Пусть A - компактный оператор. Сингулярными собственными значениями оператора A называются собственные значения положительного оператора $|A|$:

$$s_j(A) = \lambda_j|A| \tag{2.29}$$

Замечание 2.6. Оператор A - компактный, следовательно оператор A^*A - компактный. Более того, он положительный и самосопряженный, следовательно по теореме 2.7 у него существует полный набор собственных векторов и собственных значений.

Определение 2.13. Оператор A называется ядерным, если

$$\sum_j s_j(A) < +\infty \tag{2.30}$$

Теорема 2.8 (5). Оператор $A : H \to H$ является ядерным тогда и только тогда, когда для любого выбора ортонормированного базиса (e_j) в H сумма

$$\sum_j \langle e_j, Ae_j\rangle < +\infty. \tag{2.31}$$

В этом случае сумма 2.31 не зависит от выбора базиса и называется следом $\mathrm{Tr}(A)$ оператора A.

Пример 2.2. Сумма 2.31 может существовать для некоторого базиса (e_j), но оператор при этом не будет ядерным. Пусть $\{e_j\}_{j=1}^{\infty}$. Определим изометрический оператор $S : H \to H$ на элементах базиса по формуле $S(e_j) = e_{j+1}$ и продолжим действие S, называемого оператором сдвига, на всё пространство H. Заметим, что в базисе $\{e_n\}$ ряд $\sum_j \langle e_j, Se_j\rangle$ сходится, и его сумма равна нулю. Однако в ортонормированном базисе $\{f_j\}$, где $f_j = \frac{1}{\sqrt{2}}(e_j + e_{j+1})$, ряд $\sum_j \langle f_j, Sf_j\rangle$ расходится, поскольку $\langle f_j, Sf_j\rangle = \frac{1}{2}$ для любого j. Из теоремы 2.10 следует, что S не является ядерным оператором.

Определение 2.14. Спектральным следом оператора A называется сумма его собственных значений:

$$\text{Спектральный след } = \sum_j \lambda_j. \tag{2.32}$$

Теорема 2.9. Пусть A - матрица размера $n \times n$, u $\{\lambda_j(A)\}_{j=1}^n$ – собственные значения A (корни характеристического уравнения

$$\det(A - \lambda E) = 0$$

с учётом кратности). Тогда справедливо тождество

$$\mathrm{Tr}\, A = \sum_{k=1}^{n} \lambda_k(A) \tag{2.33}$$

то есть след оператора в конечномерном гильбертовом пространстве $H, \dim H < +\infty$, совпадает с его спектральным следом.

Доказательство. Заметим, что для любого унитарного оператора U (матрицы перехода к другому ортонормированному базису) выполнено

$$\det\left(U(A - \lambda E)U^*\right) = \det(A - \lambda E) = 0, \tag{2.34}$$

то есть характеристический многочлен - инвариант - не зависит от выбора базиса.

Существует базис, в котором матрица A имеет жорданову нормальную форму $A \simeq \bigoplus_j A_j$, где A_j - жорданова клетка, отвечающая собственному значению λ_j :

$$A_j = \begin{pmatrix} \lambda_j & 1 & 0 & \dots & 0 & 0 \\ 0 & \lambda_j & 1 & \dots & 0 & 0 \\ 0 & 0 & \lambda_j & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \lambda_j & 1 \\ 0 & 0 & 0 & \dots & 0 & \lambda_j \end{pmatrix}. \tag{2.35}$$

В этом базисе $\operatorname{Tr} A = \sum_{k=1}^{n} \lambda_k(A)$, а определитель

$$\det(A - \lambda E) = \det A + \dots + (-1)^{n-1} \left(\sum_j \lambda_j \right) \lambda^{n-1} + (-1)^n \lambda^n \tag{2.36}$$

Один из коэффициентов характеристического многочлена, с точностью до знака, равен спектральному следу. В произвольном базисе этот коэффициент равен $\operatorname{Tr} A$. В силу инвариантности характеристического многочлена относительно выбора базиса получаем утверждение теоремы.

Замечание 2.7. В бесконечномерном пространстве H может не существовать собственных векторов $A\psi = \lambda\psi$, как в случае оператора Вольтерры (пример 2.1).

Теорема 2.10 (В.Б. Лидский 6, 5]). Пусть A - ядерный оператор. Тогда след совпадает со спектральным следом:

$$\operatorname{Tr}(A) = \sum_j \lambda_j(A)$$

Таким образом мы получили формальное описание множества (2.26).

Теорема 2.11. Пространство квантовых состояний $\mathfrak{S}$ состоит из положительных ядерных состояний с единичным следом.

Доказательство. Пусть (ψ_j) и (π_j) - произвольный набор единичных векторов в H и произвольное дискретное распределение вероятностей соответственно. Рассмотрим состояние

$$\rho = \sum_j \pi_j \left|\psi_j\right\rangle \left\langle\psi_j\right|.$$

Для произвольного ортонормированного базиса (e_k) в H получаем

$$\sum_k \langle e_k, \rho e_k \rangle = \sum_{j,k,l} \pi_j \langle e_k, \psi_j \rangle \langle \psi_j, e_l \rangle = \sum_j \pi_j = 1.$$

Таким образом, ρ - ядерный оператор с единичным следом по теореме 2.8 . □

6.2.4 2.4. Further Properties of Nuclear Operators

Обозначим $\mathfrak{S}_1(H)$ линейное пространство ядерных операторов в гильбертовом пространстве H. Таким образом, выпуклое множество квантовых состояний $\mathfrak{S}$ состоит из положительных ядерных операторов с единичным следом.

Определение 2.15. Оператор U называется частично изометриче, если для некоторого разложения $H = K \oplus K^{\perp}$ выполнено $Uh = 0$ для любого $h \in K^{\perp}$ и $(Uf, Ug) = (f, g)$ для любых $f, g \in K$. При этом проектор $P_K = U^*U$ называется начальным, а проектор $P_{\tilde{K}} = UU^*$, где $\tilde{K} = UK, -$ финальным.

Теорема 2.12 (о полярном разложении). Для любого ограниченного оператора A существует частично изометрический оператор U такой, что $A = U|A|$.

Доказательство. Обозначим K подпространство H, представляющее собой замыкание

образа $|A|H$. Определим действие оператора U формулами $U(|A|f) = Af$ и $U|_{K^\perp} = 0$. Тогда

$$\langle U|A|f, U|A|g\rangle = \langle Af, Ag\rangle = \langle f, A^*Ag\rangle = \langle f, |A| \cdot |A|g\rangle = \langle |A|f, |A|g\rangle. \tag{2.37}$$

Следовательно, U - частично изометрический оператор, и $A = U|A|$. □

Теорема 2.13. Оператор $A \in \mathfrak{S}_1(H)$ тогда и только тогда, когда его можно представить в виде $A = \sum_j |\xi_j\rangle \langle\eta_j|$, где $\sum_j \|\xi_j\| \cdot \|\eta_j\| < +\infty$, причём

$$\operatorname{Tr} A = \sum_j \langle \eta_j, \xi_j \rangle .$$

Доказательство. Используем полярное разложение $A = U|A|$. Оператор $|A|$ можно представить в виде $|A| = \sum_j s_j |\psi_j\rangle \langle\psi_j|$, где $\{\psi_j\}$ ортонормированный базис из собственных векторов $|A|$; сингулярные собственные значения A таковы, что $s_j \geq 0$, причём $\sum_j s_j < +\infty$. Обозначим $\xi_j = U\psi_j$. В силу частичной изометричности оператора U получаем $\|\xi_j\| \leq \|\psi_j\|$. Следовательно, оператор A можно представить в виде: $A = \sum_j s_j |\xi_j\rangle \langle\psi_j|$. Обозначим $\eta_j = s_j\psi_j$. Тогда $A = \sum_j |\xi_j\rangle \langle\eta_j|$. При этом

$$\sum_j \|\xi_j\| \cdot \|\eta_j\| \leq \sum_j s_j \|\psi_j\|^2 = \sum_j s_j < +\infty. \tag{2.38}$$

Согласно теореме 2.8 след ядерного оператора не зависит от выбора ортонормированного базиса, в котором он вычисляется. Найдём след оператора A в ортонормированном базисе $\{\psi_j\}$, состоящем из собственных векторов $|A|$:

$$\operatorname{Tr} A = \sum_j \langle \psi_j, A\psi_j\rangle = \sum_j \langle \psi_j, U|\, A \mid \psi_j\rangle = \\ = \sum_j s_j \langle \psi_j, U\psi_j\rangle = \sum_j \langle \eta_j, \xi_j\rangle .$$

Пусть теперь наоборот: оператор A представим в виде: $A = \sum_j |\xi_j\rangle \langle\eta_j|$. Операторы ранга один $|\xi_j\rangle \langle\eta_j| \in \mathfrak{S}_1(H)$, а ряд сходится по норме. Следовательно, $A \in \mathfrak{S}_1(H)$. □

Следствие 2.5. Пусть C - ограниченный оператор и $\rho \in \mathfrak{S}_1(H)$. Тогда $\rho C \in \mathfrak{S}_1(H)$.

Доказательство. По теореме 2.13ρ можно представить в виде: $\rho == \sum_j |\eta_j\rangle \langle\xi_j|$, где $\sum_j \|\xi_j\| \|\eta_j\| < +\infty$. Следовательно, $\rho C = \sum_j \pi_j |\eta_j\rangle \langle\psi_j|$, где $\psi_j = C\xi_j$, причём, в силу ограниченности оператора C, выполнено неравенство $\|\psi_j\| \leq \|C\| \cdot \|\xi_j\|$. Применяя ещё раз теорему 2.13, получаем ρC доказываемое утверждение. □

Теорема 2.14. Для сопряженного пространства имеет место равенство $\mathfrak{S}_1^*(H) = B(H)$ (алгебра всех ограниченных операторов в H).

Доказательство. Пусть $A \in B(H)$. Докажем, что $A \in \mathfrak{S}_1^*(H)$. Рассмотрим любой элемент $\rho \in \mathfrak{S}_1(H)$. Обозначим $f_A(\rho) = \operatorname{Tr}(\rho A)$. Заметим, что $|f_A(\rho)| \leq \|A\|_{B(H)} \cdot \|\rho\|_1 < +\infty$, то есть f_A - ограниченный линейный функционал на пространстве $\mathfrak{S}_1(H)$, то есть $f_A \in \mathfrak{S}_1(H)^*$.

Наоборот, возьмём функционал $f \in \mathfrak{S}_1^*(H)$. Докажем, что существует оператор $A \in B(H)$, для которого $f(\rho) = \operatorname{Tr}(\rho A)$ на всех $\rho \in \mathfrak{S}_1(H)$. По теореме 2.13 любой элемент $\rho\mathfrak{S}_1(H)$ представим в виде суммы операторов ранга один. Заметим, что действие функционала f на операторы ранга один $f(|\xi\rangle\langle\eta|)$ определяет функционал, линейный по η и антилинейный по ξ. По теореме Рисса-Фреше существует единственный $A \in B(H)$ такой, что $f(|\xi\rangle\langle\eta|) = \langle\xi, A\eta\rangle$. Поскольку любой $\rho \in \mathfrak{S}_1(H)$ представим в виде сходящегося по норме ряда из операторов ранга один, и $A \in B(H)$, действие f продолжается по линейности на всё $\mathfrak{S}_1(H)$. □

6.3 A.3

6.3.1 3.1. Positive Operator - Valued Measures

Согласно теореме 2.6 любой самосопряженный оператор A определяет проекторозначную меру E на спектре $\mathrm{Spect}(A) \subset \mathbb{R}$, которая участвует в определении распределения вероятностей:

$$P_A^\rho(B) \equiv P_E^\rho = \mathrm{Tr}(\rho E(B)),$$

отвечающего паре $A \in \mathbb{A}, \rho \in \mathfrak{S}$, где $B \in \mathcal{B}(\mathbb{R})$ - произвольное борелевское множество. Меру E можно расширить на всю действительную прямую, положив её равной нулю на множествах $B, B \cap \mathrm{Spect}(A) = \emptyset$. Следующее определение даёт естественное обобщение проекторозначных мер.

Определение 3.1. Положительной операторозначной мерой называется функция $M : \mathcal{B}(\mathbb{R}) \to B(H)$ для которой выполнены следующие условия:

1. $M(B) \geq 0$ - положительный оператор;
2. $M(\emptyset) = 0$ - нулевой оператор, $M(\mathbb{R}) = I$ тождественный оператор;
3. $M\left(\bigcup_j B_j\right) = \sum_j M(B_j)$, если множества $B_j \cap B_k = \emptyset$ для любых $j \neq k$, где сходимость операторного ряда понимается в смысле сильной операторной топологии.

Определим функцию борелевского множества $B \in \mathcal{B}(\mathbb{R})$ по формуле

$$P_M^\rho(B) = \mathrm{Tr}(\rho M(B)) \tag{3.1}$$

Формула 3.1 корректно определяет некоторую вероятностную меру на прямой. Нашей целью будет выяснить, можно ли использовать проекторозначные меры для нового определения множества наблюдаемых $\mathfrak{A}$.

6.3.2 3.2. Holevo 's Theorem

Вопрос 3.1. Пусть выполнена аксиома 1.3 Макки $P_E^{\sum_j \rho_j} = \sum_j \pi_j P_E^{\rho_j}$. Обязательно ли брать в качестве множества наблюдаемых $\mathfrak{A}$ самосопряженные операторы A, определяющие проекторозначные меры E? Иными словами, можно ли расширить множество наблюдаемых?

Теорема 3.1 (А.С. Холево [13]). Пусть для любого состояния $\rho \in \mathfrak{S}$ определён набор вероятностных мер $\{P^\rho\}$, удовлетворяющих аксиоме 1.3 Макки. Тогда существует отображение $M : \mathcal{B}(\mathbb{R}) \to B(H)$ из алгебры борелевских множеств на прямой $\mathcal{B}(\mathbb{R})$ в алгебру ограниченных операторов $B(H)$, являющееся положительной операторозначной мерой в смысле определения 3.1, такое, что $P^\rho(B) = \mathrm{Tr}(\rho M(B))$.

Набросок доказательства теоремы 3.1. Представим состояние в виде: $\rho = \mathrm{Re}\,\rho + i \cdot \mathrm{Im}\,\rho$, где $\mathrm{Re}\,\rho = \frac{1}{2}(\rho + \rho^*), \mathrm{Im}\,\rho = \frac{1}{2i}(\rho - \rho^*)$ − самосопряженные операторы. Для самосопряженных $\rho = \rho^*$ справедливо представление: $\rho = \rho_+ - \rho_-$, где

$$\rho_+ = \chi_+(\rho), \chi_+(x) = \begin{cases} 1, & x > 0 \\ 0, & x \leq 0 \end{cases}$$

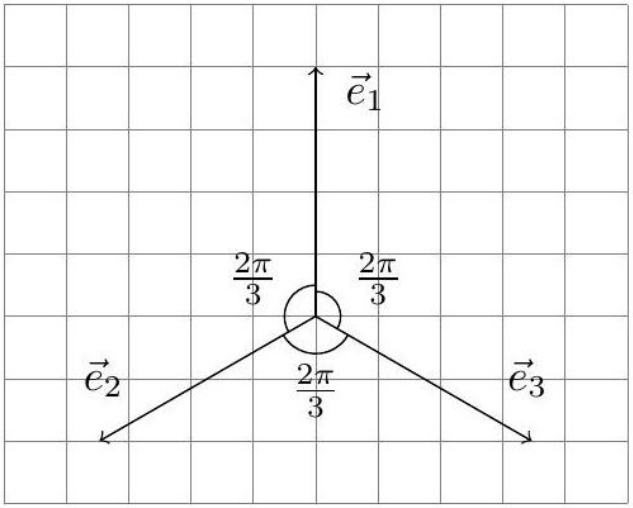
$$\rho_- = \chi_-(\rho), \chi_-(x) = \begin{cases} 0, & x \geq 0 \\ 1, & x < 0 \end{cases}$$

Определим $f \in \mathfrak{S}_1^*(H)$ по формуле

$$f\left(\frac{\rho_\pm}{\operatorname{Tr}\rho_\pm}\right)(B) = P^{\frac{\rho_\pm}{\operatorname{Tr}\rho_\pm}}(B) \tag{3.2}$$

и продолжим по линейности на всё $\mathfrak{S}_1(H)$. Согласно теореме 2.14 $\mathfrak{S}_1^*(H) = \mathfrak{B}(H)$, следовательно существует единственный оператор $M(B)$ для которого $f(\rho) = \operatorname{Tr}(\rho M(B))$. □

Пример 3.1. Рассмотрим три вектора $\vec{e}_1, \vec{e}_2$ и $\vec{e}_3$, составляющие углы $\frac{2\pi}{3}$ друг с другом на плоскости.



Проектор на направление $\vec{e} = \begin{pmatrix} \alpha & \beta \end{pmatrix}^T$, где $|\alpha|^2 + |\beta|^2 = 1$, имеет вид

$$|\vec{e}\rangle\langle\vec{e}| = \begin{pmatrix} |\alpha|^2 & \alpha\bar{\beta} \\ \bar{\alpha}\beta & |\beta|^2 \end{pmatrix}. \tag{3.3}$$

В нашем случае

$$\sum_{j=1}^{3} |e_j\rangle \langle e_j| = \frac{3}{2} I \tag{3.4}$$

Следовательно,

$$M_j = \frac{2}{3} |e_j\rangle \langle e_j| \tag{3.5}$$

Тогда для любого разбиения действительной оси на четыре борелевских множества $\mathbb{R} = B_1 \cup B_2 \cup B_3 \cup B_4$ можно определить положительную операторозначную меру по формуле

$$M(B_j) = \begin{cases} \frac{2}{3} |e_j\rangle \langle e_j|, & j \in \overline{1,3} \\ 0, & j = 4 \end{cases} \tag{3.6}$$

Из теоремы 3.1 немедленно вытекает

Следствие 3.1. Вместо множества самосопряженных операторов $\mathfrak{A}$ в качестве наблюдаемых можно взять множество положительных операторозначных мер $\mathfrak{M}$. При этом распределение вероятностей, отвечающее паре $M \in \mathfrak{M}, \rho \in \mathfrak{S}$, задаётся формулой

$$P_M^\rho(B) = \operatorname{Tr}(\rho M(B)) \tag{3.7}$$

$B \in \mathcal{B}(\mathbb{R})$.

Доказательство. Поскольку M является счётно-аддитивной мерой, это свойство наследуется P_M^ρ. Остаётся проверить выполнение аксиомы 1.2. Порложим

$$P^{\rho}_{M^f}(B) = P^{\rho}_{M}\left(f^{-1}(B)\right) = \mathrm{Tr}\left(\rho M\left(f^{-1}(B)\right)\right), \tag{3.8}$$

$B \in \mathcal{B}(\mathbb{R})$. Условие $B \cap C = \emptyset$ влечёт $f^{-1}(B) \cap f^{-1}(C) = \emptyset$ для $B, C \in \mathcal{B}(\mathbb{R})$. Следовательно, (3.8) корректно определяет распределение вероятностей.

Следующая теорема проясняет структуру положительных операторозначных мер.

Теорема 3.2 (М.А. Наймарк [8]). Для любой положительной операторозначной меры $M : \mathcal{B}(\mathbb{R}) \to B(H)$ существует гильбертово пространство K, в которое H изометрически вложено, и проекторозначная мера $E : \mathcal{B}(\mathbb{R}) \to B(K)$ такая, что $M(B) = (P_H E(B))|_H$.

Доказательство. Рассмотрим простые функции $f, g : \mathbb{R} \to H$, то есть такие, что $f(t) = \sum_j f_j \chi_{B_j}(t), g(t) = \sum_k g_k \chi_{C_k}(t)$, где $\chi_B(t) == \begin{cases} 1, & t \in B; \\ 0, & t \notin B. \end{cases}$ Определим скалярное произведение по формуле

$$(f, g)_K = \sum_{j,k} \langle f_j, M\left(B_j \cap C_k\right) g_k \rangle_H \tag{3.9}$$

Гильбертово пространство K получим с помощью замыкания линейной оболочки простых функций по норме $\| \cdot \|_K = \sqrt{(\cdot, \cdot)_K}$. Любому элементу $f \in H$ соответствует элемент $f\chi_{\mathbb{R}}(t) \in K$, при этом $(f\chi_{\mathbb{R}}, g\chi_{\mathbb{R}})_K = \langle f, M(\mathbb{R})g \rangle_H = \langle f, g \rangle_H$, то есть пространство H изометрически вложено в пространство K.

Для любого элемента $\xi \in K$ определим проектор

$$(E(B)\xi)(t) = \begin{cases} \xi(t), & t \in B \\ 0, & t \notin B \end{cases} \tag{3.10}$$

Заметим, что

$$E(B)g\chi_{\mathbb{R}} = \begin{cases} g, & t \in B \\ 0, & t \notin B \end{cases} \tag{3.11}$$

Следовательно, $(f\chi_{\mathbb{R}}, E(B)g\chi_{\mathbb{R}})_K = \langle f, M(B)g \rangle_H$. Таким образом, $M(B) = (P_H E(B))|_H$.

6.3.3 3.3. Classical and Quantum Probability Theories (??!!!)

3.3.1. Классическая теория вероятностей

Рассмотрим знаменитую тройку Колмогорова (Ω, Σ, P), где Ω - пространство элементарных событий, Σ - сигма-алгебра событий, $P : \Sigma \to\to [0, 1]$ - вероятностная мера [35].

Случайная величина ξ - измеримая функция $\Omega \to \mathbb{R}$, то есть для любого борелевского множества $B \in \mathcal{B}(\mathbb{R})$ выполнено $\xi^{-1}(B) \in \Sigma$. Задать случайную величину ξ - значит определить вероятности: $P\left(\xi^{-1}(B)\right)$.

Важную роль играют следующие два частных случая.

Пример 3.2 (случайная величина с дискретным распределением). Возьмём набор непересекающихся борелевских множеств $B_k \in \mathcal{B}(\mathbb{R})$,

действительные числа $\lambda_k \in \mathbb{R}$, и определим дискретную случайную величину по формуле

$$\xi(\omega) = \sum_k \lambda_k \chi_{B_k}(\omega), \tag{3.12}$$

$\omega \in \Omega$, где χ_{B_k} - индикаторная функция подмножества B_k. Со случайной величиной (3.12) ассоциировано распределение вероятностей:

$$\Pr\left(\xi = \lambda_k\right) = P\left(B_k\right). \tag{3.13}$$

Для случайной величины ξ можно определить математическое ожидание $\mathbb{E}(\xi)$ и дисперсию $\mathrm{Var}(\xi)$ по формулам

$$\mathbb{E}(\xi) = \sum_k \lambda_k Pr\left(\xi = \lambda_k\right) = \sum_k \lambda_k P\left(B_k\right),$$
$$\mathrm{Var}(\xi) = \mathbb{E}\left((\xi - \mathbb{E}(\xi))^2\right) = \sum_k \left(\lambda_k - \mathbb{E}(\xi)^2 P\left(B_k\right).\right.$$

Пример 3.3 (случайная величина с абсолютно непрерывным распределением). Предположим, что существует такая функция $p_\xi(x)$, называемая плотностью распределения $\Pr(\xi \in B)$, что

$$\Pr(\xi \in B) = \int_B p_\xi(x)dx, B \in \mathcal{B}(\mathbb{R})$$

Тогда говорят, что распределение абсолютно непрерывно. В этом случае, математическое ожидание $\mathbb{E}(\xi)$ и дисперсия $\mathrm{Var}(\xi)$ определяются формулами

$$\mathbb{E}(\xi) = \int_{\mathbb{R}} x p_\xi(x)dx$$
$$\mathrm{Var}(\xi) = \mathbb{E}\left((\xi - \mathbb{E}(\xi))^2\right) = \int_{\mathbb{R}} (x - \mathbb{E}(\xi))^2 p_\xi dx$$

3.3.2. Квантовая теория вероятностей

Попробуем построить некоторое подобие аксиоматики квантовой теории вероятностей. По аналогии с тройкой Колмогорова, рассмотрим тройку $(H, \mathfrak{P}, \mu)$, где H - гильбертово пространство, $\mathfrak{P}$ - множество всех ортогональных проекторов в H и $\mu : \mathfrak{P} \to [0,1]$ - некоторая функция, сопоставляющая каждому $P \in \mathfrak{P}$ число $0 \leq \mu(P) \leq 1$.

Определение 3.2. Элементы $\xi \in H, \|\xi\| = 1$, которые можно отождествить с одномерными проекторами $|\xi\rangle\langle\xi|$, будем называть элементарными событиями. Если квантовая система приготовлена в некотором чистом состоянии $\xi, \|\xi\| = 1$, будем говорить, что элементарное событие произошло. Элементы $\mathfrak{P}$ будем называть событиями. Если квантовая система находится в состоянии ξ будем считать, что событие $P \in \mathfrak{P}$ произошло, если $\xi \in H_P = PH$.

Определение 3.3. Наименъшей общей гранью $P \vee Q$ называется ортогональный проектор на пересечение подпространств $H_P \cap H_Q$.Hau большей общей гранью $P \wedge Q$ называется ортогональный проектор на подпространство, порождённое $H_P \cup H_Q$.

Замечание 3.1. Наименьшая $P \vee Q$ и наибольшая $P \wedge Q$ грани всегда определены, поскольку $H_P \cap H_Q$ содержит как минимум нулевой вектор, а $H_P \cup H_Q$ принадлежит H. Множество, для любого набора элементов которого определены точная нижняя и точная верхняя грани, называется решёткой. Таким образом, множество проекторов является решёткой.

Определение 3.4. События $P_k \in \mathfrak{P}, 1 \leq k \leq N$, называются совместимыми, если они попарно коммутируют $[P_k, P_m] = 0$. Отметим, что для совместимых событий любое их произведение также является событием $P_{k_1} P_{k_2} \ldots P_{k_n} \in \mathfrak{P}, 1 \leq k_s \leq N$.

Определение 3.5. Будем называть функцию $\mu : \mathfrak{P} \to [0,1]$ вероятностной мерой, если

1. $\mu(0) = 0, \mu(I) = 1$;

2. $\mu\left(\vee_j P_j\right) = \sum_j \mu\left(P_j\right)$, если $P_j \wedge P_k = 0$ для $j \neq k$.

Определение 3.6. Будем говорить, что тройка $\left(H, \mathfrak{P}, \mu \right)$ задаёт квантовое вероятностное пространство, если H - гильбертово пространство элементарных событий, $\mathfrak{P}$ - решётка проекторов, элемнты которой события, и μ - вероятностная мера на $\mathfrak{P}$.

Вопрос 3.2. Как задать меру μ на $\mathcal{P}$?

Теорема 3.3 (Э. Глизон, 1957 [31]. Пусть μ-мера на $\mathcal{P} u \dim H > 2$. Тогда существует единственное $\rho \in \mathfrak{S}$ такое, что $\mu(P) = \mathrm{Tr}(\rho P)$.

Замечание 3.2. Условие $\dim H > 2$ существенно. Рассмотрим случай $\dim H = 2$. Фиксируем $H_0 \subset H, \dim H_0 = 1$. Зададим меру μ на проекторах P_K на всевозможные подпространства $K \subset H$. Если $K \neq H_0$,

положим $\mu\left(P_K\right) = 1$ или 0 по желанию (произвольно) и установим $\mu\left(P_{K^\perp}\right) = \mu\left(I - P_K\right) = 1 - \mu(K)$. Зададим $\mu\left(P_{H_0}\right) = \mu\left(P_{H_0^\perp}\right) = \frac{1}{2}$. Эта мера не представима в виде $\mu(P) = \mathrm{Tr}(\rho P)$ ни для какого состояния ρ. Указанные меры не нашли применение в квантовой механике. С другой стороны, в двумерном пространстве H формула $\mu(P) = \mathrm{Tr}(\rho P)$ корректно задаёт меру для любого фиксированного $\rho \in \mathfrak{S}$.

Для начала, будем считать, что множество наблюдаемых $\mathfrak{A}$ состоит из самосопряженных операторов в гильбертовом пространстве H, то есть, согласно теореме 2.6 $A \in \mathfrak{A}$ сопоставлена проекторозначная функция E. По аналогии с классической теорией вероятностей будем называть элементы $\mathfrak{A}$ квантовыми случайными величинами, поскольку проекторозначная мера E задаёт распределение вероятностей на прямой $\mathbb{R}$ по формуле

$$\Pr(A \in B) = \mu(E(B)) = \mathrm{Tr}(\rho E(B)), B \in \mathcal{B}(\mathbb{R}), \tag{3.14}$$

где левая часть равенства (3.14 интерпретируется как вероятность того, что квантовая случайная величина A принимает значение из множества B.

Определение 3.7. Математическим ожиданием $\mathbb{E}_\rho(A)$ и дисперсией $\mathrm{Var}_\rho(A)$ квантовой случайной величины A называются величины:

$$\mathbb{E}_\rho(A) = \mathrm{Tr}(\rho A), \mathrm{Var}_\rho(A) = \mathbb{E}_\rho\left((A - \mathrm{Tr}(\rho A))^2\right).$$

Для попарно коммутирующих квантовых случайных величин $A_k \in\in \mathfrak{A}, [A_k, A_m] = 0, 1 \leq k, m \leq N, k \neq m$, их проекторозначные меры, определённые формулой $E_k(B) = \chi_B\left(A_k\right), B \in \mathcal{B}(\mathbb{R}), 1 \leq k \leq N$, также коммутируют. Следовательно, проекторы $P_k = E_k\left(B_k\right) \in \mathfrak{P}$ являются совместимыми событиями в смысле определения 3.4, и можно ввести совместное распределение вероятностей:

$$\Pr\left(A_{k_1} \in B_1, \ldots A_{k_n} \in B_n\right) = \mathrm{Tr}\left(\rho E_{k_1}\left(B_1\right) \ldots E_{k_n}\left(B_n\right)\right) \tag{3.15}$$

$B_k \in \mathcal{B}(\mathbb{R}), 1 \leq k, k_n \leq N$.

По аналогии с классической теорией вероятностей рассмотрим два примера.

Пример 3.4 (квантовая случайная величина с дискретным распределением). Положим $A = \sum_j \lambda_j P_j \in \mathfrak{A}$, где $P_j \wedge P_k = \emptyset, \lambda_j \in \mathbb{R}$, и события $P_j \in \mathfrak{P}$ образуют полный набор ортогональных проекторов
$\sum_j P_j = I$. Тогда дискретная квантовая случайная величина определяется распределением вероятностей $\Pr\left(A = \lambda_j\right) = \mu\left(P_j\right) = \mathrm{Tr}\left(\rho P_j\right)$, где μ - мера на $\mathcal{P}$, определяемая состоянием $\rho \in \mathfrak{S}$.

Тогда математическое ожидание $\mathbb{E}_\rho(A)$ и дисперсия $\mathrm{Var}_\rho(A)$ определяются по формуле

$$\mathbb{E}_\rho(A) = \sum_j \lambda_j \mu\left(P_j\right)$$
$$\mathrm{Var}_\rho(A) = \sum_j \left(\lambda_j - \mathrm{Tr}(\rho A)\right)^2 \mu\left(P_j\right)$$

Пример 3.5 (квантовая случайная величина с абсолютно непрерывным распределением). Предположим, что найдётся функция $p_A(x)$, называемая плотностью распределения $\Pr(A \in B)$, такая, что $\Pr(A \in B) = \int_{\mathbb{R}} x p_A(x) dx$, тогда говорят, что A имеет абсолютно непрерывное распределение. В этом случае, математическое ожидание $\mathbb{E}_\rho(A)$ и дисперсия $\mathrm{Var}_\rho(A)$ даются формулами

$$\mathbb{E}_\rho(A) = \int_{\mathbb{R}} x p_A(x),$$
$$\mathrm{Var}_\rho(A) = \mathbb{E}_\rho\left((A - \mathrm{Tr}(\rho A))^2\right).$$

6.3.4 3.4. Quantum Random Variables (Observables) Using the Example of a Quantum Harmonic Oscillator

Рассмотрим гамильтониан квантового гармонического осциллятора:

$$H = \frac{p^2}{2} + \frac{q^2}{2} \tag{3.16}$$

Решим задачу о собственных числах и собственных значениях H :

$$H\psi = \lambda\psi \tag{3.17}$$

Введём вспомогательные операторы, называемые операторами рождения и уничтожения, по формуле

$$a^+ = \frac{q - ip}{\sqrt{2}}, a = \frac{q + ip}{\sqrt{2}} \tag{3.18}$$

Операторы (3.18) удовлетворяют коммутационному соотношению:

$$\left[a, a^+\right] = \mathrm{I} \tag{3.19}$$

Выражая p и q через (3.18) и подставляя соответствующие выражения в 3.16 получаем

$$H = \frac{1}{2}\mathrm{I} + a^+ a \tag{3.20}$$

Нормированное решение уравнения:

$$a \mid 0 >= 0 \tag{3.21}$$

удовлетворяет уравнению 3.17 с $\lambda = \frac{1}{2}$, называется основным состоянием квантового гармонического осциллятора и имеет волновую функцию:

$$< x \Big| 0 >= \frac{1}{\pi^{1/4}} \exp\left(-\frac{x^2}{2}\right) \tag{3.22}$$

Положим

$$\left| n >= \frac{1}{\sqrt{n!}} \left(a^+\right)^n \right| 0 > \tag{3.23}$$

тогда, в силу коммутационного соотношения (3.19), $\mid n >$ удовлетворяет уравнению 3.17 с $\lambda = \frac{1}{2} + n$, называется n-м возбуждённым состоянием осциллятора и имеет волновую функцию:

$$< x \left| n >= \frac{1}{\pi^{1/4} n! 2^n} H_n(x) \exp\left(-\frac{x^2}{2}\right), \right. \tag{3.24}$$

где

$$H_n(x) = (-1)^n \exp\left(x^2\right) \frac{d^n}{dx^n} \left(\exp\left(-x^2\right)\right)$$

- полиномы Эрмита. В квантовой оптике важную роль играют когерентные состояния $\mid \alpha >, \alpha \in \mathbb{C}$, являющиеся решением уравнения

$$a|\alpha >= \alpha|\alpha > \tag{3.25}$$

и имеющие волновые функции:

$$< x \left| \alpha >= \frac{1}{\pi^{1/4}} \exp\left(-\frac{(x - \sqrt{2}\,\mathrm{Re}(\alpha))^2}{2} + i\sqrt{2}\,\mathrm{Im}(\alpha)x\right) \right. \tag{3.26}$$

Также полезно выражение когерентного состояния через возбуждённые состояния:

$$\left|\alpha >= \exp\left(-\frac{|\alpha|^2}{2}\right) \sum_{n=0}^{+\infty} \frac{\alpha^n}{\sqrt{n!}}\right| n > \tag{3.27}$$

Для математического ожидания и дисперсии наблюдаемых q и p в когерентных состояниях получаем

$$\begin{aligned}
\mathbb{E}_{|\alpha\rangle}(q) &= \frac{1}{\sqrt{2}} \langle\alpha| \left(a^+ + a\right) |\alpha\rangle = \sqrt{2}\,\mathrm{Re}(\alpha), \\
\mathbb{E}_{|\alpha\rangle}(p) &= \frac{i}{\sqrt{2}} \langle\alpha| \left(a^+ - a\right) |\alpha\rangle = \sqrt{2}\,\mathrm{Im}(\alpha), \\
\mathrm{Var}_{|\alpha\rangle}(q) &= \frac{1}{2} \langle\alpha| \left(a^+ + a\right)^2 |\alpha\rangle - 2\,\mathrm{Re}(\alpha)^2 = \\
&= \frac{1}{2} \left(\bar{\alpha}^2 + \alpha^2 + 1 - 2|\alpha|^2\right) - 2\,\mathrm{Re}(\alpha)^2 = \frac{1}{2}, \\
\mathrm{Var}_{|\alpha\rangle}(p) &= \frac{1}{2} \langle\alpha| - \left(a^+ - a\right)^2 |\alpha\rangle - 2\,\mathrm{Im}(\alpha)^2 = \\
&= \frac{1}{2} \left(-\bar{\alpha}^2 - \alpha^2 + 1 - 2|\alpha|^2\right) - 2\,\mathrm{Im}(\alpha)^2 = \frac{1}{2}.
\end{aligned}$$

Фиксируем $\gamma \neq 0$ и введём операторы

$$b = \frac{\gamma q + i\frac{1}{\gamma} p}{\sqrt{2}}, b^+ = \frac{\gamma q - i\frac{1}{\gamma} p}{\sqrt{2}} \tag{3.28}$$

Операторы (3.28), как и операторы (3.18), удовлетворяют соотношению

$$\left[b, b^+\right] = \mathrm{I}$$

Отметим, что операторы (3.28) связаны с операторами (3.18) соотношениями

$$b = \mathrm{ch}(\alpha)a + \mathrm{sh}(\alpha)a^+, b^+ = \mathrm{sh}(\alpha)a + \mathrm{ch}(\alpha)a^+ \tag{3.29}$$

$\alpha = \ln(\gamma)$ при $\gamma > 0$. Соотношения (3.29) называются преобразованием Боголюбова. Нормированными решениями уравнения

$$b\psi_{\gamma,\alpha} = \alpha\,|\psi_{\gamma,\alpha}\rangle$$

будут функции

$$\langle x \mid \psi_{\gamma,\alpha}\rangle = \frac{\sqrt{|\gamma|}}{\pi^{1/4}} \exp\left(-\frac{\gamma^2(x-\sqrt{2}Re\alpha)^2}{2} + i\sqrt{2}\gamma\,\mathrm{Im}(\alpha)x\right). \tag{3.30}$$

Выразим канонические наблюдаемые через операторы рождения и уничтожения b^+, b :

$$q = \frac{\gamma}{\sqrt{2}}\left(b^+ + b\right), p = \frac{i}{\gamma\sqrt{2}}\left(b^+ - b\right). \tag{3.31}$$

Принимая во внимание (3.31), получаем аналогично случаю когерентных состояний:

$$\mathbb{E}_{\psi_{\gamma,\alpha}}(q) = \sqrt{2}Re(\alpha), \mathbb{E}_{\psi_{\gamma,\alpha}}(p) = \sqrt{2}Im(\alpha)$$
$$\mathrm{Var}_{\psi_{\gamma,\alpha}}(q) = \frac{\gamma^2}{2}, \mathrm{Var}_{\psi_{\gamma,\alpha}}(p) = \frac{1}{2\gamma^2}$$

Состояния $\psi_{\gamma,\alpha}$ при $\gamma \neq 1$ принято называть сжатыми когерентными состояниями. Состояние $\psi_{\gamma,0}$ при $\gamma \neq 1$ называется сжатым вакуумом.

Предположим теперь, что некоторые абстрактные алгебраические элементы A^+и A удовлетворяют соотношению $[A, A^+] = 1$. Построим их представление в качестве линейных неограниченных операторов в гильбертовом пространстве H с ортонормированным базисом $(f_n, n = 0, 1, 2, \ldots)$ по формуле

$$A^+ f_n = \sqrt{n+1} f_{n+1}$$
$$Af_n = \sqrt{n} f_{n-1}, n > 0, Af_0 = 0 \tag{3.32}$$

Получаем, что операторы A^+и A унитарно эквивалентны операторам рождения и уничтожения a^+и a. Следовательно, все полиномиальные функции от них также будут унитарно эквивалентны. Таким образом, если рассматриваемые два оператора удовлетворяют соотношению (3.19) мы всегда можем думать о них как об операторах рождения и уничтожения в модели квантового гармонического осциллятора.

3.4.1. Распределение Пуассона

$$B = a^+ a$$

Найдём распределение вероятностей, отвечающее квантовой случайной величине (наблюдаемой) B в когерентном состоянии $\mid \alpha >$. Поскольку спектральное разложение имеет вид

$$B = \sum_{n=0}^{+\infty} n|n><n| \tag{3.33}$$

получаем

$$\Pr(B = n) =< \alpha\|n >< n\|\alpha >= |< n|\alpha >|^2 = \exp\left(-|\alpha|^2\right)\frac{|\alpha|^2}{n!}. \tag{3.34}$$

Нетрудно видеть, что 3.34 представляет собой распределение Пуассона с параметром $|\alpha|^2$, то есть

$$\mathbb{E}_{|\alpha\rangle}(B) = \mathrm{Var}_{|\alpha>}(B) = |\alpha|^2.$$

Немного видоизменим задачу (это пригодится нам при конструкции пуассоновского случайного процесса). Фиксируем $\lambda > 0$ и положим

$$B_1 = b^+ b,$$

где

$$b = a + \sqrt{\lambda}\mathrm{I}. \tag{3.35}$$

Тогда

$$\left[b, b^+\right] = \mathrm{I}$$

и спектр B_1 совпадает со спектром B, но B_1 имеет другие собственные векторы. Решим уравнение

$$b\,|0'\rangle = 0. \tag{3.36}$$

Подставляя (3.35) в (3.36), получаем, что решением уравнения будет когерентное состояние:

$$|0'\rangle = |-\sqrt{\lambda}\rangle.$$

Остальные собственные векторы вычисляются по формуле

$$|n'\rangle = \frac{(b^+)^n}{\sqrt{n!}}\,|0'\rangle$$

Теперь мы готовы вычислить распределение вероятностей, связанное с парой ($B_1, |0\rangle$):

$$\Pr\left(B_1 = n\right) = \left|\langle 0|\frac{(b^+)^n}{\sqrt{n!}}\right|0'\Big\rangle\,|^2 = \frac{1}{n!}\left|\Big\langle (a+\sqrt{\lambda}\mathrm{I})^n 0 \mid -\sqrt{\lambda}\Big\rangle\right|^2 = e^{-\lambda}\frac{\lambda^n}{n!}.$$

Таким образом, мы получили распределение Пуассона с параметром λ.

3.4.2. Гауссовское распределение

$$C = a^+ + a.$$

Найдём распределение вероятностей квантовой случайной величины (наблюдаемой) C в когерентном состоянии $\mid \alpha >$. Поскольку $C = \sqrt{2}q$ и

спектральная мера наблюдаемой q представляет собой оператор умножения на индикаторную функцию χ_B множества $B \in \mathcal{B}(\mathbb{R})$, получаем

$$\begin{aligned}\Pr(C \in B) =& \langle\alpha|\chi_{\sqrt{2}B}|\alpha\rangle = \frac{1}{\sqrt{\pi}}\int_{\sqrt{2}B}\exp\left(-(x-\sqrt{2}\,\mathrm{Re}(\alpha))^2\right)dx = \\ &= \frac{1}{\sqrt{2\pi}}\int_B \exp\left(-\frac{(x-2\,\mathrm{Re}(\alpha))^2}{2}\right)dx\end{aligned} \tag{3.37}$$

Таким образом, 3.37 представляет собой гауссовское распределение с параметрами

$$\mathbb{E}_{|\alpha\rangle}(C) = 2\,\mathrm{Re}(\alpha), \mathrm{Var}_{|\alpha>}(C) = 1$$

6.3.5 3.5. Randomization

В классической теории вероятностей рандомизированная случайная величина ξ принимает на элементарном событии ω не одно, а целый ряд значений $\xi(\omega) \in \{\xi_j, 1 \leq j \leq n\}$ с некоторыми вероятностями $p_j, 1 \leq j \leq n$ [4]. В квантовой теории вероятностей роль рандомизированных случайных величин играют положительные операторозначные меры 13 .

Пример 3.6. Пусть $A \in \mathfrak{A}$ - квантовая случайная величина, то есть $A = A^*$, и ей отвечает пректорозначная мера E. Роль элементарного события в квантовой теории вероятностей играет одномерный проектор $|\xi\rangle\langle\xi|, \xi \in H, \|\xi\| = 1$. Каково бы ни было борелевское множество $B \subset \mathcal{B}(\mathbb{R})$, всегда найдётся такое элементарное событие $\xi \in E(B)H$, что

$$P_A^\xi(B) = \langle \xi, E(B)\xi\rangle = 1$$

Таким образом, ξ задана точно.
Пусть теперь $M \in \mathfrak{M}$ - обобщённая квантовая наблюдаемая (положительная операторозначная мера). Тогда для любого элементарного события $\xi \in H$:

$$P_M^\xi(B) = \langle \xi, M(B)\xi\rangle < 1$$

поскольку скалярное произведение может равняться единице только в случае, когда $M(B)$ - проектор. Но в последнем случае M будет являться проекторозначной мерой.

По теореме 3.2 (Наймарка) $M(B) = P_H E(B)|_H, H \subset K$, где $E-$ проекторозначная мера. Рандомизированные квантовые случайные величины можно интерпретировать следующим образом. Исходная квантовая система H является открытой. Если добавить к ней резервуар (расширить пространство состояний до $K \supset H$), тогда значение квантовой случайной величины будет чётко определено. Значение квантовой случайной величины являлось нечётким, поскольку часть информации «теряется» в резервуаре.

6.3.6 3.6. The Ratio of Uncertainties

Пусть A, B - два самосопряженных оператора (наблюдаемых), и $\lambda \in\in \mathbb{R}$. Тогда

$$\begin{aligned} 0 \leq \|(A - i\lambda B)\psi\|^2 = \langle A\psi, A\psi\rangle - i\lambda\langle A\psi, B\psi\rangle + \\ +i\lambda\langle B\psi, A\psi\rangle + \lambda^2\langle B\psi, B\psi\rangle. \end{aligned} \tag{3.38}$$

Используем следующие соотношения:

$$\langle A\psi, B\psi\rangle = \langle \psi, AB\psi\rangle, \tag{3.39}$$

$$\langle B\psi, A\psi\rangle = \langle \psi, BA\psi\rangle = \overline{\langle \psi, AB\psi\rangle} \tag{3.40}$$

$$2\,\mathrm{Re}(-i\lambda\langle A\psi, B\psi\rangle) = 2\lambda\,\mathrm{Im}(\langle A\psi, B\psi\rangle) = \frac{2\lambda}{2i}\langle \psi, (AB - BA)\psi\rangle. \tag{3.41}$$

Следовательно, неравенство (3.38) выполнено для любого ψ при условии

$$\frac{\mathcal{D}}{4} = (\mathrm{Im}\langle A\psi, B\psi\rangle)^2 - \langle A\psi, A\psi\rangle\langle B\psi, B\psi\rangle \leq 0. \tag{3.42}$$

Таким образом,

$$(\mathrm{Im}\langle A\psi, B\psi\rangle)^2 \leq \left\langle \psi, A^2\psi \right\rangle \left\langle \psi, B^2\psi \right\rangle \tag{3.43}$$

Получаем неравенство

$$\left\langle \psi, A^2\psi \right\rangle \left\langle \psi, B^2\psi \right\rangle \geq \frac{1}{4}|\langle \psi, [A, B]\psi\rangle|^2. \tag{3.44}$$

Произведём замену $A \mapsto A - \mathbb{E}_\psi(A)I, B \mapsto B - \mathbb{E}_\psi(B)I$. Тогда коммутатор $[A, B]$ не изменится, а в левой части неравенства появятся дисперсии. В результате получится соотношение неопределённостей:

$$\mathrm{Var}_\psi(A)\,\mathrm{Var}_\psi(B) \geq \frac{1}{4}|\langle \psi, [A, B]\psi\rangle|^2. \tag{3.45}$$

Пример 3.7. Для $A = q, B = p$ формула 3.45 даёт соотношение неопределённгостей:

$$\sigma_q^2\sigma_p^2 \geq \frac{1}{4} \tag{3.46}$$

Равенство достигается, когда ψ - когерентное состояние.

6.3.7 3.7. Classical and Quantum Covariance

Определение 3.8. Ковариация двух классических случайных величин ξ и η определяется по формуле

$$\mathrm{Cov}(\xi, \eta) = \mathbb{E}[(\xi - \mathbb{E}\xi)(\eta - \mathbb{E}\eta)] \tag{3.47}$$

Определение 3.9. Матрицей ковариаций для классических случайных величин $\xi_k, 1 \leq k \leq N$, называется матрица с коэффициентами

$$c_{jk} = \mathrm{Cov}\left(\xi_j, \xi_k\right)$$

Определение 3.10. Ковариация двух совместимых наблюдаемых A и $B, [A, B] = 0$, определяется по формуле

$$\mathrm{Cov}(A, B) = \mathrm{Tr}[\rho(A - \mathrm{Tr}(\rho A))(B - \mathrm{Tr}(\rho B))] \tag{3.48}$$

Определение 3.11. Матрицей ковариаций попарно совместимых наблюдаемых из множеств $\{A_j, 1 \leq j \leq N\}$ и $\{B_k, 1 \leq k \leq M\}, [A_j, B_k] == 0$, называется матрица с коэффициентами

$$c_{jk} = \mathrm{Cov}\left(A_j, B_k\right) \tag{3.49}$$

Утверждение (Б.С. Цирельсон, 1980 [23]). Существует пример квантовой матрицы ковариаций, которая не реализуется в классическом случае.

6.4 A.4

6.4.1 4.1. Composite Quantum Systems

До сих пор мы рассматривали квантовые системы, которым соответствовало фиксированное гильбертово пространство H. По этой причине мы обозначали множество состояний (положительных операторов с единичным следом) $\mathfrak{S}$ без указания H. Теперь для изучения составных квантовых систем, мы введём обозначение $\mathfrak{S}(H)$ для множества всех состояний в H. Напомним, что $\rho \in \mathfrak{S}(H)$ называется чистым, если $\rho = |\psi\rangle\langle\psi|, \psi \in H$. В противном случае состояние называется смешанным.

Определение 4.1. Пусть H, K - гильбертовы пространства, $\{e_j\}_{j=1}^{\infty} \subset\subset H, \{h_k\}_{k=1}^{\infty} \subset K$ - ортонормированные базисы в них. Тензорным произведением гильбертовых пространств $H \otimes K$ называется гильбертово пространство с ортонормированным базисом $\{e_j \otimes h_k\}$, так что скалярное произведение определяется на базисных векторах по формуле

$$\langle e_j \otimes h_k, e_{j'} \otimes h_{k'} \rangle = \delta_{jj'}\delta_{kk'},$$

и продолжается по линейности на всё пространство.

Определение 4.2. Пусть H, K - гильбертовы пространства, $H \times K == \{(e, h) \mid e \in H, h \in K\}$ - их декартово произведение. Назовём элементарными тензорами объекты вида $e \otimes h$, где $e \in H, h \in K$. Определим скалярное произведение на элементарных тензорах по формуле

$$\langle e \otimes h, \tilde{e} \otimes \tilde{h} \rangle_{H \otimes K} = \langle e, \tilde{e} \rangle_H \langle h, \tilde{h} \rangle_K$$

Тогда $\|x\| = \sqrt{(x, x)}$ - согласованная с этим скалярным произведением норма. Тензорным произведением гильбертовых пространств называется $H \otimes K = H \times K / \sim$, где элементы $x \sim y$ эквивалентны тогда и только тогда, когда $\|x - y\| = 0$.

Утверждение 4.1. Определения 4.1 и 4.2 эквивалентны.

Замечание 4.1. Не все элементы $H \otimes K$ являются элементарными тензорами.

Пусть двум квантовым системам соответствуют гильбертовы пространства H и K соответственно. Тогда составной системе, состоящей из двух подсистем отвечает тензорное произведение $H \otimes K$. Предположим, что чистое состояние составной системы задаётся элементарным тензором $e \otimes h \in H \otimes K$. Тогда первая система находится в чистом

состоянии $e \in H$, а вторая в чистом состоянии $h \in K$. Состояния $e \otimes h$ называются сепарабельными. Состояния не представимые в виде элементарного тензора называются сцепленными (entangled) чистыми состояниями. Из аксиом Макки следует, что кроме чистых состояний $|\psi\rangle\langle\psi|$ определены также смешанные состояния $\sum_j \pi_j |\psi_j\rangle \langle\psi_j|$. Смешанные состояния классифицируются на сепарабельные и сцепленные аналогично чистым. Более формально это важнейшее понятие определяется следующим образом.

Определение 4.3. Пусть $\rho \in \mathfrak{S}(H \otimes K)$ - состояние составной системы. Если существует наборы состояний $\{\rho_H^j\} \subset \mathfrak{S}(H)$ и $\{\rho_K^j\} \subset\subset \mathfrak{S}(K)$ и набор чисел $\{\pi_j\} \subset \mathbb{R}$ таких, что $\pi_j > 0, \sum_j \pi_j = 1$, и $\rho = \sum_j \pi_j \rho_H^j \otimes \rho_K^j$ (состояние ρ является выпуклой комбинацией состояний $\rho_H^j \otimes \rho_K^j$), то состояние ρ называется сепарабельным. В противном случае (если состояние ρ не представимо в таком виде) состояние ρ называется сцепленным.

Замечание 4.2. Существует много вариантов перевода слова entangled на русский язык. В физике существует традиция перевода прилагательными запутанное или перепутанное. В математике - сцепленное или зацепленное. Один из величайших физиков XX века Л.В. Келдыш переводил этот термин как переплетённое. Нельзя забывать, что entangled уже является переводом на английский язык с немецкого первоначального термина Verschräenkung, введённого Э. Шредингером.

Пример 4.1. Пусть обеим системам соответствует одно и то же гильбертово пространство

$H, \dim H = 2$ и $\{|\uparrow\rangle, |\downarrow\rangle\}$ - ортонормированный базис в H. Тогда составная система описывается гильбертовым пространством $H \otimes H$. Рассмотрим два состояния из $H \otimes H$:

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle|\downarrow\rangle - |\downarrow\rangle|\uparrow\rangle),$$
$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle|\uparrow\rangle + |\downarrow\rangle|\downarrow\rangle).$$

Эти состояния не представимы в виде элементарных тензоров, то есть являются сцепленными. В физике ψ_0 называется синглетным состоянием (спин равен нулю), а ψ_1 - триплетным (спин равен единице).

Определение 4.4. Пусть $T : H \to H$ и $S : K \to K$ - линейные ограниченные операторы в гильбертовых пространствах H и K соответственно. Тогда их тензорным произведением $T \otimes S$ называется

линейный оператор в $H \otimes K$, действующий на элементарные тензоры по формуле: $(T \otimes S)(e \otimes h) = Te \otimes Sh$ и далее продолжающийся на всё $H \otimes K$ по линейности. Элементарные тензоры $T \otimes S$ порождают алгебру всех линейных ограниченных операторов $B(H \otimes K)$ в гильбертовом пространстве тензорного произведения $H \otimes K$.

6.4.2 4.2. The State of Purification

Определение 4.5. Пусть $\{|\xi_k\rangle\langle\xi_s| \otimes |\eta_k\rangle\langle\eta_s|\}$ - базис в $B(H \otimes K)$, состоящий из операторов ранга один. Частичиым следом называется отображение $\mathrm{Tr}_K : \mathfrak{S}(H \otimes K) \to \mathfrak{S}(H)$, определённое на базисных элементах по формуле

$$\mathrm{Tr}_K\left(|\xi_k\rangle\langle\xi_s| \otimes |\eta_k\rangle\langle\eta_s|\right) = |\xi_k\rangle\langle\xi_s| \cdot \langle\eta_s, \eta_k\rangle. \tag{4.1}$$

На остальные элементы $B(H \otimes K)$ частичный след Tr_K продолжается по линейности.

Теорема 4.1. Пусть $\rho \in \mathfrak{S}(H)$. Тогда существует гильбертово пространство K и вектор $\psi \in H \otimes K$ такие, что $\rho = \mathrm{Tr}_K(|\psi\rangle\langle\psi|)$.

Доказательство. Используем спектральное разложение:

$$\rho = \sum_{j=1}^{N} \pi_j |\psi_j\rangle\langle\psi_j|,$$

где $\langle\psi_j, \psi_k\rangle = \delta_{jk}, \pi_j \geq 0, \sum_j \pi_j = 1$. Возьмём гильбертово пространство $K, \dim K = N$, с ортонормированным базисом $\{|j\rangle\}_{j=1}^N$. Положим $|\psi\rangle = \sum_j \sqrt{\pi_j}|\psi_j\rangle \otimes |j\rangle \in H \otimes K$. Заметим, что $\langle\psi, \psi\rangle = 1$. По определению частичного следа получаем:

$$\mathrm{Tr}_K(|\psi\rangle\langle\psi|) = \mathrm{Tr}_K\left(\sum_{j,k} \sqrt{\pi_j\pi_k}|\psi_j\rangle\langle\psi_k| \otimes |j\rangle\langle k|\right) =$$
$$= \sum_{j,k} \sqrt{\pi_j\pi_k} \cdot \langle j \mid k\rangle \cdot |\psi_j\rangle\langle\psi_k| == \sum_{j,k} \sqrt{\pi_j\pi_k} \cdot \delta_{jk} \cdot |\psi_j\rangle\langle\psi_k| = \sum_j \pi_j |\psi_j\rangle\langle\psi_j|.$$

Теорема 4.2. Пусть $\psi \in H \otimes K, \|\psi\| = 1$. Тогда существуют $\{e_j\} \subset\subset H, \{h_j\} \subset K$-ортонормированные базисы в H и K, а также набор чисел $\left\{\pi_j : \pi_j \geq 0, \sum_j \pi_j = 1\right\}$, так что справедливо разложение:

$$|\psi\rangle = \sum_j \sqrt{\pi_j}|e_j\rangle \otimes |h_j\rangle,$$

называемое разложением Шмидта состояния ψ.

Доказательство. Обозначим $\rho = \mathrm{Tr}_K(|\psi\rangle\langle\psi|)$. Рассмотрим спектральное разложение $\rho = \sum_{j=1}^N \pi_j |e_j\rangle \langle e_j|$, где $\langle e_j, e_k\rangle = \delta_{jk}, \pi_j \geq 0, \sum_j \pi_j = 1$. Поскольку $\{e_j \otimes e_k\}$ является ортонормированным базисом в $H \otimes K$, можно найти разложение $\psi = \sum_{j,k} \lambda_{jk} |e_j\rangle \otimes |e_k\rangle$. Определим h_j по формуле

$$|h_j\rangle = \frac{\sum_k \lambda_{jk} |e_k\rangle}{\sqrt{\sum_k |\lambda_{jk}|^2}} \tag{4.2}$$

Тогда $\|h_j\| = 1$, так что получается искомое разложение $|\psi\rangle = \sum_j \lambda_j |e_j\rangle \otimes \otimes |h_j\rangle$. Следовательно,

$$\sum_{j=1}^N \pi_j |e_j\rangle \langle e_j| = \rho = \mathrm{Tr}_K(|\psi\rangle\langle\psi|) = \sum_{j,k} \lambda_j \overline{\lambda_k} |e_j\rangle \langle e_k| \langle h_k, h_j\rangle . \tag{4.3}$$

Сравнивая полученные выражения, получаем $\langle h_j, h_k\rangle = \delta_{jk}, |\lambda_j|^2 == \pi_j$. Таким образом, $|\psi\rangle = \sum_j \sqrt{\pi_j} |e_j\rangle \otimes |h_j\rangle$.

Следствие 4.1. $\mathrm{Spect}\left(\mathrm{Tr}_K(|\psi\rangle\langle\psi|)\right) = \mathrm{Spect}\left(\mathrm{Tr}_H(|\psi\rangle\langle\psi|)\right)$.

Замечание. Физические условия накладывают дополнительные требования на состояния составной системы. Для бозонов требуется рассматривать симметризованное тензорное произведение $H \otimes_s K$, в то время как для фермионов - антисимметризованное $H \otimes_a K$. Также для фермионов нужно использовать правила суперотбора [18.

6.4.3 4.3. Tsirelson Boundary

Вернёмся к ковариационной матрице, введённой в п. 3.7 предыдущей лекции. Сразу следует отметить, что в квантовой теории для наблюдаемых $A_j, B_k \in \mathfrak{A}, \mathbb{E}_\psi(A_j) = \mathbb{E}_\psi(B_k) = 0$, имеет смысл рассматривать ковариационную матрицу:

$$c_{jk} = \mathbb{E}_\psi(A_j B_k)$$

только если наблюдаемые попарно коммутируют $[A_j, B_k] = 0$ (то есть измеримы одновременно).

Лемма 4.1. Пусть $X_k, Y_k \in \mathbb{R}, k = 1, 2, |X_k| \leq 1, |Y_k| \leq 1$. Тогда $|X_1Y_1 + X_1Y_2 + X_2Y_1 - X_2Y_2| \leq 2$.

Доказательство. Обозначим $M = |X_1Y_1 + X_1Y_2 + X_2Y_1 - X_2Y_2|$. Тогда

$$\begin{aligned} M &= |X_1(Y_1 + Y_2) + X_2(Y_1 - Y_2)| \leq |X_1|\,|Y_1 + Y_2| + |X_2|\,|Y_1 - Y_2| \leq \\ &\leq |Y_1 + Y_2| + |Y_1 - Y_2| \leq 2 \end{aligned}$$

Следствие 4.2. Для классических случайных величин X_k, Y_k таких, что $|X_k| \leq 1, |Y_k| \leq 1, k = 1, 2$, выполнено неравенство

$$-2 \leq \mathbb{E}(X_1Y_1 + X_1Y_2 + X_2Y_1 - X_2Y_2) \leq 2. \tag{4.4}$$

Замечание 4.3. Из следствия 4.2 вытекает, что коэффициенты классической ковариационной матрицы $c_{jk} = \mathbb{E}(X_jY_k)$ удовлетворяют соотношению

$$|c_{11} + c_{12} + c_{21} - c_{22}| \leq 2 \tag{4.5}$$

Условие на матрицу ковариаций (4.5) называется неравенством Белла-Клаузера-Хорна-Шимони.

Вопрос 4.1. Верно ли, что в случае квантовых случайных величин A_j, B_k с аналогичными свойствами как yX_j, Y_k для коэффициентов квантовой ковариационной матрицы $c_{jk} = \mathbb{E}_\psi (A_j B_k)$ выполняется неравенство (4.5)?

Ответ: Нет, это, вообще говоря, не так.

Пример 4.2. Рассмотрим гильбертово пространство $H, \dim H = 2$, описывающее состояние частицы со спином $\frac{1}{2}$. Базис в H естественно обозначить

$$|\uparrow\rangle = \begin{pmatrix}1\\0\end{pmatrix}, |\downarrow\rangle = \begin{pmatrix}0\\1\end{pmatrix}, \tag{4.6}$$

Введём наблюдаемую «удвоенная проекция спина на направление $\vec{a} == (a_x, a_y, a_z)$, которую обозначим $\sigma(\vec{a})$:

$$\sigma(\vec{a}) = a_x\sigma_x + a_y\sigma_y + a_z\sigma_z = \begin{pmatrix} a_z & a_x - ia_y \\ a_x + ia_y & -a_z \end{pmatrix} \tag{4.7}$$

где $\sigma_x, \sigma_y, \sigma_z$ - матрицы Паули:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{4.8}$$

Тогда

$$\langle\uparrow |\sigma(\vec{a})| \uparrow\rangle = a_z, \langle\downarrow |\sigma(\vec{a})| \downarrow\rangle = -a_z, \tag{4.9}$$

$$\langle\downarrow |\sigma(\vec{a})| \uparrow\rangle = a_x + ia_y, \langle\uparrow |\sigma(\vec{a})| \downarrow\rangle = a_x - ia_y. \tag{4.10}$$

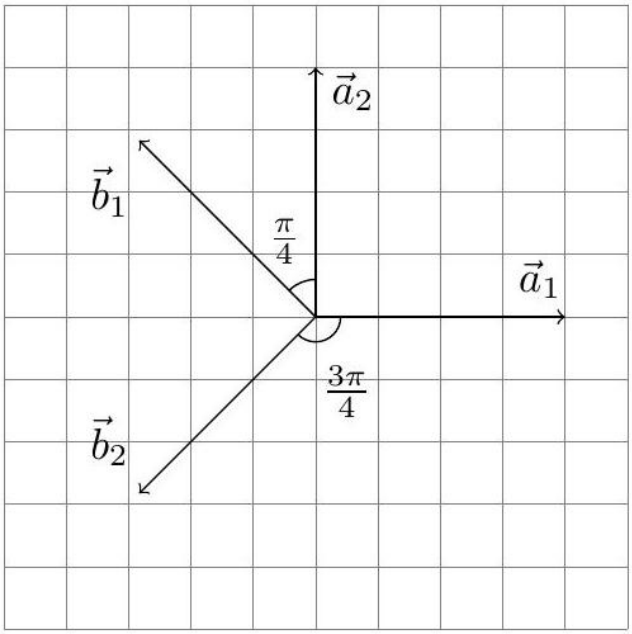
Теперь рассмотрим составную систему $H \otimes K, \dim H = \dim K = 2$. Будем считать, что гильбертовы пространства H и K описывают состояния двух систем со спином $\frac{1}{2}$. Тогда составная система $H \otimes K$ описывает состояние системы из двух фермионов, так что ортонормированный базис в ней будем обозначать $|\uparrow\uparrow\rangle, |\uparrow\downarrow\rangle, |\downarrow\uparrow\rangle, |\downarrow\downarrow\rangle$. Рассмотрим пару коммутирующих наблюдаемых $A = \sigma(\vec{a})\otimes \mathrm{I}$ и $B = \mathrm{I}\otimes\sigma(\vec{b})$, отвечающих паре произвольных векторов $\vec{a}$ и $\vec{b}$. Пусть система находится в синглетном состоянии:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle).$$

Тогда из (4.9) и 4.10 немедленно вытекает, что

$$E_\psi(A) = E_\psi(B) = 0, \mathrm{Var}_\psi(A) = \mathrm{Var}_\psi(B) = 1 \tag{4.11}$$

$$\langle\psi|AB|\psi\rangle = -\vec{a}\vec{b} \tag{4.12}$$



Зададим направления $\overrightarrow{a_j}, \overrightarrow{b_k}$ так, как это указано на рисунке. Тогда для коэффициентов ковариационной матрицы получаем

$$c_{11} + c_{12} + c_{21} - c_{22} = 2\sqrt{2}.$$

Теорема 4.3 (Б.С. Цирельсон, 1980 [23]). Пусть операторы A_k, B_k ($k = 1, 2$) таковы, что

$$A_k^2 = B_k^2 = I, [A_k, B_j] = 0, \{A_k, A_j\} = \{B_k, B_j\} = c \cdot I, \tag{4.13}$$

$$-I < A_k \leq I, \quad -I < B_k \leq I. \tag{4.14}$$

Тогда $\mathbb{E}\left(A_1B_1 + A_2B_1 + A_1B_2 - A_2B_2\right) \leq 2\sqrt{2}$. Величина $2\sqrt{2}$ называется границей Цирельсона.

Замечание 4.4. Здесь $[\cdot,\cdot]$ - коммутатор, $\{\cdot,\cdot\}$ - антикоммутатор. Неравенство $A < I$ означает, что $I - A > 0$, то есть оператор $I - A$ положительный. Для любого оператора A выполнено неравенство $A << \|A\|I$, следовательно сравнение с I корректно.

Ниже дано доказательство из [23]. Более изящное доказательство приведено в 16 .

Доказательство. Обозначим $M = A_1B_1 + A_2B_1 + A_1B_2 - A_2B_2$. Тогда

$$M = \frac{1}{\sqrt{2}}\left(A_1^2 + A_2^2 + B_1^2 + B_2^2\right) -$$

$$-\frac{\sqrt{2}-1}{8}\left\{\left(\left(\sqrt{2}+1\right)\left(A_1 - B_1\right) + A_2 - B_2\right)^2 +\right.$$

$$+\left(\left(\sqrt{2}+1\right)\left(A_1 - B_2\right) - A_2 - B_1\right)^2 +$$

$$\left.+\left(\left(\sqrt{2}+1\right)\left(A_2 + B_2\right) - A_1 - B_1\right)^2\right\} \leq$$

$$\leq \frac{1}{\sqrt{2}}\left(A_1^2 + A_2^2 + B_1^2 + B_2^2\right) \leq \frac{4}{\sqrt{2}} = 2\sqrt{2}$$

Замечание. Выше мы показали, что граница Цирельсона достигается на синглетном состоянии в задаче о системе двух частиц со спином $\frac{1}{2}$.

6.5 A.5

6.5.1 5.1. Eigenfunctions and Eigenvalues of the Fourier Transform

Рассмотрим преобразование Фурье, определённое для функций $\psi \in\in L^1(\mathbb{R})$ формулой

$$\mathcal{F}[\psi](y) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} e^{-ixy}\psi(x)dx \tag{5.1}$$

Действие $\mathcal{F}$ можно продолжить на функции из пространства $L^2(\mathbb{R})$, что будет частным случаем того, что мы получим в этом пункте. Рассмотрим операторы рождения и уничтожения, введённые нами при рассмотрении задачи о квантовом гармоническом осцилляторе:

$$a = \frac{q + ip}{\sqrt{2}}, a^+ = \frac{q - ip}{\sqrt{2}}.$$

Из 5.1 следует, что

$$\mathcal{F} \circ q = -p \circ \mathcal{F}, \mathcal{F} \circ p = q \circ \mathcal{F} \tag{5.2}$$

Таким образом, выполнено тождество

$$\mathcal{F} \circ a = ia \circ \mathcal{F} \tag{5.3}$$

Тем самым решение уравнения

$$a|0\rangle = 0$$

является неподвижной точкой преобразования Фурье:

$$\mathcal{F}|0\rangle = |0\rangle \tag{5.4}$$

Действительно, уравнение (5.4) имеет единственное нормированное решение:

$$\langle x \mid 0\rangle = \frac{1}{\pi^{\frac{1}{4}}} \exp\left(-\frac{x^2}{2}\right),$$

называемое основиым состоянием квантового гармонического осциллятора. Таким образом, тождество (5.3) гарантирует, что это неподвижная точка преобразования Фурье. Ниже мы покажем, что это
единственная (нормированная) неподвижная точка $\mathcal{F}$. Аналогично, поскольку

$$a|\alpha\rangle = \alpha|\alpha\rangle$$

для когерентных состояний осциллятора $|\alpha\rangle, \alpha \in \mathbb{C}$, с волновыми функциями

$$\langle x \mid \alpha\rangle = \frac{1}{\pi^{1/4}} \exp\left(-\frac{(x - \sqrt{2}\,\mathrm{Re}(\alpha))^2}{2} + i\sqrt{2}\,\mathrm{Im}(\alpha)x\right)$$

получаем

$$\mathcal{F}|\alpha\rangle = -i\alpha| - i\alpha\rangle,$$

$\alpha \in \mathbb{C}$. Отметим, что отсюда немедленно получается, что

$$\mathbb{E}_{|\alpha\rangle}(q) = \mathbb{E}_{|\alpha\rangle}(p) = 0$$
$$\mathrm{Var}_{|\alpha\rangle}(q) = \mathrm{Var}_{|\alpha\rangle}(p) = \frac{1}{2}$$

что минимизирует соотношение неопределённостей:

$$\mathrm{Var}_\rho(q)\,\mathrm{Var}_\rho(p) \geq \frac{1}{4}$$

Рассмотрим возбуждённые состояния осциллятора:

$$|n\rangle = \frac{(a^+)^n}{\sqrt{n!}}|0\rangle, n = 1, 2, 3, \ldots \tag{5.5}$$

Теорема 5.1. Система основного и возбуждённых состояний осциллятора образует полную систему собственных функ,ий преобразования Фурье:

$$\mathcal{F}|n\rangle = (-i)^n|n\rangle, n = 0, 1, 2, \ldots \tag{5.6}$$

Замечание 5.1. Из теоремы 5.1 следует, что основное состояние осциллятора является единственной неподвижной точкой преобразования Фурье.
Замечание 5.2. Поскольку система собственных векторов $\mathcal{F}$ образует ортонормированный базис в $L^2(\mathbb{R})$, преобразование Фурье $\mathcal{F}$, заданное первоначально формулой (5.1), корректно заданной в $L^1(\mathbb{C})$, можно продолжить до преобразования функций из пространства $L^2(\mathbb{R})$. Более того, справедливо равенство Парсеваля:

$$\|\mathcal{F}(\psi)\|_{L^2(\mathbb{R})} = \|\psi\|_{L^2(\mathbb{R})}$$

Доказательство. Из (5.2) следует, что

$$\mathcal{F} \circ a^+ = -ia^+ \circ \mathcal{F}.$$

Таким образом, из (5.5) вытекает выполнение (5.6). Поскольку система из основного и возбуждённых состояний образует ортонормированный базис в $L^2(\mathbb{R})$, заключаем, что мы полностью описали спектр преобразования Фурье. □

6.5.2 5.2. The Action of a Group of Unitary Operators Associated with a QHO on Canonical Observables

Рассмотрим чистое состояние $\rho = |\psi\rangle\langle\psi| \in \mathfrak{S}$ и $A \in \mathfrak{A}$ - наблюдаемая в гильбертовом пространстве H, обладающая циклическим вектором $\psi_0 \in H$ (замыкание линейных комбинаций $A^n\psi_0$ порождают всё H). Тогда, согласно теореме 2.4, паре ($|\psi\rangle, A$) отвечает волновая функция $\psi_A(x)$. Для операторов координаты q и импульса p функция

$$\psi_0(x) = \frac{1}{\pi^{\frac{1}{4}}} \exp\left(-\frac{x^2}{2}\right)$$

(основное состояние квантового гармонического осциллятора) является циклическим вектором. В случае, когда $A = q$ или p, говорят, что $\psi_q(x)$ и $\psi_p(x)$ - волновые функции состояния в координатном и импульсном представлении соответственно.

Волновые функции в координатном и импульсном представлении связаны преобразованием Фурье:

$$\psi_p(y) = \mathcal{F}\left[\psi_q\right](y) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} e^{-ixy}\psi_q(x)dx. \tag{5.7}$$

Как уже было подмечено (вопрос 1.1, знание $|\psi_q|^2$ и $|\psi_p|^2$ не позволяет восстановить состояние ψ.

Вопрос 5.1. Сколько наблюдаемых A необходимо взять, чтобы по квадратам модулей $|\psi_A(x)|^2$ можно было восстановить состояние ψ ?

Утверждение ([33]). Достаточно знать $|\psi_A(x)|^2$ для всех наблюдаемых вида $A = \cos\varphi \cdot q + \sin\varphi \cdot p$, где $\varphi \in [0, \pi]$.

Обозначим $H = \frac{q^2+p^2}{2}$ гамильтониан квантового гармонического осциллятора. Заметим, что оператор H - самосопряженный, следовательно, следовательно к нему применима спектральная теорема и для функции $f_\varphi(x) = \exp(-i\varphi x)$ корректно определён оператор $f_\varphi(H) == \exp(-i\varphi H)$, который является унитарным в силу того, что $\mathrm{Spect}\,(f_\varphi(H)) = f_\varphi(\mathrm{Spect}(H)) = \{e^{i\varphi x}, x \in \mathbb{R}\}$ в силу теоремы об отображении спектра. Нам будет удобно определить семейство унитарных операторов формулой

$$U_\varphi = e^{\frac{i}{2}\varphi} f_\varphi(H), \tag{5.8}$$

поскольку в этом случае $U_{\frac{\pi}{2}} = \mathcal{F}$ совпадает с преобразованием Фурье.

Замечание 5.3. Из определения U_φ следует $U_{\varphi_1+\varphi_2} = U_{\varphi_1}U_{\varphi_2}$, то есть $\{U_\varphi\}$ - однопараметрическая подгруппа в группе всех унитарных операторов. Отметим, что для любого $f \in H$ последовательность $U_{\varphi+\delta}f$
$\to U_\varphi f$ при $\delta \to 0$, что называется непрерывностью орбит в смысле сильной операторной топологии.

Теорема 5.2.

$$U_\varphi q U_\varphi^* = \cos\varphi q + \sin\varphi p,$$
$$U_\varphi p U_\varphi^* = -\sin\varphi q + \cos\varphi p,$$

$t \in \mathbb{R}$.

Доказательство. Коммутатор операторов координаты q и импульса p равен

$$[q, p] = qp - pq = i \tag{5.9}$$

Используя (5.9), вычислим

$$\left[q^2, p\right] = q^2p - pq^2 = q^2p - (qp - i)q = q^2p + iq - q(qp - i) = 2iq. \tag{5.10}$$

Аналогичным образом

$$\left[p^2, q\right] = -2ip \tag{5.11}$$

Отметим, что в общем случае

$$[f(q), p] = if'(q), [f(p), q] = -if'(p) \tag{5.12}$$

для аналитической функции f.

Обозначим

$$\Delta_\varphi = U_\varphi p U_\varphi^* = \exp(i\varphi H) q \exp(-i\varphi H). \tag{5.13}$$

Тогда

$$\Delta'_\varphi\big|_{\varphi=0} = i(Hp - pH) = i[H, p] = -q. \tag{5.14}$$

Из группового свойства $U_{\varphi_1+\varphi_2} = U_\varphi U_\varphi$ следует, что Δ_φ удовлетворяет дифференциальному уравнению

$$\frac{d}{d\varphi}\Delta_\varphi = i\,[H, \Delta_\varphi] \tag{5.15}$$

называемому уравнением Лиувилля-фон Неймана. Поставим для уравнения (5.15) начальное условие Коши:

$$\Delta_0 = q \tag{5.16}$$

Будем искать решение задачи (5.15) - (5.16) в виде

$$\Delta_\varphi = \alpha(\varphi) \cdot q + \beta(\varphi) \cdot p \tag{5.17}$$

Подставляя (5.17) в уравнение (5.15) и принимая во внимание (5.10) и (5.11) получаем

$$\alpha''(\varphi) = -\beta(\varphi), \quad \beta''(\varphi) = \alpha(\varphi), \tag{5.18}$$

$$\alpha(0) = 1, \quad \beta(0) = 0. \tag{5.19}$$

Решая систему (5.18) - (5.19) получаем $\alpha(\varphi) = \cos(\varphi), \beta(\varphi) = \sin(\varphi)$. Действие на оператор импульса p получается аналогичным образом.

Замечание 5.4. Можно показать, что действие унитарного оператора $U_\varphi = \exp(i\varphi H), \varphi \neq 0$, представимо в виде интегрального оператора

$$(U_\varphi \psi)(x) =$$

$$= \frac{1}{\sqrt{2\pi|\sin\varphi|}} \exp\left(\frac{i\cos\varphi \cdot x^2}{2\sin\varphi}\right) \int_{-\infty}^{+\infty} \exp\left(\frac{i\cos\varphi \cdot y^2}{2\sin\varphi} - \frac{ixy}{\sin\varphi}\right) \psi(y) dy \tag{5.20}$$

$\psi \in L^1(\mathbb{R})$.

Замечание 5.5. В силу группового свойства $U_{\varphi_1+\varphi_2} = U_{\varphi_1} U_{\varphi_2}$ получаем

$$\left(U_{\frac{\pi}{2n}}\right)^n = U_{\frac{\pi}{2}} = \mathcal{F}$$

то есть преобразование $U_{\frac{\pi}{2n}}$ является корнем n-й степени из преобразования Фурье $\mathcal{F}$. По этой причине группа $\{U_\varphi\}$ называется дробным преобразованием Фурье 40. Поскольку основное и возбуждённые состояния осциллятора являются полной системой собственных функций гамильтониана H, получаем

$$U_\varphi \left| n \right> = e^{i\varphi n} \left| n \right>, n = 0, 1, 2, \ldots \tag{5.21}$$

6.5.3 5.3. A Family of Unitary Transformations of Canonical Observables

Определим модифицированные операторы координаты и импульса:

$$q_{\mu,\nu} = \mu \cdot q - \nu \cdot p$$

$$p_{\mu,\nu} = \nu \cdot q + \mu \cdot p$$

$\mu, \nu \in \mathbb{R}$. Отметим, что, поскольку для исходных операторов $[q, p] = i$, модифицированные операторы удовлетворяют соотношению

$$[q_{\mu,\nu}, p_{\mu,\nu}] = i\left(\mu^2 + \nu^2\right)$$

Определение 5.1. Для фиксированных $\mu, \nu \in \mathbb{R}, \nu \neq 0$, определим интегральное преобразование $\mathcal{F}_{\mu,\nu}$ в пространстве $L^1(\mathbb{R})$ формулой

$$\mathcal{F}_{\mu,\nu}[\psi](x) = \frac{1}{\sqrt{2\pi|\nu|}} \exp\left(\frac{i\mu x^2}{2\nu}\right) \int_{-\infty}^{+\infty} \exp\left(\frac{i\mu y^2}{2\nu} - \frac{ixy}{\nu}\right) \psi(y)dy \tag{5.22}$$

Замечание 5.6. Поскольку преобразование (5.22) является композицией преобразования Фурье и оператора умножения на функцию с единичном модулем, оно продолжается на пространство $L^2(\mathbb{R})$ и сохраняет норму

$$\|\mathcal{F}_{\mu,\nu}(\psi)\|_{L^2(\mathbb{R})} = \|\psi\|_{L^2(\mathbb{R})}$$

Лемма 5.1.

$$\mathcal{F}_{\mu,\nu} \circ q = q_{\mu,\nu} \circ \mathcal{F}_{\mu,\nu}$$
$$\mathcal{F}_{\mu,\nu} \circ p = p_{\mu,\nu} \circ \mathcal{F}_{\mu,\nu}$$

Доказательство. Докажем первое тождество.

$$(\mu q + \nu p) \circ \mathcal{F}_{\mu,\nu}[\psi](x) =$$
$$= \frac{1}{\sqrt{2\pi|\nu|}} \exp\left(\frac{i\mu x^2}{2\nu}\right) \int_{-\infty}^{+\infty} \exp\left(\frac{i\mu y^2}{2\nu} - \frac{ixy}{\nu}\right) (\mu x - \mu x + y)\psi(y)dy$$

Второе тождество доказывается аналогично.

6.6 A.6

6.6.1 6.1. The Task of Error- Free Coding

Будем характеризовать классический канал связи неориентированным графом, в котором вершины изображают передаваемую информацию, а рёбра - искажение информации. Если вершины u и v соединены ребром, тогда при передаче v может быть получено u вместо v и при передаче u может быть получено v вместо u.

Задача 6.1. Какое кодирование нужно использовать, чтобы после передачи информации её можно было безошибочно декодировать?

Пример 6.1. Рассмотрим граф G с множеством вершин:

$$V = \{A, B, C, D\}$$

и множеством рёбер:

$$E = \{(A, B), (C, D), (D, E)\}$$

В графе G возможны следующие искажения при передаче информации: $A \to B, B \to A, C \to D, D \to C, D \to E$ и $E \to D$. Если использовать для кодирования вершины A и E, то по полученному сообщению можно однозначно восстановить отправленное, поскольку множества вершин $[A]$ и $[B]$, в которые могут перейти сообщения A и B, не пересекаются. С другой стороны, если использовать для кодирования A, C и E, отправленная информация не всегда восстанавливается

однозначно, поскольку при получении D нельзя достоверно заключить, было ли отправлено E или C.

Набор вершин, которые можно использовать для безошибочной передачи информации называется антикликой.

6.6.2 6.2. Encoding of Quantum Information

Носителем квантовой информации является набор состояний $\psi \in H$. По аналогии с классическим случаем, можно считать, что вершинами «графа», отвечающего каналу связи, являются состояния $\psi_k \in H$, $k \in \overline{1,N}$. Тогда рёбрами такого «графа» (ошибками) следует считать унитарные операторы $\psi_k \mapsto U\psi_k$. Обозначим множество «ошибок» $\mathcal{U}$. В силу того, что вершины, соединённые ребром, могут переходить друг в друга по условию, получаем требование $U \in \mathcal{U}$, которое влечёт $U^* \in \mathcal{U}$. Обязательно нужно предполагать, что искажение может

и не происходить. Следовательно, $I \in U$. Конечно, приведённые выше соображения не являются точными определениями и нужны только для того, чтобы вызвать удобные ассоциации.

Определение 6.1. Линейное пространство $\mathcal{V}$, состоящее из ограниченных операторов в гильбертовом пространстве H, называется некоммутативным операторным графом, если выполнены следующие условия:

1. если оператор $A \in \mathcal{V}$, тогда $A^* \in \mathcal{V}$;
2. тождественный оператор $I \in \mathcal{V}$.

Замечание 6.1. Определение некоммутативного операторного графа в контексте квантовой теории информации было дано в [27]. На самом деле, в функциональном анализе некоммутативные операторные графы известны под названием операторных систем [22. Более полное обсуждение теории квантовьх кодов, исправляющих ошибки можно найти в 15,16 .

Теорема 6.1 ([26]). В кочечномерном гильбертовом пространстве $\mathcal{V}$ является некоммутативным операторным графом тогда и только тогда, когда существует набор операторов $M_j \in \mathcal{V}, M_j > 0, \sum_j M_j == I$, такой, что $\mathcal{V} = \operatorname{span}\{M_j\}$.

Доказательство. Пусть $\mathcal{V} = \operatorname{span}\{M_j\}$. Тогда все свойства из определения некоммутативного операторного графа выполнены.

Пусть, наоборот, $\mathcal{V}$ - некоммутативный операторный граф. Тогда, в силу свойства 1 из определения графа, в $\mathcal{V}$ существует базис из самосопряженных операторов. Такой базис будет состоять из конечного числа элементов в силу конечномерности гильбертова пространства H. Поскольку $\mathrm{I}+\frac{A}{\|A\|} > 0$ для любого самосопряженного оператора A, можно построить базис с нужными свойствами S.

Определение 6.2. Проектор P в H такой, что $\dim(PH) \geq 2$, называется антикликой для некоммутативного операторного графа $\mathcal{V}$, если $\dim(P\mathcal{V}P) = 1$, то есть для любого $X \in \mathcal{V}$ выполнено $PXP = \lambda P$, где $\lambda \in \mathbb{C}$.

Замечание 6.2. Обозначим $H_P = PH$. Пусть $\{\xi_j\}$ - ортонормированный базис в H_P. Тогда выполнены следующие свойства:

$$\langle \xi_j, X\xi_j \rangle = \langle \xi_k, X\xi_k \rangle \quad \forall j,k \forall X \in \mathcal{V}; \tag{6.1}$$

$$\langle \xi_j, X\xi_k \rangle = 0 \quad \forall j \neq k \forall X \in \mathcal{V}. \tag{6.2}$$

Замечание 6.3. Если $U \in \mathcal{U}$ - унитарный оператор, то для ортонормированного базиса $\{\xi_j\}$ выполнено $U\xi_k \perp \xi_j$.
Следствие. Состояния $\{\xi_j\}_{j=1}^{\dim P}$ можно выбрать для кодирования информации.

Основы излагаемой теории заложены в [36]. Следует также упомянуть пионерскую работу 43 .
Пример 6.2. Пусть $H = \mathbb{C}^2$ - кубит и унитарные операторы, порождающие граф (ошибки), - матрицы Паули:

$$\sigma_0 = I, \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{6.3}$$

Опишем физический смысл ошибок. Матрица σ_x отвечает перевороту направления спина (flip): $|\uparrow\rangle \mapsto |\downarrow\rangle, |\downarrow\rangle \mapsto |\uparrow\rangle$. Матрица σ_z отвечает сдвигу по фазе на π (phase shift): $|\uparrow\rangle \mapsto |\uparrow\rangle, |\downarrow\rangle \mapsto -|\downarrow\rangle$. Матрица σ_y представляет собой композицию переворота и сдвига по фазе. Код Шора [43 строится из девяти кубитов и способен исправить произвольную ошибку, осуществляемую матрицами Паули, которая воздействует на один из них. Такая ситуация неудивительна, поскольку построенный код вкладывается в общую теорию 36 .
Утверждение 6.1. Если $\dim \mathcal{V} = (\dim H)^2$, то есть $\mathcal{V}$ - алгебры всех матриц, то не существует антиклики P.
Утверждение 6.2. Если $\mathcal{V}$ - максимальная коммутативная подалгебра, то не существует антиклики P.
Теорема 6.2. Пусть $\dim \mathcal{V} \cdot (\dim \mathcal{V} + 1) \leq \frac{\dim H}{\operatorname{rank} P}$, тогда существует антиклика P размерности $\operatorname{rank} P$.

Доказательство. Используется обобщённая теорема Радона 37 .
Пример 6.3. Рассмотрим двухкубитное пространство $H = \mathbb{C}^2 \otimes \mathbb{C}^2$ и пространство ошибок $\mathcal{V} = \operatorname{span}\{I, T, U, V, W\}$, где $T = \sigma_x \otimes I$, $U = \sigma_y \otimes I, V = I \otimes \sigma_y, W = I \otimes \sigma_z$.

Положим

$$f_+ = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad f_- = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ -1 \end{pmatrix}. \tag{6.4}$$

Тогда

$$\langle f_\pm, X f_\pm \rangle = \langle f_\mp, X f_\pm \rangle = 0 \tag{6.5}$$

Следовательно, проектор P на подпространство $H_P = PH = \{\mathbb{C} f_\pm\}$ – антиклика для $\mathcal{V}$.

6.6.3 6.3. Covariant Positive Operator - Valued Measures

Рассмотрим локально-компактную хаусдорфову топологическую группу G и σ-кольцо $\mathcal{B}(G)$, порождённое её компактными подмножествами. Фиксируем гильбертово пространство H и обобщим определение 3.1 меры на действительной прямой.

Определение 6.3. Отображение $M : \mathcal{B}(G) \to B(H)$ называется положительной операторозначной мерой на группе G :

1. $M(B) \geq 0$ - положительный оператор для любого $B \in \mathcal{B}(G)$;
2. $M(\emptyset) = 0$ - нулевой оператор, $M(G) = \mathrm{I}$ - тождественный оператор;
3. $M\left(\bigcup_j B_j\right) = \sum_j M(B_j)$, если множества $B_j \cap B_k = \emptyset$ для любых $j \neq k$, где сходимость операторного ряда понимается в смысле сильной операторной топологии.

Пример 6.4. Согласно теореме 6.1 для некоммутативного операторного графа $\mathcal{V}$ в конечномерном гильбертовом пространстве найдётся базис $\{M_j, 0 \leq j \leq N\}$, состоящий из положительных операторов $M_j > 0$, образующих разложение единицы $\sum_{j=0}^{N-1} M_j = I$, таких, что $\mathcal{V} = \mathrm{span}\,\{M_j, 0 \leq j \leq N\}$. Рассмотрим циклическую группу

$$\mathbb{Z}_{\mathbb{N}} = \{0, 1, \ldots, N-1\}$$

и определим отображение на G по формуле

$$M(\{j\}) = M_j, 0 \leq j \leq N \tag{6.6}$$

Тогда (6.6) естественным образом продолжается до положительной операторозначной меры на G.

Пусть, теперь $G \nu g \rightarrow U_g$ - проективное унитарное представление группы G в гильбертовом пространстве H.

Определение 6.4. Положительная операторозначная мера $\{M(B),\ B \in \mathcal{B}(G)\}$ называется ковариантной относительно действия $\{U_g, g \in \in G\}$, если

$$U_g M(B) U_g^* = M(gB, g \in G, B \in \mathcal{B}(G)$$

Теорема 6.3 ([13]). Пусть G - локально-компактная группа с мерой Хаара ν, гильбертово пространство H конечномерно u

$$\{M(B), B \in \mathcal{B}(G)\}$$

- положительная операторозначная мера, ковариантная относительно $\{U_g, g \in G\}$. Тогда в H найдётся такой оператор $M_0 > 0$, что

$$M(B) = \int_B U_g M_0 U_g^* d\nu(g), \quad B \in \mathcal{B}(G)$$

Циклическую группу $\mathbb{Z}_N$ можно рассматривать как подгруппу максимальной коммутативной группы вращений единичной окружности $\mathbb{T}$. При этом элементы $\mathbb{Z}_N$ можно рассматривать как повороты на углы $\frac{2\pi j}{N}, 0 \leq j \leq N-1$. Пример 6.4 может быть расширен следующим образом:

Пример 6.5 ([19]). Зададим унитарное представление группы вращений $\mathbb{T} = \{\varphi, \varphi \in [0, 2\pi]\}$ в гильбертовом пространстве $H = \mathbb{C}^2 \otimes \mathbb{C}^2$. Определим ортогональные проекторы P_0 и P_1 по формулам

$$P_0 = \frac{1}{2}(|00\rangle + |11\rangle >)(\langle 00| + \langle 11|) + \frac{1}{2}(|01\rangle + |10\rangle)(\langle 01| + \langle 10|), \tag{6.7}$$

$$P_1 = \frac{1}{2}(|00\rangle - |11\rangle >)(\langle 00| - \langle 11|) + \frac{1}{2}(|01\rangle - |10\rangle)(\langle 01| - \langle 10|) \tag{6.8}$$

и положим

$$U_\varphi = P_0 + e^{i\varphi} P_1, \varphi \in \mathbb{T}$$

Определим проектор Q формулой

$$Q = |00\rangle\langle 00| + |01\rangle\langle 01| \tag{6.9}$$

тогда некоммутативный операторный граф

$$\mathcal{V} = \text{span}\left\{U_\varphi Q U_\varphi^*, \varphi \in \mathbb{T}\right\}$$

имеет антиклики P_0 и P_1 ранга 2 .

С другой стороны, циклическая группа $\mathbb{Z}_N$ вкладывается в дискретную некоммутативную группу Гейзенберга-Вейля G_2, которая для $N = 4$ сводится к группе, порождённой матрицами Паули.

Пример 6.6 ([20]). Операторы, кратные единичному, I, -I, iI, -iI вместе с матрицами Паули (6.3) образуют группу относительно операции умножения. Обозначим эту группу G_2. Определим приводимое унитарное представление G_2 в гильбертовом пространстве $H = \mathbb{C}^2 \otimes \mathbb{C}^2$ по формуле

$$U_{mI} = mI, m \in \{1, -1, i, -i\},$$
$$U_{\sigma_x} = |00\rangle\langle 11| + |11\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01|,$$
$$U_{\sigma_z} = |00\rangle\langle 00| - |11\rangle\langle 11| + |01\rangle\langle 01| - |10\rangle\langle 10|.$$

Представление для σ_y определяется условием: $\sigma_y = i\sigma_z\sigma x$. Возьмём тот же проектор (6.9) и определим некоммутативный операторный граф формулой

$$\mathcal{V} = \text{span}\left\{U_g Q U_g^*, g \in G_2\right\}.$$

Антикликами для него являются те же проекторы P_0 и P_1, что в предыдущем примере (6.7) - 6.8.

6.7 A.7

6.7.1 7.1. Classical and Quantum Random Processes (!!!!)

Целью лекции будет рассказ о том, как классические винеровский и пуассоновский случайные процессы вкладываются в симметричное (бозонное) пространство Фока. Что касается винеровского процесса, идеология такого вложения следует разложению Винера-Ито пространства L^2-функционалов от броуновского движения [12. Вложение пуассоновского процесса было предложено в пионерской работе 32 .

Всюду ниже T обозначено одно из множеств $\mathbb{R}, \mathbb{R}_+, \mathbb{Z}$ или $\mathbb{Z}_+$.

Определение 7.1. Однопараметрическое множество случайных величин $\{\xi_t, t \in T\}$ называется (классическим) случайным процессом, если задано совместное распределение вероятностей:

$$\Pr\left(\xi_{t_1} \in B_1, \ldots, \xi_{t_n} \in B_n\right)$$

для любого выбора индексов $t_j \in T$ и подмножеств $B_j \in \mathcal{B}(\mathbb{R})$.

Определение 7.2. Процесс $\{\xi_t, t \in T\}$ называется случайным процессом с независимыми приращениями, если случайные величины $\xi_{t_1} - \xi_{s_1}$ и $\xi_{t_2} - \xi_{s_2}$ независимы при любом выборе непересекающихся интервалов $(s_1, t_1) \cap (s_2, t_2)$.

Пример 7.1. Случайный процесс с независимыми приращениями $\{\xi_t, t \in \mathbb{R}_+\}$называется винеровским, если $\xi_t - \xi_s \in \mathcal{N}(0, t-s)), s < t$, то есть распределение вероятностей $\xi_t - \xi_s$ является гауссовским:

$$\Pr\left(\xi_t - \xi_s \in B\right) = \frac{1}{\sqrt{2\pi(t-s)}} \int_B \exp\left(-\frac{x^2}{2(t-s)}\right) dx$$

$s < t, B \in \mathcal{B}\left(\mathbb{R}_+\right)$.

Пример 7.2. Случайный процесс с независимыми приращениями $\{\xi_t, t \in \mathbb{R}_+\}$называется

пуассоновским, если $\xi_t - \xi_s \in \mathcal{P}(t-s), s < t$, то есть распределение вероятностей $\xi_t - \xi_s$ является пуассоновским:

$$\Pr\left(\xi_t - \xi_s = k\right) = e^{-t+s}\frac{(t-s)^k}{k!},$$

$s < t, k = 0, 1, 2, \ldots$

Определение классических случайных процессов с независимыми приращениями может быть перенесено на квантовый случай в следующей форме:

Определение 7.3. Пара $(\ \{X_t, t \in T\}, \rho\ )$, состоящая из семейства наблюдаемых $X_t \in \mathfrak{A}$ и состояния $\rho \in \mathfrak{S}$, называется квантовым случайным процессом с независимыми приращениями, если приращения процесса $X_{st} = X_t - X_s$ коммутируют (наблюдаемые совместимы):

$$[X_{s_1t_1}, X_{s_2t_2}] = 0$$

для непересекающихся интервалов $(s_1, t_1) \cap (s_2, t_2) = \emptyset$ и классические случайные величины $\xi_{s_jt_j}$ с совместным распределением, определяемым формулой (см. определение 3.15:

$$\Pr\left(\xi_{s_1t_1} \in B_1, \ldots, \xi_{s_nt_n} \in B_n\right) = \mathrm{Tr}\left(\rho E_1\left(B_1\right)\ldots E_n\left(B_n\right)\right)$$

где (E_j) - проекторозначные меры, отвечающие наблюдаемым $(\ X_{s_jt_j}\ )$, независимы.

6.7.2 7.2. Symmetric Fock Space

Рассмотрим тензорное произведение $H^{\otimes^n}$, состоящее из n копий гильбертова пространства H. Скалярное произведение в $H^{\otimes^n}$ задаётся на элементарных тензорах формулой

$$\langle f_1 \otimes \cdots \otimes f_n, g_1 \otimes \cdots \otimes g_n\rangle_{H^{\otimes^n}} = \prod_{j=1}^{n}\langle f_j, g_j\rangle_H$$

$f_j, g_j \in H$, и продолжается затем на всё пространство по линейности.
Определим ортогональный проектор $P_s : H^{\otimes^n} \to H^{\otimes^n}$ по формуле

$$P_s e_1 \otimes e_2 \otimes \cdots \otimes e_n = \frac{1}{n!}\sum_{s\in S} e_{s(1)} \otimes \cdots \otimes e_{s(n)},$$

где суммирование ведётся по множеству S, состоящему из всех перестановок множества $\{1, \ldots, n\}$ и $e_j \in H$.
Определение 7.4. Подпространство $H^{\otimes_s^n} = P_s H^{\otimes^n}$ называется симметризованным тензорным произведением n копий пространства H.

Определение 7.5. Гильбертово пространство:

$$F(H) = \{\mathbb{C}\Omega\} \oplus \bigoplus_{n=1}^{+\infty} H^{\otimes_s^n}$$

называется симметричным (бозонным) пространством Фока. Фиксированный вектор Ω называется вакуумным, пространство H - одночастичным, а пространства $H^{\otimes_s^n}$ – n-частичными.

Ранее мы рассматривали модель квантового гармонического осциллятора. Нашей целью теперь будет построение модели бесконечного множества квантовых гармонических осцилляторов в гильбертовом пространстве $F(H)$. Модель, которую мы построим, будет

сводится к единичному осциллятору, когда $\dim H = 1$. Следующее определение даёт аналог когерентных состояний для $F(H)$.

Определение 7.6. Для $f \in H$ элемент $e(f) \in F(H)$, определяемый формулой

$$e(f) = \sum_{n=0}^{+\infty} \frac{f^{\otimes^n}}{\sqrt{n!}},$$

называется экспоненицальным вектором.

Непосредственно проверяется, что скалярное произведение экспоненциальных векторов равно

$$\langle e(f), e(g) \rangle_{F(H)} = e^{\langle f,g \rangle_H} \tag{7.1}$$

Лемма 7.1. Линейные комбинации экспоненциальных векторов из множества

$$\{e(f), f \in H\}$$

плотны в $F(H)$.

Доказательство. Заметим, что

$$\frac{d^n}{dt^n}(e(tf))\bigg|_{t=0} = \sqrt{n!} f^{\otimes^n}$$

С другой стороны, множество линейных комбинаций элементарных тензоров вида $f^{\otimes^n}$ позволяет выразить любой элементарный тензор из $H^{\otimes^n_s}$. Докажем это по индукции. Для $n = 2$ получаем

$$f \otimes g + g \otimes f = (f + g) \otimes (f + g) - f \otimes f - g \otimes g. \tag{7.2}$$

Пусть утверждение доказано для n. Докажем его для $n + 1$. Рассмотрим элемент h, представляющий собой симметризованное тензорное произведение f и $g^{\otimes^n}$:

$$h = f \otimes g^{\otimes^n} + g \otimes f \otimes g^{\otimes^{n-1}} + \cdots + g^{\otimes^n} \otimes f \tag{7.3}$$

где $f, g \in H$. Утверждение верно, если из равенства нулю скалярного произведения

$$\left\langle h, u^{\otimes^{n+1}} \right\rangle_{H^{\otimes^{n+1}}} = 0 \tag{7.4}$$

для любого $u \in H$ следует, что

$$h = 0.$$

Заметим, что

$$\left\langle h, u^{\otimes^{n+1}} \right\rangle_{H^{\otimes^{n+1}}} = (n + 1)\langle f, u \rangle_H \langle g, u \rangle_H^n. \tag{7.5}$$

Положим $u = f$, тогда из (7.4)-(7.5) вытекает $\langle g, f \rangle_H = 0$ для всех $f \in H$, так что $g = 0$. Аналогично, подставляя $u = g$, получаем, что $f = 0$. Тем самым $h = 0$.

В силу леммы 7.1 любой линейный оператор в $F(H)$ достаточно задать на экспоненциальных векторах. Экспоненциальные вектора обладают ещё одним важным свойством, которое нам потребуется в дальнейшем.

Лемма 7.2. Отображение $U : F(H \oplus K) \to F(H) \otimes F(K)$, заданное на экспоненциальных векторах формулой

$$U(e(f \oplus g)) = e(f) \otimes e(g), \quad f \in H, \quad g \in K$$

является унитарным оператором.

Доказательство. Нам нужно доказать, что U сохраняет скалярное произведение. Заметим, что

$$\langle e(f_1)\otimes e(g_1), e(f_2)\otimes e(g_2)\rangle_{F(H)\otimes F(K)} = \langle e(f_1), e(f_2)\rangle_{F(H)} \langle e(g_1), e(g_2)\rangle_{F(K)} = \\ = e^{\langle f_1,f_2\rangle_H + \langle g_1,g_2\rangle_K}, f_j \in H, g_k \in K.$$

С другой стороны,

$$\langle e(f_1\oplus g_1), e(f_2\oplus g_2)\rangle_{F(H\oplus K)} = e^{\langle f_1,f_2\rangle_H + \langle g_1,g_2\rangle_H}$$

$f_j \in H, g_k \in K$.

Для $f \in H$ определим оператор $a(f)$ на экспоненциальных векторах по формуле

$$a(f)e(g) = \langle f, g\rangle e(g), g \in H \tag{7.6}$$

Из формулы (7.6) следует, что экспоненциальные векторы являются аналогом когерентных состояний квантового гармонического осциллятора. Оператор $a^+(f)$, сопряжённый с $a(f)$, полностью определяется формулой

$$\big\langle e(g), a^+(f)e(h)\big\rangle_{F(H)} = \langle a(f)e(g), e(h)\rangle = \overline{\langle f,g\rangle_H} e^{\langle f,g\rangle_H}. \tag{7.7}$$

Операторы $a^+(f), a(g), f, g \in H$ называются операторами рождения и уничтожения в симметричном пространстве Фока $F(H)$. Следующее свойство операторов рождения полезно для технических расчётов.

Лемма 7.3.

$$a^+(f)e(g) = \frac{d}{dt}(e(g+tf))\Big|_{t=0} \tag{7.8}$$

Доказательство. Заметим, что

$$\frac{d}{dt}\langle e(h), e(g+tf)\rangle_{F(H)} = \frac{d}{dt} e^{\langle h,g\rangle_H + t\langle h,f\rangle_H} = \langle h,f\rangle_H e^{\langle h,g\rangle_H + t\langle h,f\rangle_H}$$

Теорема 7.1. Операторы рождения и уничтожения $a^+(f), a(g), f, g \in H$, удовлетворяют каноническим коммутационным соотношениям:

$$a(f)a^+(g) - a^+(g)a(f) = \langle f,g\rangle_H \mathrm{I}, \\ a(f)a(g) - a(g)a(f) = 0, a^+(f)a^+(g) - a^+(g)a^+(f) = 0, \tag{7.9}$$

$f, g \in H$.

Замечание 7.1. Тождества (7.9) называются каноническими коммутационными соотношениями.

Доказательство. Докажем первое из соотношений (7.9). Остальные доказываются аналогично. Заметим, что

$$\big\langle e(v), a^+(f)a(g)e(u)\big\rangle_{F(H)} = \langle a(f)e(v), a(g)e(u)\rangle_{F(H)} = \\ = \overline{\langle f,v\rangle_H}\,{}_H\langle g,u\rangle_H e^{\langle v,u\rangle_H}.$$

С другой стороны, применяя лемму 7.3, получаем

$$\left\langle e(v), a(g)a^+(f)e(u)\right\rangle_{F(H)} = \frac{d}{dt}\langle e(v), a(g)e(u+tf)\rangle_{F(H)}\Big|_{t=0} =$$
$$= \frac{d}{dt}\left(\langle g, u+tf\rangle_H e^{\langle v,u+tf\rangle_H}\right)\Big|_{t=0} = \left(\langle g,f\rangle_H + \langle g,u\rangle_H\langle v,f\rangle_H\right)e^{\langle v,u\rangle_H}$$

6.7.3 7.3. Realization of Wiener and Poisson Processes in Fock's Space

Нашей целью будет реализация случайных процессов примеров 7.1 и 7.2 в виде линейных неограниченных операторов в симметричном пространстве Фока. Для этого мы будем использовать одночастичное пространство Фока $H = L^2(\mathbb{R})$. Обозначим

$$H_{st} = \left\{\mathbb{C}\chi_{[s,t]}\right\}$$

одномерное гильбертово пространство, натянутое на индикаторную функцию

$$\chi_{[s,t]}(x) = \begin{cases} 1, & x \in [s,t]; \\ 0, & x \notin [s,t]. \end{cases}$$

Рассмотрим пространство Фока $F\left(H_{st}\right) \subset F(H)$. Введём семейства операторов

$$A^+_{st} = a^+\left(\chi_{[s,t]}\right), A_{st} = a\left(\chi_{[s,t]}\right) \tag{7.10}$$

Лемма 7.4. Действие операторов (7.10) относительно представления

$$F\left(H_{st}\oplus H^\perp_{st}\right) \cong F\left(H_{st}\right)\otimes F\left(H^\perp_{st}\right)$$

имеет вид

$$A^+_{st} \cong A^+_{st}\big|_{F(H_{st})}\otimes \mathrm{I}_{F\left(H^\perp_{st}\right)}, \quad A_{st} \cong A_{st}|_{F(H_{st})}\otimes \mathrm{I}_{F\left(H^\perp_{st}\right)}$$

Доказательство. Непосредственно следует из определения действия A^+_{st}и A_{st} на экспоненциальные векторы $7.6 - 7.8$ и леммы 7.2

Положим

$$Q_t = A^+_{0t} + A_{0t}$$

Теорема 7.2. Пара ($Q_t, |\Omega\rangle$) определяет винеровский случайный процесс.

Доказательство. Из теоремы 7.1 следует, что операторы A^+_{st}и A_{st} удовлетворяют каноническому коммутационному соотношению вида

$$\left[A_{st}, A^+_{st}\right] = (t-s)\mathrm{I}$$

Если отождествить ортонормированный базис в $F\left(H_{st}\right)$ с основным и возбуждённым состояниями квантового осциллятора согласно правилу

$$|0\rangle = |\Omega\rangle, |n\rangle = \frac{1}{\sqrt{(t-s)^n}}\chi^{\otimes^n}_{[s,t]}$$

получим, что оператор $A^+_{st}+A_{st} = \sqrt{t-s}C$, где оператор C рассмотрен в примере 3.4.2. Следовательно, приращения процесса $Q_t - Q_s == A^+_{st} + A_{st} \in \mathcal{N}(0, t-s)$ в состоянии, определяемом вакуумным вектором $|\Omega\rangle$. Коммутативность наблюдаемых, входящих в процесс $[Q_t, Q_s] = 0$, следует из канонических коммутационных соотношений теоремы

7.1. Осталось доказать, что классические случайные величины, порождённые $Q_{t_1} - Q_{s_1}$ и $Q_{t_2} - Q_{s_2}$ в вакуумном состоянии, независимы. Для гауссовских случайных величин независимость следует из некоррелированности. Заметим, что

$$\mathrm{Cov}_\rho\left(Q_{t_1} - Q_{s_1}, Q_{t_2} - Q_{s_2}\right) = \langle\Omega|\left(A^+_{s_1t_1} + A_{s_1t_1}\right)\left(A^+_{s_2t_2} + A_{s_2t_2}\right)|\Omega\rangle_{F(H)} =$$
$$= \left\langle A^+_{s_1t_1}\Omega \mid A^+_{s_2t_2}\Omega\right\rangle_{F(H)} = \left\langle\chi_{[s_1,t_1]}, \chi_{[s_2,t_2]}\right\rangle_H = 0,$$
$$\text{если } (s_1,t_1)\cap(s_2,t_2) = \emptyset \text{ в состоянии } \rho = |\Omega\rangle\langle\Omega|.$$

Рассмотрим двухпараметрическое семейство операторов:

$$\Lambda_{st} = \frac{1}{t-s}\left(A^+_{st}A_{st}\right), s < t$$

Лемма 7.5. Для любого выбора $s \le r \le t$ справедливо

$$\Lambda_{sr} + \Lambda_{rt} = \Lambda_{st}.$$

Доказательство. По определению действия A^+_{st}и A_{st} получаем

$$\Lambda_{st}|\Omega\rangle = 0$$
$$\Lambda_{st}\chi^{\otimes^n}_{[s,t]} = n\chi^{\otimes^n}_{[s,t]}$$

В силу леммы 7.4 получаем

$$\Lambda_{st} \cong \Lambda_{st}|_{F(H_{st})} \otimes \mathrm{I}_{F\left(H^{\perp}_{st}\right)}$$

Таким образом, получаем

$$\Lambda_{st} \cong \Lambda_{sr}|_{F(H_{sr})} \otimes \mathrm{I}_{F(H_{rt})} \otimes \mathrm{I}_{F\left(H^{\perp}_{st}\right)} +$$
$$+ \mathrm{I}_{F(H_{sr})} \otimes \Lambda_{rt}\big|_{F(H_{rt})} \otimes \mathrm{I}_{F\left(H^{\perp}_{st}\right)}$$

□

Фиксируем $\lambda > 0$ и положим

$$N_t = \Lambda_{0t} + \sqrt{\lambda}Q_t + \lambda t\mathrm{I}.$$

Теорема 7.3. Пара ($N_t, |\Omega\rangle$) определяет пуассоновский случайный процесс с распределением:

$$N_t - N_s \in \mathcal{P}(\lambda(t-s))$$

Доказательство. В силу леммы 7.5 для приращений N_t справедливо представление

$$N_t - N_s = \left(\frac{1}{\sqrt{t-s}}A^+_{st} + \sqrt{\lambda(t-s)}\mathrm{I}\right)\left(\frac{1}{\sqrt{t-s}}A_{st} + \sqrt{\lambda(t-s)}\mathrm{I}\right)$$

Тогда из примера 3.4.1. получаем

$$N_t - N_s \in \mathcal{P}(\lambda(t-s))$$

Попарная коммутативность операторов N_t следует из теоремы 7.1. Осталось доказать независимость классических случайных величин, порождённых приращениями $N_{t_1} - N_{s_1}$ и $N_{t_2} - N_{s_2}$ в вакуумном состоянии для непересекающихся интервалов $(s_1,t_1)\cap(s_2,t_2) = \emptyset$. Для этого достаточно проверить некоррелированность в состоянии $\rho = |\Omega\rangle\langle\Omega|$. Заметим, что

$$\langle\Omega|\left(\frac{1}{\sqrt{t_1-s_1}}A^+_{s_1t_1}+\sqrt{\lambda\,(t_1-s_1)}\mathrm{I}\right)\left(\frac{1}{\sqrt{t_1-s_1}}A_{s_1t_1}+\sqrt{\lambda\,(t_1-s_1)}\mathrm{I}\right)\times$$
$$\times\left(\frac{1}{\sqrt{t_2-s_2}}A^+_{s_2t_2}+\sqrt{\lambda\,(t_2-s_2)}\mathrm{I}\right)\left(\frac{1}{\sqrt{t_2-s_2}}A_{s_2t_2}+\sqrt{\lambda\,(t_2-s_2)}\mathrm{I}\right)|\Omega\rangle=$$
$$=\left(\sqrt{\lambda}\left\langle\chi_{[s_1,t_1]}\right|+\lambda\,(t_1-s_1)\,\langle\Omega|\right)\left(\sqrt{\lambda}\left|\chi_{[s_2,t_2]}\right\rangle+\lambda\,(t_2-s_2)\,|\Omega\rangle\right)=$$
$$=\lambda^2\,(t_1-s_1)\,(t_2-s_2)$$

для непересекающихся интервалов $(s_1,t_1)\cap(s_2,t_2)=\emptyset$. Следовательно,

$$\mathrm{Cov}_\rho\left(N_{t_1}-N_{s_1},N_{t_2}-N_{s_2}\right)=$$
$$=\mathbb{E}_\rho\left(N_{t_1}-N_{s_1}-\lambda\,(t_1-s_1)\,,N_{t_2}-N_{s_2}-\lambda\,(t_2-s_2)\right)=0$$

6.8 A.8

6.8.1 8.1. Tomographic Representation of Quantum Mechanics

Под томографическим представлением квантовой механики мы понимаем некоторую процедуру при которой удаётся перейти от операторов состояний и наблюдаемых к функциям некоторого количества переменных. Разработка томографического представления привело к созданию следующего формализма [25, 38]. В гильбертовом пространстве H вводятся множества операторов $U(\mathbf{x})$ и $D(\mathbf{x})$, зависящих от n-мерного вектора $\mathbf{x}=(x_1,x_2,\ldots,x_n)$ таким образом, что оператору A на H сопоставляется функция

$$f_A(\mathbf{x})=\mathrm{Tr}(U(\mathbf{x})A), \tag{8.1}$$

называемая его символом, и оператор может быть восстановлен по своему символу с использованием формулы

$$A=\int D(\mathbf{x})f_A(\mathbf{x})d\mathbf{x} \tag{8.2}$$

Семейства $U(\mathbf{x})$ и $D(\mathbf{x})$ получили названия де-квантизатора и квантизатора соответственно.

В конечномерном пространстве H (спиновая томография) такой подход может быть реализован математически безупречно [28]. Этого нельзя сказать про бесконечномерный случай, когда семейства $U(\mathbf{x})$ и $D(\mathbf{x})$ фактически состоят не из операторов, а лишь определяют линейные формы:

$$A\to\mathrm{Tr}(U(\mathbf{x})A),A\to\mathrm{Tr}(D(\mathbf{x})A), \tag{8.3}$$

смысл которых необходимо математически точно объяснять. Причина сложностей состоит в том, что, как было установлено в теореме 2.14, пространство ядерных операторов $\mathfrak{S}_1(H)$ является предсопряженным к алгебре всех ограниченных операторов $(B(H)^*=\mathfrak{S}_1(H)$. Таким образом, если рассматривать ограниченные операторы в качестве наблюдаемых, алгебра наблюдаемых является сопряженным пространством к пространству состояний. Если мы хотим, чтобы неограниченные операторы входили в пространство наблюдаемых $\mathfrak{A}$ и пространство состояний $\mathfrak{S}$ обладало свойством $(\mathfrak{S})'=\mathfrak{A}$, мы должны взять некоторое подмножество в $\mathfrak{S}_1(H)$. Мы будем придерживаться такого подхода.

6.8.2 8.2. The Finite - Dimensional Case

В случае $\dim H < +\infty$ де-квантизатор (8.1) и квантизатор (8.2) представляют собой семейства ограниченных операторов в H. Из соотношений 8.1 и 8.2 тут же следует, что если

$$f_\rho(\mathbf{x}) = \mathrm{Tr}\,(U(\mathbf{x}\rho), g_A(\mathbf{x}) = \mathrm{Tr}(D(\mathbf{x})A) \tag{8.4}$$

для двух операторов $\rho, A \in B(H)$, тогда

$$\mathrm{Tr}(\rho A) = \int g_A(\mathbf{x}) f_\rho(\mathbf{x}) d\mathbf{x} \tag{8.5}$$

Таким образом, формулу (8.5) можно воспринимать как действие функционала A на элемент ρ, так что она отражает тот факт, что в конечномерном случае $B(H)^* \cong B(H)$.

Различные примеры де-квантизаторов и квантизаторов для конечномерного случая приведены в [28, 29. Мы не будем здесь их все воспроизводить и ограничимся простейшим случаем $\dim H = 2$, когда формулы выглядят наиболее просто. Положим $\mathbf{x} := (m, \alpha, \beta)$, где $m = \pm\frac{1}{2}$ представляет собой два возможных результата измерения величины спина по направлению, задаваемому углами Эйлера: $\alpha \in\in [0, 2\pi], \beta \in [0, \pi]$. Тогда де-квантизатор и квантизатор еределяются формулами:

$$U(\mathbf{x}) = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + m\begin{pmatrix} \cos\beta & -e^{i\alpha}\sin\beta \\ -e^{-i\alpha}\sin\beta & -\cos\beta \end{pmatrix} \tag{8.6}$$

$$D(\mathbf{x}) = 3U(\mathbf{x}) - \mathrm{I} \tag{8.7}$$

Здесь нужно положить

$$\int \mathrm{d}\mathbf{x} := \sum_{m=-1/2}^{1/2} \frac{1}{2\pi} \int_0^{2\pi} \mathrm{d}\alpha \int_0^{\pi} \sin\beta \mathrm{d}\beta \tag{8.8}$$

6.8.3 8.3. Representation by Characteristic Functions

Обозначим $S(\mathbb{R}^n)$ пространство Шварца, состоящее из бесконечно дифференцируемых функций, убывающих быстрее любой степени на бесконечности, с обычной топологией для такого пространства. Пусть $H = L^2(\mathbb{R})$. Пространство $S(\mathbb{R})$ плотно в области определения всех степеней операторов координаты $(q\psi)(x) = x\psi(x)$ и импульса $(p\psi)(x) =$
$= -i\frac{d\psi}{dx}(x)$. Нам также потребуются операторы рождения $a^\dagger = \frac{q-ip}{\sqrt{2}}$ и уничтожения $a = \frac{q+ip}{\sqrt{2}}$.

Оператор $T \in B(H)$ называется оператором Шварца [34, если он ограничен относительно семейства полунорм:

$$\|T\|_{n,m,\psi} = \|q^n p^m T\psi\|, \tag{8.9}$$

$n, m = 0, 1, 2, \ldots, \psi \in S(\mathbb{R})$. Обозначим $\mathcal{S}$ множество всех операторов Швариа. В [34 было показано: для того чтобы $T \in \mathcal{S}$, необходимо и достаточно, чтобы он имел вид

$$(T\psi)(x) = \int \rho(x, y)\psi(y) dy \tag{8.10}$$

где ядро $\rho(\cdot, \cdot) \in S(\mathbb{R}^2)$. Множество $\mathcal{S}$ является пространством Фреше относительно семейства полунорм (8.9).

Унитарные операторы:

$$W(x,y) = \exp(i(xq + yp)) \tag{8.11}$$

в пространстве $H = L^2(\mathbb{R})$ называются операторами Вейля. В квантовой механике часто используется следующее полезное свойство.

Лемма 8.1 (формула Бейкера-Кэмпбелла-Хаусдорфа). Пусть $[A, B] == cI$ (пропорционален тождественному оператору), тогда

$$\exp(A + B) = \exp(A)\exp(B)\exp\left(-\frac{1}{2}[A, B]\right)$$

Замечание 8.1. Из леммы 8.1 немедленно следует, что

$$\exp(ixq + iyp) = \exp(ixq)\exp(iyp)\exp(ixy/2) \tag{8.12}$$

Доказательство. Заметим, что из $[A, B] = cI$ следует

$$[A, F(B)] = cF'(B)$$

что влечёт

$$[A, \exp(B)] = c\exp(B)$$

Тогда

$$\exp(-B)A\exp(B) = A + cI$$

и

$$\exp(-B)\exp(A)\exp(B) = \exp(A + cI) = \exp(A)\exp(c)$$

В итоге

$$\exp(A)\exp(B) = \exp(B)\exp(A)\exp([A, B]) \tag{8.13}$$

Рассмотрим семейство операторов:

$$U_t = \exp(tA)\exp(tB)\exp\left(-\frac{t^2}{2}\right) \tag{8.14}$$

Применяя к операторам tB и sA соотношение (8.13), получаем для (8.14):

$$U_t U_s = U_{t+s}$$

так что семейство операторов 8.14 является решением задачи Коши:

$$\frac{dU_t}{dt} = (A + B)U_t, t \geq 0, U_0 = I \tag{8.15}$$

Решением той же системы 8.15 является семейство операторов: $\exp(t(A + B))$, откуда можно сделать вывод:

$$U_t = \exp(t(A + B)), t \geq 0$$

Подстановка $t = 1$ завершает доказательство.

Положим $\mathbf{x} = (x, y)$ и определим де-квантизатор с помощью оператора Вейля: $U(x, y) = W(x, y)$. Тогда можно ввести символ оператора $\rho \in \mathfrak{S}_1(H)$ по формуле

$$f_\rho^W(x,y) = \mathrm{Tr}(W(x,y)\rho). \tag{8.16}$$

В случае $\rho \in \mathfrak{S}(H)$, символ (8.16) называется характеристической функи,ией состояния ρ [13]. Соответствующий квантизатор дается формулой 13:

$$D(x,y) = \frac{1}{2\pi} W(-x,-y) \tag{8.17}$$

Мы будем называть (8.16) вейлевской характеристической функцией оператора $\rho \in \mathfrak{S}_1(H)$.

Лемма 8.2. Пусть $\rho \in \mathcal{S}$. Тогда вейлевская характеристическая функи,ия $f_\rho^W \in S(\mathbb{R}^2)$. Более того, если функция $f \in S(\mathbb{R}^2)$, тогда полученный из нее с помощью квантизатора оператор $T \in \mathcal{S}$.

Доказательство. Из (8.12) немедленно следует, что

$$W(x,y) = e^{\frac{i}{2}xy} V_x U_y \tag{8.18}$$

где

$$(V_x\psi)(z) = e^{ixz}\psi(z), (U_y\psi)(z) = \psi(z+y) \tag{8.19}$$

$\psi \in H$. Поскольку $\rho \in \mathcal{S}$, в силу 8.10 получаем

$$\begin{gathered} f_\rho^W(x,y) = \mathrm{Tr}(W(x,y)\rho) = \\ = \int_{\mathbb{R}} e^{\frac{i}{2}xy} e^{ixt} \rho(t+y,t)dt = \int_{\mathbb{R}} e^{ixt} \rho\left(t + \frac{y}{2}, t - \frac{y}{2}\right) dt \end{gathered} \tag{8.20}$$

Функция $\tilde{\rho}(t,y) = \rho\left(t+\frac{y}{2}, t-\frac{y}{2}\right)$ принадлежит пространству Шварца $S(\mathbb{R}^2)$. Следовательно, её преобразование Фурье по переменной t также принадлежит $S(\mathbb{R}^2)$.

Пусть теперь наоборот: $f \in S(\mathbb{R}^2)$. Положим

$$T = \frac{1}{2\pi} \int f(x,y) W(-x,-y) dxdy \tag{8.21}$$

Определим, как действует T на функцию $\psi \in H$.

$$\begin{gathered} (T\psi)(t) = \frac{1}{2\pi} \iint_{\mathbb{R}^2} f(x,y) e^{-\frac{i}{2}xy} e^{-ix(t-y)} \psi(t-y) dxdy = \\ = -\frac{1}{2\pi} \int_{\mathbb{R}^2} f(x,t-s) e^{-\frac{i}{2}x(t-s)} e^{-ixs} \psi(s) dxds = \int_{\mathbb{R}} \rho(t,s)\psi(s) ds \end{gathered} \tag{8.22}$$

где ядро оператора $\rho(t,s)$ определяется формулой

$$\rho(t,s) = -\frac{1}{2\pi} \int_{\mathbb{R}} e^{-\frac{i}{2}tx} f(x,t-s) dx \tag{8.23}$$

Получаем, что отображение $f \to \rho$ представляет собой композицию сдвига и преобразования Фурье по одной из переменных. Таким образом, $\rho \in S(\mathbb{R}^2)$ и T тем самым является оператором Шварца.

Используя операторы рождения и уничтожения формулу 8.16, можно переписать в виде

$$f_\rho^W(x,y) = f_\rho^W(z) = \mathrm{Tr}\left(\exp\left(za^\dagger - \bar{z}a\right)\rho\right) \tag{8.24}$$

где

$$z = \frac{y + ix}{\sqrt{2}} \tag{8.25}$$

В квантовой физике используются также характеристические функции [24]:

$$f_\rho^P(x,y) = f_\rho^P(z) = \mathrm{Tr}\left(\exp\left(za^\dagger\right)\exp(-\bar{z}a)\rho\right) \tag{8.26}$$

и

$$f_\rho^Q(x,y) = f_\rho^Q(z) = \mathrm{Tr}\left(\exp(-\bar{z}a)\exp\left(za^\dagger\right)\rho\right) \tag{8.27}$$

называемые характеристической функцией Глаубера-Сударшана и характеристической функцией Хусими. Функкции (8.16), (8.26) и (8.27) связаны простым соотношением

$$f_\rho^W(z) = f_\rho^P(z)e^{\frac{-|z|^2}{2}} = f_\rho^Q(x)e^{\frac{|z|^2}{2}} \tag{8.28}$$

Характеристические функции Глаубера-Сударшана и Хусими также можно считать символами оператора ρ. Обратное преобразование (квантизатор) представляет собой композицию (8.28) и квантизатора для вейлевской характеристической функции. Введём множества $S_\pm(\mathbb{R}^2)$, состоящие из функций $\psi_\pm$, представимых в виде

$$\psi_\pm(x,y) = \exp\left(\pm\frac{x^2+y^2}{4}\right)\psi(x,y)$$

где $\psi \in S(\mathbb{R}^2)$. Лемма 8.2 и 8.28 влечет справедливость утверждения ниже.

Следствие 8.1. Пусть $\rho \in \mathcal{S}$. Тогда характеристические функции $f_\rho^P \in S_+(\mathbb{R}^2), f_\rho^Q \in S_-(\mathbb{R}^2)$. Более того, если функция f принадлежит соответствующему классу, тогда полученный из нее с помощью квантизатора оператор $T \in \mathcal{S}$.

6.8.4 8.4. Representation by Quasi - Distributions

Для вейлевских характеристических функций справедливо равенство 13 :

$$\frac{1}{(2\pi)^2}\int_{\mathbb{R}^2} f_\rho^W(x,y)f_\sigma^W(x,y)dxdy = \mathrm{Tr}(\rho\sigma) \tag{8.29}$$

$\rho, \sigma \in \mathcal{S}$. С помощью соотношения (8.29) можно расширить отображение $\rho \to f_\rho^W$ с $\mathcal{S}$ до $\mathcal{S}'$. В этом случае символами полиномов от операторов координаты и импульса q и p станут линейные комбинации сингулярных обобщенных функций $\delta^{(n)}(x)\delta^{(m)}(y)$ [1. По-видимому, поэтому исторически [47, 39] был выбран другой символ, представляющий собой преобразование Фурье от характеристической функции f^W.

Рассмотрим преобразование Фурье F функции $f \in S(\mathbb{R}^2)$:

$$F(f)(q,p) \equiv \hat{f}(q,p) = \frac{1}{(2\pi)^2}\int_{\mathbb{R}^2} e^{-iqx-ipy}f(x,y)dxdy \tag{8.30}$$

Функция

$$W(q,p) = \hat{f}_\rho^W(q,p) \tag{8.31}$$

называется функи,ией Вигнера. Поскольку преобразование Фурье переводит $S(\mathbb{R}^2)$ в себя, справедливо следующее утверждение.

Лемма 8.3. Функи,ия Вигнера $W_\rho \in S(\mathbb{R}^2)$ тогда и только тогда, когда оператор ρ, по которому она построена, является оператором Швариа.

Обозначим

$$\hat{S}_{-}\left(\mathbb{R}^{2}\right)=F\left(S_{-}\left(\mathbb{R}^{2}\right)\right) \tag{8.32}$$

Лемма 8.4. Элементами $\hat{S}_{-}\left(\mathbb{R}^{2}\right)$ являются функции ψ, представимые в виде свертки:

$$\psi=\xi_{0}\star\xi \tag{8.33}$$

где $\xi_{0}(q,p)=\exp\left(-q^{2}-p^{2}\right)u\xi\in S\left(\mathbb{R}^{2}\right)$.

Доказательство. При преобразовании Фурье умножение на функцию переходит в свёртку. Таким образом, достаточно заметить, что для $f_{0}(x,y)=e^{-\frac{x^{2}+y^{2}}{4}}$ имеем $F\left(f_{0}\right)(q,p)=\frac{1}{2\pi}e^{-q^{2}-p^{2}}$.

Положим

$$\alpha=\frac{q+ip}{\sqrt{2}}. \tag{8.34}$$

Тогда функция

$$Q_{\rho}(\alpha)=\hat{f}_{\rho}^{Q}(q,p) \tag{8.35}$$

называется функцией Хусими. Как известно,

$$Q_{\rho}(\alpha)=\frac{1}{\pi}\left(\psi_{\alpha},\rho\psi_{\alpha}\right) \tag{8.36}$$

По построению функция Хусими получаем справедливость следующего утверждения.

Лемма 8.5. Функиия Хусими $Q_{\rho}\in\hat{S}\left(\mathbb{R}^{2}\right)$ тогда и только тогда, когда оператор ρ, по которому она построена, является оператором Швариа.

Заметим, что преобразование Фурье 8.30 можно расширить не только на обобщенные функции медленного роста класса $S'\left(\mathbb{R}^{2}\right)$, но и на функции класса $S_{+}\left(\mathbb{R}^{2}\right)$. Преобразование Фурье функции $\psi_{+}\ \in\in\ S_{+}\left(\mathbb{R}^{2}\right.$ является обобщенной функцией $F\left(\psi_{+}\right)\in\hat{S}'_{-}\left(\mathbb{R}^{2}\right)$, так что

$$<F\left(\psi_{+}\right),\overline{F\left(\psi_{-}\right)}>:=<\psi_{+},\overline{\psi_{-}}>=\int_{\mathbb{R}^{2}}\psi_{+}(x,y)\overline{\psi_{-}(x,y)}dxdy \tag{8.37}$$

где $\psi_{\pm}\in S_{\pm}\left(\mathbb{R}^{2}\right)$. Делая замену переменной (8.34), можно определить

$$P_{\rho}(\alpha)=\hat{f}_{\rho}^{P}(q,p) \tag{8.38}$$

называемую P-функцией Глаубера-Сударшана. Из равенства Парсеваля следует, что

$$\int_{\mathbb{C}}P_{\rho}(\alpha)Q_{\sigma}(\alpha)d^{2}\alpha=\mathrm{Tr}(\rho\sigma) \tag{8.39}$$

для двух $\rho,\sigma\in\mathcal{S}$. Отсюда немедленно вытекает известная формула:

$$\rho=\int_{\mathbb{C}}P_{\rho}(\alpha)\left|\psi_{\alpha}><\psi_{\alpha}\right|d^{2}\alpha \tag{8.40}$$

6.8.5 8.5. Optical Tomogram Presentation and Its Dual

Оптическая томограмма 21 также может быть использована для определения символов операторов Шварца. Используя ядро интегрального оператора (8.10) можно выразить оптическую томограмму в виде 17:

$$\omega_\rho(x,\varphi)=\frac{1}{2\pi}\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty}e^{is(t\cos\varphi-x)}\rho\left(t-\frac{s\sin\varphi}{2},t+\frac{s\sin\varphi}{2}\right)dtds \tag{8.41}$$

Если определить отображение

$$\Omega_\rho(x,\varphi)=\int_{0}^{+\infty}\int_{-\infty}^{+\infty}te^{i(x+t\sin\varphi)s}\rho\left(t-\frac{s\sin\varphi}{2},t+\frac{s\sin\varphi}{2}\right)dtds \tag{8.42}$$

получим 17:

$$\int_0^{2\pi}\int_0^{+\infty}\Omega_\rho(x,\varphi)\omega_\sigma(x,\varphi)dxd\varphi=\mathrm{Tr}(\rho\sigma) \tag{8.43}$$

где $\rho,\sigma\in\mathcal{S}$. Оптический томографический символ обладает свойством: $\omega_\rho(-x,\varphi):=\omega_\rho(x,\varphi+\pi)$. Обозначим S_{opt} образ $S\left(\mathbb{R}^2\right)$ при отображении (8.41). Справедливо следующее утверждение [17:

Теорема 8.1. Элементы пространства S_{opt} обладаеют следующими двумя свойствами:
(i) $\omega_\rho(\cdot,\varphi)\in S(\mathbb{R})$ для фиксированного $\varphi\in[0,2\pi]$;
(ii) $\omega_\rho(x,\cdot)$ - бесконечно дифференииируемая 2π-периодическая функция для фиксированного $x\in\mathbb{R}$.

6.9 A.9

6.9.1 9.1. Quantum Dynamic Mappings

Рассмотрим линейное отображение $\Phi:B(H)\to B(H)$, заданное на алгебре всех ограниченных операторов $B(H)$ в гильбертовом пространстве H :

- отображение Φ называется положительным, если для любого $A>0$ выполнено $\Phi(A)>0$;
- отображение Φ называется n-положительным, если

$$\Phi\otimes\mathrm{id}_n:B(H)\otimes\mathcal{M}_n(\mathbb{C})\to B(H)\otimes\mathcal{M}_n(\mathbb{C})$$

является положительным;

- отображение Φ называется вполне положительным, если оно n-положительно для любого n.

То, что для некоммутативного случая положительность отличается от n-положительности, заметил В.Ф. Стайнспринг, которому и принадлежит определение полной положительности.

Теорема 9.1. Для того чтобы отображение $\Phi:B(H)\to B(H)$ было вполне положительным, необходимо и достаточно, чтобы для любого выбора $Y_j\in B(H)$ и $\xi_j\in H$ выполнялось условие:

$$\sum_{j,k}\left\langle\xi_j,\Phi\left(Y_j^*Y_k\right)\xi_k\right\rangle\geq 0.$$

Доказательство. По определению $\Phi \otimes \mathrm{id} : B(H) \otimes B(K) \to B(H) \otimes\otimes B(K)$, где $\dim K = n$, - положительное отображение, то есть для любого $X \in B(H) \otimes B(K)$, такого что $X > 0$, выполнено $(\ \Phi \otimes \mathrm{id}\ )\ (\ X\ ) >> 0$. Положим

$$X = \begin{pmatrix} X_{11} & \dots & X_{1n} \\ \dots & \dots & \dots \\ X_{n1} & \dots & X_{nn} \end{pmatrix}, \tag{9.1}$$

где $X_{ij} \in B(H)$. Тогда

$$(\Phi \otimes \mathrm{id})(X) = \begin{pmatrix} \Phi(X_{11}) & \dots & \Phi(X_{1n}) \\ \dots & \dots & \dots \\ \Phi(X_{n1}) & \dots & \Phi(X_{nn}) \end{pmatrix}. \tag{9.2}$$

Пусть $\xi = (f_1, \dots, f_n)^T \in \mathcal{H} \otimes K$, где $f_j \in \mathcal{H}$. Из условия

$$(\Phi \otimes \mathrm{id})(X) > 0$$

следует

$$\langle \xi, (\Phi \otimes \mathrm{id})(X)\xi \rangle \geq 0 \tag{9.3}$$

что эквивалентно

$$\sum_{i,j} \langle f_i, \Phi(Y_i^* Y_j) f_j \rangle \geq 0 \tag{9.4}$$

поскольку для $X > 0$ существует набор операторов $\{Y_i\}$ такой, что

$$X = \begin{pmatrix} Y_1^* \\ \vdots \\ Y_n^* \end{pmatrix} \begin{pmatrix} Y_1 & \dots & Y_n \end{pmatrix}. \tag{9.5}$$

Пример 9.1. Отображение $\Phi(X) = X^T$ является положительным, но не является вполне положительным, поскольку элемент

$$X = \begin{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & \frac{1}{2} \\ 0 & \frac{1}{2} \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 0 \\ \frac{1}{2} & 0 \\ \frac{1}{2} & 0 \\ 0 & 0 \end{pmatrix} \end{pmatrix} > 0 \tag{9.6}$$

переводится отображением Φ в

$$\Phi(X) = \begin{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & \frac{1}{2} \\ 0 & 0 \\ \frac{1}{2} & 0 \end{pmatrix} & \begin{pmatrix} 0 & \frac{1}{2} \\ 0 & 0 \\ \frac{1}{2} & 0 \\ 0 & 0 \end{pmatrix} \end{pmatrix} \not> 0. \tag{9.7}$$

Утверждение 9.1. Пусть $\dim \mathcal{H} = n < \infty$, тогда полная положительность эквивалентна n-положительности.

Определение 9.1. Отображение Φ называется унитальным, если оно сохраняет тождественный оператор

$$\Phi(I) = I$$

Определение 9.2. Линейное отображение $\pi : B(H) \to B(K)$ называется представлением $B(H)$ в гильбертовом пространстве K, если оно является *-морфизмом, то есть

$$\pi\left(A^*\right) = (\pi(A))^*, \pi(AB) = \pi(A)\pi(B),$$

для всех $A, B \in B(H)$.

Теорема 9.2 (Стайнспринг [44]). Отображение Φ является вполне положительным и унитальным тогда и только тогда, когда существуют изометрическое вложение $V : H \hookrightarrow K$ и представление $\pi : B(H) \to B(K)$ такие, что

$$\Phi(A) = V^*\pi(A)V \tag{9.8}$$

где сопряженное отображение V^* определяется из условия

$$\langle Vf, \xi\rangle_K = \langle f, V^*\xi\rangle_H \tag{9.9}$$

Доказательство. Определим на множестве пар (f, A), где $f \in H$, $A \in B(H)$, двухточечную функцию

$$\langle (f, A), (g, B)\rangle_K \stackrel{\text{def}}{=} \langle f, \Phi\left(A^*B\right) g\rangle_H, \tag{9.10}$$

линейную по второму и антилинейную по первому аргументам. Пополняя $\{(f, A)\}$ по норме, определенной скалярным произведением (9.10), получим гильбертово пространство K. Определим вложение $V : f \mapsto\mapsto (f, I)$ и представление $\pi(A) : (f, B) \mapsto (f, AB)$.

Следствие 9.1. Для любого вполне положительного унитального отображения $\Phi : B(H) \to B(H)$ найдётся семейство операторов $V_j \in B(H)$ такое, что справедливо следующее представление:

$$\Phi(A) = \sum_j V_j^* A V_j, \sum_j V_j^* V_j = I. \tag{9.11}$$

Замечание 9.1. Представление 9.11 называется представлением Крауса, а операторы (V_j) - операторами Крауса. Представление Крауса не является единственным. Минимально возможное число операторов Крауса в 9.11 для заданного Φ называется рангом Чоя (M.D. Choi).

Доказательство. Пусть V и π - оператор изометрического вложения и представление, определённые в теореме Стайнспринга. Из теории представлений следует, что найдётся такое гильбертово пространство $H_0, \dim H_0 \geq 0$, что $\pi \simeq \tilde{\pi}$, где $\tilde{\pi}$ - представление $B(H)$ в $B\left(H \otimes H_0\right)$ вида $\tilde{\pi}(A) = A \otimes I$. Определим операторы V_j формулой

$$\langle f, V_j g\rangle_H \stackrel{\text{def}}{=} \langle f \otimes e_j, Vg\rangle_{H\otimes H_0}, \tag{9.12}$$

где $\{e_j\}$ - ортонормированный базис в H_0. Тогда

$$\Phi(A) = \sum_{j=1}^{\dim H_0} V_j^* A V_j, A \in B(H).$$

Определение 9.3. Отображение $\Phi_* : \mathfrak{S}(H) \to \mathfrak{S}(H)$ называется предсопряженным к отображению $\Phi : B(H) \to B(H)$, если

$$\mathrm{Tr}\left(\Phi_*(\rho)A\right) = \mathrm{Tr}(\rho\Phi(A)) \tag{9.13}$$

где $\rho \in \mathfrak{S}(H), A \in B(H)$.

Определение 9.4. Отображение Φ_* называется квантовым каналом, если Φ - вполне положительное унитальное отображение.

Замечание 9.2. Существует единственное продолжение Φ_* на всю алгебру ограниченных операторов $B(H)$.
Замечание 9.3. Из представления Крауса 9.11 для Φ немедленно вытекает, что

$$\Phi_*(\rho) = \sum_j V_j \rho V_j^*, \rho \in \mathfrak{S}(H)$$

6.9.2 9.2. Defacing Channels

В этом пункте использованы результаты [14, 2] .

Определение 9.5. Пусть $\{e_j\}$ - ортонормированный базис в H. Дефазирующим называется канал

$$\Phi\left(|e_n\rangle\langle e_m|\right) = \lambda(n,m)\,|e_n\rangle\langle e_m|\,, \tag{9.14}$$

удовлетворяющий условиям:

1. $\lambda(n,n) = 1$ (сохранение следа);
2. $\sum_{n,m} \lambda(n,m)\overline{c_n}c_m \geq 0, c_n \in \mathbb{C}$ (положительная определённость).

Определение 9.6. Для фиксированных $x, y \in \mathbb{R}$ определим отображение $|x\rangle\langle y| : C(\mathbb{R}) \times C(\mathbb{R}) \to \mathbb{C}$ по формуле

$$\langle f \mid x\rangle\langle y \mid g\rangle \stackrel{\text{def}}{=} \overline{f(x)}g(y), \tag{9.15}$$

то есть $|x\rangle\langle y|$ отображает каждую пару непрерывных функций $f, g \in\in C(\mathbb{R})$ в комплексное число, причём отображение линейно по второму аргументу и антилинейно по первому.
Пусть $H = L^2(\mathbb{R})$. Тогда, согласно теореме Рисса-Фреше, для любого оператора $A \in B(H)$ существует такая функция $\rho_A(x,y)$, что

$$\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} \rho_A(x,y)\overline{f(x)}f(y)dxdy = \langle f, Ag\rangle \tag{9.16}$$

Используя определение 9.6 можно переписать 9.16 в виде

$$A = \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} \rho_A(x,y)|x\rangle\langle y|dxdy \tag{9.17}$$

Определим отображение

$$\Phi(|x\rangle\langle y|) = \lambda(x,y)|x\rangle\langle y|, \tag{9.18}$$

понимая его в том смысле, что

$$\langle f, \Phi(|x\rangle\langle y|)g\rangle = \int_{-\infty}^{+\infty}\int_{-\infty} \lambda(x,y)\overline{f(x)}g(y)dxdy \tag{9.19}$$

где $f, g \in H$. Тогда

$$\Phi(A) = \int_{-\infty}^{+\infty}\int_{\rho_A} (x,y)\lambda(x,y)|x\rangle\langle y|dxdy \tag{9.20}$$

Определение 9.7. Отображение 9.20 называется обобщённым дефазирующим каналом, если оно удовлетворяет следующим условиям:

1. $\lambda(x,x)=1$ (сохранение следа);

2. $\iint \lambda(x,y)\overline{c(x)}c(y)dxdy \geq 0$ (положительная определённость).

Определение 9.8. Каналы, демпфирующими фазу, называются *де* фазирующими каналами 9.14, для которых

$$\lambda(n,m)=\lambda(n-m), \lambda(-n)=\overline{\lambda(n)}.$$

В непрерывном случае каналы, демпфирующие фазу, называются обобщёнными дефазирующими каналами (9.20) для которых

$$\lambda(x,y)=\lambda(x-y), \lambda(-x)=\overline{\lambda(x)}.$$

Определение 9.9. Пусть G-локально компактная абелева группа. Тогда локально компактная абелева группа $\hat{G}$, дуальная к G, состоит из отображений $c : G \to \mathbb{C}$, называемых характерами, таких, что $c(gh)=c(g)c(h), g,h \in G$.

Теорема 9.3 (С. Бохнер [11). Пусть $\lambda : G \to \mathbb{C}$ - функи,ия на локально компактной абелевой группе, которая удовлетворяет условиям:

1. $\int_G \int_G \lambda(x-y)\overline{c(x)}c(y)d\mu(x)d\mu(y) > 0$, где μ - мера Хаара на группе G;

2. $\lambda(-x)=\overline{\lambda(x)}, \lambda(0)=1$.

Тогда существует мера ν на дуальной группе $\hat{G}$ такая, что функция λ имеет вид

$$\lambda(g)=\int_{\hat{G}} \langle h,g\rangle d\nu(h) \tag{9.21}$$

Рассмотрим, как работает теорема Бохнера в трёх важных частных случаях.

- $\dim H = N < +\infty, G=\mathbb{Z}_N$. Тогда $\hat{G}=\mathbb{Z}_N$ и

$$\lambda(n)=\sum_{k=0}^{N-1} \exp\left(\frac{2\pi nki}{N}\right)\pi_k \tag{9.22}$$

где $\pi_k \geq 0, \sum_{k=0}^{N-1}\pi_k = 1$ - некоторое распределение вероятностей.
Положим $\pi_1 = 1$ (и все остальные - нули). Тогда

$$\lambda(n)=\exp\left(\frac{2\pi ni}{N}\right) \tag{9.23}$$

Рассмотрим канал, демпфирующий фазу, определённый (9.23):

$$\Phi\left(|e_n\rangle\langle e_m|\right)=\exp\left(\frac{2\pi(n-m)i}{N}\right)|e_n\rangle\langle e_m| \tag{9.24}$$

Канал Φ можно представить в виде

$$\Phi(\rho)=\sum_{k=0}^{N-1}\pi_k U^k \rho U^{-k} \tag{9.25}$$

где

$$U|e_n\rangle=\exp\left(\frac{2\pi ni}{N}\right)|e_n\rangle$$

- $\dim H = +\infty, G = \mathbb{Z}$. Тогда $\hat{G} = \mathbb{T} = [0, 2\pi]$ и

$$\lambda(n) = \int_{\mathbb{T}} \exp(nti) d\nu(t) \tag{9.26}$$

где ν - некоторая мера на $\mathbb{T}$. Рассмотрим канал, демпфирующий фазу, определённый (9.26). Для него справедливо представление:

$$\Phi(\rho) = \int_{\mathbb{T}} U_t \rho U_t^* d\nu(t) \tag{9.27}$$

где

$$U_t \left|e_n\right\rangle = \exp(nti) \left|e_n\right\rangle .$$

- $\dim H = +\infty, G = \mathbb{R}$. Тогда $\hat{G} = \mathbb{R}$ и

$$\lambda(x) = \int_{\mathbb{R}} \exp(itx) d\nu(t) \tag{9.28}$$

где ν - некоторая вероятностная мера на $\mathbb{R}$. Рассмотрим канал, демпфирующий фазу, определённый (9.28). Для него справедливо представление:

$$\Phi(\rho) = \int_{\mathbb{R}} U_t \rho U_t^* d\nu(t) \tag{9.29}$$

где

$$\left(U_t f\right)(x) = \exp(itx) f(x), f \in H.$$

7 I Fundamental concepts by Nielsen, Chang

7.0.1 Preface

This book provides an introduction to the main ideas and techniques of the field of quantum computation and quantum information. The rapid rate of progress in this field and its cross-disciplinary nature have made it difficult for newcomers to obtain a broad overview of the most important techniques and results of the field.

Our purpose in this book is therefore twofold. First, we introduce the background material in computer science, mathematics and physics necessary to understand quantum computation and quantum information. This is done at a level comprehensible to readers with a background at least the equal of a beginning graduate student in one or more of these three disciplines; the most important requirements are a certain level of mathematical maturity, and the desire to learn about quantum computation and quantum information. The second purpose of the book is to develop in detail the central results of quantum computation and quantum information. With thorough study the reader should develop a working understanding of the fundamental tools and results of this exciting field, either as part of their general education, or as a prelude to independent research in quantum computation and quantum information.

Introduction to the Tenth Anniversary Edition

Quantum mechanics has the curious distinction of being simultaneously the most successful and the most mysterious of our scientific theories. It was developed in fits and starts over a remarkable period from 1900 to the 1920s, maturing into its current form in the late 1920s. In the decades following the 1920s, physicists had great success applying quantum mechanics to understand the fundamental particles and forces of nature, culminating in the development of the standard model of particle physics. Over the same period, physicists had equally great success in applying quantum mechanics to understand an astonishing range of phenomena in our world, from polymers to semiconductors, from superfluids to superconductors. But, while these developments profoundly advanced our understanding of the natural world, they did only a little to improve our understanding of quantum mechanics.

This began to change in the 1970s and 1980s, when a few pioneers were inspired to ask whether some of the fundamental questions of computer science and information theory could be applied to the study of quantum systems. Instead of looking at quantum systems purely as phenomena to be explained as they are found in nature, they looked at them as systems that can be designed. This seems a small change in perspective, but the implications are profound. No longer is the quantum world taken merely as presented, but instead it can be created. The result was a new perspective that inspired both a resurgence of interest in the fundamentals of quantum mechanics, and also many new questions combining physics, computer science, and information theory. These include questions such as: what are the fundamental physical limitations on the space and time required to construct a quantum state? How much time and space are required for a given dynamical operation? What makes quantum systems difficult to understand and simulate by conventional classical means?

Writing this book in the late 1990s, we were fortunate to be writing at a time when these and other fundamental questions had just crystallized out. Ten years later it is clear such questions offer a sustained force encouraging a broad research program at the foundations of physics and computer science. Quantum information science is here to stay. Although the theoretical foundations of the field remain similar to what we discussed 10 years ago, detailed knowledge in many areas has greatly progressed. Originally, this book served as a comprehensive overview of the field, bringing readers near to the forefront of research. Today, the book provides a basic foundation for understanding the field, appropriate either for someone who desires a broad perspective on quantum information science, or an entryway for further investigation of the latest research literature. Of course,
many fundamental challenges remain, and meeting those challenges promises to stimulate exciting and unexpected links among many disparate parts of physics, computer science, and information theory. We look forward to the decades ahead!

- Michael A. Nielsen and Isaac L. Chuang, March, 2010.

Afterword to the Tenth Anniversary Edition

An enormous amount has happened in quantum information science in the 10 years since the first edition of this book, and in this afterword we cannot summarize even a tiny fraction of that work. But a few especially striking developments merit comment, and may perhaps whet your appetite for more.

Perhaps the most impressive progress has been in the area of experimental implementation. While we are still many years from building large-scale quantum computers, much progress has been made. Superconducting circuits have been used to implement simple two-qubit quantum algorithms, and three-qubit systems are nearly within reach. Qubits based on nuclear spins and single photons have been used, respectively, to demonstrate proof-of-principle for simple forms of quantum error correction and quantum simulation. But the most impressive progress

of all has been made with trapped ion systems, which have been used to implement many two- and three-qubit algorithms and algorithmic building blocks, including the quantum search algorithm and the quantum Fourier transform. Trapped ions have also been used to demonstrate basic quantum communication primitives, including quantum error correction and quantum teleportation.

A second area of progress has been in understanding what physical resources are required to quantum compute. Perhaps the most intriguing breakthrough here has been the discovery that quantum computation can be done via measurement alone. For many years, the conventional wisdom was that coherent superposition-preserving unitary dynamics was an essential part of the power of quantum computers. This conventional wisdom was blown away by the realization that quantum computation can be done without any unitary dynamics at all. Instead, in some new models of quantum computation, quantum measurements alone can be used to do arbitrary quantum computations. The only coherent resource in these models is quantum memory, i.e., the ability to store quantum information. An especially interesting example of these models is the one-way quantum computer, or cluster-state computer. To quantum compute in the cluster-state model requires only that the experimenter have possession of a fixed universal state known as the cluster state. With a cluster state in hand, quantum computation can be implemented simply by doing a sequence of single-qubit measurements, with the particular computation done being determined by which qubits are measured, when they are measured, and how they are measured. This is remarkable: you're given a fixed quantum state, and then quantum compute by "looking" at the individual qubits in appropriate ways.

A third area of progress has been in classically simulating quantum systems. Feynman's pioneering 1982 paper on quantum computing was motivated in part by the observation that quantum systems often seem hard to simulate on conventional classical computers. Of course, at the time there was only a limited understanding of how difficult it is to simulate different quantum systems on ordinary classical computers. But in the 1990s and, especially, in the 2000s, we have learned much about which quantum systems are easy
to simulate, and which are hard. Ingenious algorithms have been developed to classically simulate many quantum systems that were formerly thought to be hard to simulate, in particular, many quantum systems in one spatial dimension, and certain two-dimensional quantum systems. These classical algorithms have been made possible by the development of insightful classical descriptions that capture in a compact way much or all of the essential physics of the system in question. At the same time, we have learned that some systems that formerly seemed simple are surprisingly complex. For example, it has long been known that quantum systems based on a certain type of optical component - what are called linear optical systems - are easily simulated classically. So it was surprising when it was discovered that adding two seemingly innocuous components - single-photon sources and photodetectors - gave linear optics the full power of quantum computation. These and similar investigations have deepened our understanding of which quantum systems are easy to simulate, which quantum systems are hard to simulate, and why.

A fourth area of progress has been a greatly deepened understanding of quantum communication channels. A beautiful and complete theory has been developed of how entangled quantum states can assist classical communication over quantum channels. A plethora of different quantum protocols for communication have been organized into a comprehensive family (headed by "mother" and "father" protocols), unifying much of our understanding of the different types of communication possible with quantum information. A sign of the progress is the disproof of one of the key unsolved conjectures reported in this book (p. 554), namely, that the communication capacity of a quantum channel with product states is equal to the unconstrained capacity (i.e., the capacity with any entangled state allowed as input). But, despite the progress, much remains beyond our understanding. Only very recently, for example, it

was discovered, to considerable surprise, that two quantum channels, each with zero quantum capacity, can have a positive quantum capacity when used together; the analogous result, with classical capacities over classical channels, is known to be impossible.

One of the main motivations for work in quantum information science is the prospect of fast quantum algorithms to solve important computational problems. Here, the progress over the past decade has been mixed. Despite great ingenuity and effort, the chief algorithmic insights stand as they were 10 years ago. There has been considerable technical progress, but we do not yet understand what exactly it is that makes quantum computers powerful, or on what class of problems they can be expected to outperform classical computers.

What is exciting, though, is that ideas from quantum computation have been used to prove a variety of theorems about classical computation. These have included, for example, results about the difficulty of finding certain hidden vectors in a discrete lattice of points. The striking feature is that these proofs, utilizing ideas of quantum computation, are sometimes considerably simpler and more elegant than prior, classical proofs. Thus, an awareness has grown that quantum computation may be a more natural model of computation than the classical model, and perhaps fundamental results may be more easily revealed through the ideas of quantum computation.

Structure of the book

The basic structure of the book is depicted in Figure 1. The book is divided into three parts. The general strategy is to proceed from the concrete to the more abstract whenever possible. Thus we study quantum computation before quantum information; specific quantum error-correcting codes before the more general results of quantum information theory; and throughout the book try to introduce examples before developing general theory.

Part I provides a broad overview of the main ideas and results of the field of quantum computation and quantum information, and develops the background material in computer science, mathematics and physics necessary to understand quantum computation and quantum information in depth. Chapter 1 is an introductory chapter which outlines the historical development and fundamental concepts of the field, highlighting some important open problems along the way. The material has been structured so as to be accessible even without a background in computer science or physics. The background material needed for a more detailed understanding is developed in Chapters 2 and 3 , which treat in depth the fundamental notions of quantum mechanics and computer science, respectively. You may elect to concentrate more or less heavily on different chapters of Part I, depending upon your background, returning later as necessary to fill any gaps in your knowledge of the fundamentals of quantum mechanics and computer science.

Part II describes quantum computation in detail. Chapter 4 describes the fundamen-

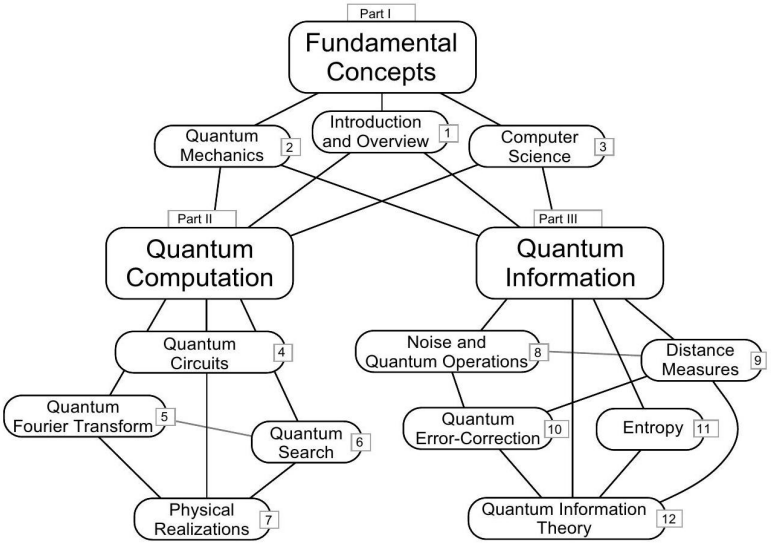


Figure 1. Structure of the book.

tal elements needed to perform quantum computation, and presents many elementary operations which may be used to develop more sophisticated applications of quantum computation. Chapters 5 and 6 describe the quantum Fourier transform and the quantum search algorithm, the two fundamental quantum algorithms presently known. Chapter 5 also explains how the quantum Fourier transform may be used to solve the factoring and discrete logarithm problems, and the importance of these results to cryptography. Chapter 7 describes general design principles and criteria for good physical implementations of quantum computers, using as examples several realizations which have been successfully demonstrated in the laboratory.

Part III is about quantum information: what it is, how information is represented and communicated using quantum states, and how to describe and deal with the corruption of quantum and classical information. Chapter 8 describes the properties of quantum noise which are needed to understand real-world quantum information processing, and the quantum operations formalism, a powerful mathematical tool for understanding quantum noise. Chapter 9 describes distance measures for quantum information which allow us to make quantitatively precise what it means to say that two items of quantum information are similar. Chapter 10 explains quantum error-correcting codes, which may be used to protect quantum computations against the effect of noise. An important result in this chapter is the threshold theorem, which shows that for realistic noise models, noise is in principle not a serious impediment to quantum computation. Chapter 11 introduces the fundamental information-theoretic concept of entropy, explaining many properties of entropy in both classical and quantum information theory. Finally, Chapter 12 discusses the information carrying properties of quantum states and quantum communication chan-
nels, detailing many of the strange and interesting properties such systems can have for the transmission of information both classical and quantum, and for the transmission of secret information.

A large number of exercises and problems appear throughout the book. Exercises are intended to solidify understanding of basic material and appear within the main body of the text. With few exceptions these should be easily solved with a few minutes work. Problems appear at the end of each chapter, and are intended to introduce you to new and interesting material for which there was not enough space in the main text. Often the problems are in multiple parts, intended to develop a particular line of thought in some depth. A few of the problems were unsolved as the book went to press. When this is the case it is noted in the statement of the problem. Each chapter concludes with a summary of the main results of the

chapter, and with a 'History and further reading' section that charts the development of the main ideas in the chapter, giving citations and references for the whole chapter, as well as providing recommendations for further reading.

The front matter of the book contains a detailed Table of Contents, which we encourage you to browse. There is also a guide to nomenclature and notation to assist you as you read.

The end matter of the book contains six appendices, a bibliography, and an index. Appendix 1 reviews some basic definitions, notations, and results in elementary probability theory. This material is assumed to be familiar to readers, and is included for ease of reference. Similarly, Apendix 2 reviews some elementary concepts from group theory, and is included mainly for convenience. Appendix 3 contains a proof of the SolovayKitaev theorem, an important result for quantum computation, which shows that a finite set of quantum gates can be used to quickly approximate an arbitrary quantum gate. Appendix 4 reviews the elementary material on number theory needed to understand the quantum algorithms for factoring and discrete logarithm, and the RSA cryptosystem, which is itself reviewed in Appendix 5. Appendix 6 contains a proof of Lieb's theorem, one of the most important results in quantum computation and quantum information, and a precursor to important entropy inequalities such as the celebrated strong subadditivity inequality. The proofs of the Solovay-Kitaev theorem and Lieb's theorem are lengthy enough that we felt they justified a treatment apart from the main text.

The bibliography contains a listing of all reference materials cited in the text of the book. Our apologies to any researcher whose work we have inadvertently omitted from citation.

The field of quantum computation and quantum information has grown so rapidly in recent years that we have not been able to cover all topics in as much depth as we would have liked. Three topics deserve special mention. The first is the subject of entanglement measures. As we explain in the book, entanglement is a key element in effects such as quantum teleportation, fast quantum algorithms, and quantum error-correction. It is, in short, a resource of great utility in quantum computation and quantum information. There is a thriving research community currently fleshing out the notion of entanglement as a new type of physical resource, finding principles which govern its manipulation and utilization. We felt that these investigations, while enormously promising, are not yet complete enough to warrant the more extensive coverage we have given to other subjects in this book, and we restrict ourselves to a brief taste in Chapter 12. Similarly, the subject of distributed quantum computation (sometimes known as quantum communication complexity) is an enormously promising subject under such active development that we
have not given it a treatment for fear of being obsolete before publication of the book. The implementation of quantum information processing machines has also developed into a fascinating and rich area, and we limit ourselves to but a single chapter on this subject. Clearly, much more can be said about physical implementations, but this would begin to involve many more areas of physics, chemistry, and engineering, which we do not have room for here.

How to use this book

This book may be used in a wide variety of ways. It can be used as the basis for a variety of courses, from short lecture courses on a specific topic in quantum computation and quantum information, through to full-year classes covering the entire field. It can be used for independent study by people who would like to learn just a little about quantum computation and quantum information, or by people who would like to be brought up to the research frontier. It is also intended to act as a reference work for current researchers in the field. We hope that it will be found especially valuable as an introduction for researchers new to the field.

Note to the independent reader

The book is designed to be accessible to the independent reader. A large number of exercises are peppered throughout the text, which can be used as self-tests for understanding of the material in the main text. The Table of Contents and end of chapter summaries should enable you to quickly determine which chapters you wish to study in most depth. The dependency diagram, Figure 1, will help you determine in what order material in the book may be covered.

Note to the teacher

This book covers a diverse range of topics, and can therefore be used as the basis for a wide variety of courses.

A one-semester course on quantum computation could be based upon a selection of material from Chapters 1 through 3, depending on the background of the class, followed by Chapter 4 on quantum circuits, Chapters 5 and 6 on quantum algorithms, and a selection from Chapter 7 on physical implementations, and Chapters 8 through 10 to understand quantum error-correction, with an especial focus on Chapter 10.

A one-semester course on quantum information could be based upon a selection of material from Chapters 1 through 3, depending on the background of the class. Following that, Chapters 8 through 10 on quantum error-correction, followed by Chapters 11 and 12 on quantum entropy and quantum information theory, respectively.

A full year class could cover all material in the book, with time for additional readings selected from the 'History and further reading' section of several chapters. Quantum computation and quantum information also lend themselves ideally to independent research projects for students.

Aside from classes on quantum computation and quantum information, there is another way we hope the book will be used, which is as the text for an introductory class in quantum mechanics for physics students. Conventional introductions to quantum mechanics rely heavily on the mathematical machinery of partial differential equations. We believe this often obscures the fundamental ideas. Quantum computation and quantum information offers an excellent conceptual laboratory for understanding the basic concepts and unique aspects of quantum mechanics, without the use of heavy mathematical machinery. Such a class would focus on the introduction to quantum mechanics in Chapter 2, basic material on quantum circuits in Chapter 4, a selection of material on quantum algorithms from Chapters 5 and 6, Chapter 7 on physical implementations of quantum computation, and then almost any selection of material from Part III of the book, depending upon taste.

Note to the student

We have written the book to be as self-contained as possible. The main exception is that occasionally we have omitted arguments that one really needs to work through oneself to believe; these are usually given as exercises. Let us suggest that you should at least attempt all the exercises as you work through the book. With few exceptions the exercises can be worked out in a few minutes. If you are having a lot of difficulty with many of the exercises it may be a sign that you need to go back and pick up one or more key concepts.

Further reading

As already noted, each chapter concludes with a 'History and further reading' section. There are also a few broad-ranging references that might be of interest to readers. Preskill's [Pre 98*b*] superb lecture notes approach quantum computation and quantum information from a somewhat different point of view than this book. Good overview articles on specific subjects

include (in order of their appearance in this book): Aharonov's review of quantum computation [Aha99 b], Kitaev's review of algorithms and error-correction [Kit97 b], Mosca's thesis on quantum algorithms [Mos99], Fuchs' thesis [Fuc96] on distinguishability and distance measures in quantum information, Gottesman's thesis on quantum errorcorrection [Got97] , Preskill's review of quantum error-correction [Pre97] , Nielsen's thesis on quantum information theory [Nie98], and the reviews of quantum information theory by Bennett and Shor [BS98] and by Bennett and DiVincenzo [BD00]. Other useful references include Gruska's book [Gru99], and the collection of review articles edited by Lo, Spiller, and Popescu[LSP98].

7.0.2 Nomenclature and notation

There are several items of nomenclature and notation which have two or more meanings in common use in the field of quantum computation and quantum information. To prevent confusion from arising, this section collects many of the more frequently used of these items, together with the conventions that will be adhered to in this book.

Linear algebra and quantum mechanics

All vector spaces are assumed to be finite dimensional, unless otherwise noted. In many instances this restriction is unnecessary, or can be removed with some additional technical work, but making the restriction globally makes the presentation more easily comprehensible, and doesn't detract much from many of the intended applications of the results.

A positive operator A is one for which $\langle\psi|A|\psi\rangle \geq 0$ for all $|\psi\rangle$. A positive definite operator A is one for which $\langle\psi|A|\psi\rangle > 0$ for all $|\psi\rangle \neq 0$. The support of an operator is defined to be the vector space orthogonal to its kernel. For a Hermitian operator, this means the vector space spanned by eigenvectors of the operator with non-zero eigenvalues.

The notation U (and often but not always V) will generically be used to denote a unitary operator or matrix. H is usually used to denote a quantum logic gate, the Hadamard gate, and sometimes to denote the Hamiltonian for a quantum system, with the meaning clear from context.

Vectors will sometimes be written in column format, as for example,

$$\left[\begin{array}{c} 1 \\ 2 \end{array} \right], \tag{0.1}$$

and sometimes for readability in the format $(1, 2)$. The latter should be understood as shorthand for a column vector. For two-level quantum systems used as qubits, we shall usually identify the state $|0\rangle$ with the vector (1,0), and similarly $|1\rangle$ with (0,1). We also define the Pauli sigma matrices in the conventional way - see 'Frequently used quantum gates and circuit symbols', below. Most significantly, the convention for the Pauli sigma z matrix is that $\sigma_z|0\rangle = |0\rangle$ and $\sigma_z|1\rangle = -|1\rangle$, which is reverse of what some physicists (but usually not computer scientists or mathematicians) intuitively expect. The origin of this dissonance is that the $+1$ eigenstate of σ_z is often identified by physicists with a so-called 'excited state', and it seems natural to many to identify this with $|1\rangle$, rather than with $|0\rangle$ as is done in this book. Our choice is made in order to be consistent with the usual indexing of matrix elements in linear algebra, which makes it natural to identify the first column of σ_z with the action of σ_z on $|0\rangle$, and the second column with the action on $|1\rangle$. This choice is also in use throughout the quantum computation and quantum information community. In addition to the conventional notations σ_x, σ_y and σ_z for the Pauli sigma matrices, it will also be convenient to use the notations $\sigma_1, \sigma_2, \sigma_3$ for these
three matrices, and to define σ_0 as the 2×2 identity matrix. Most often, however, we use the notations I, X, Y and Z for $\sigma_0, \sigma_1, \sigma_2$ and σ_3, respectively.

Information theory and probability

As befits good information theorists, logarithms are always taken to base two, unless otherwise noted. We use $\log(x)$ to denote logarithms to base 2 , and $\ln(x)$ on those rare occasions when we wish to take a natural logarithm. The term probability distribution is used to refer to a finite set of real numbers, p_x, such that $p_x \geq 0$ and $\sum_x p_x = 1$. The relative entropy of a positive operator A with respect to a positive operator B is defined by $S(A\|B) \equiv \mathrm{tr}(A \log A) - \mathrm{tr}(A \log B)$.

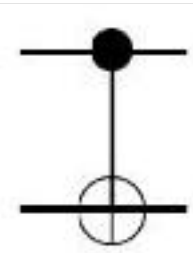
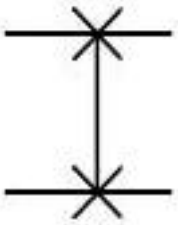
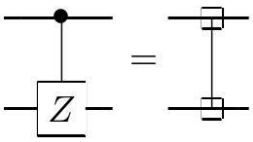
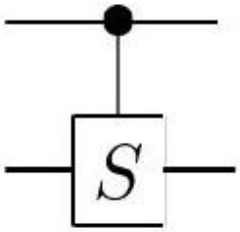
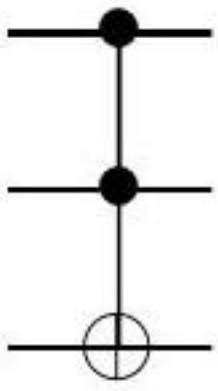
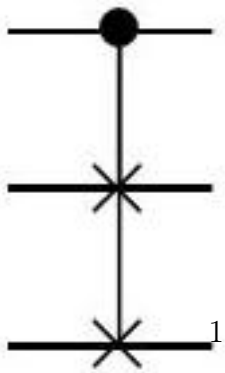
Miscellanea

$\oplus$ denotes modulo two addition. Throughout this book ' z ' is pronounced 'zed'.

Frequently used quantum gates and circuit symbols

Certain schematic symbols are often used to denote unitary transforms which are useful in the design of quantum circuits. For the reader's convenience, many of these are gathered together below. The rows and columns of the unitary transforms are labeled from left to right and top to bottom as $00\ldots0, 00\ldots1$ to $11\ldots1$ with the bottom-most wire being the least significant bit. Note that $e^{i\pi/4}$ is the square root of i, so that the $\pi/8$ gate is the square root of the phase gate, which itself is the square root of the Pauli- Z gate.

Hadamard	$-\boxed{H}-$	$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Pauli- X	$-\boxed{X}-$	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli- Y	$-\boxed{Y}-$	$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli- Z	$-\boxed{Z}-$	$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Phase	$-\boxed{S}-$	$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$	$-\boxed{T}-$	$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$

controlled-NOT		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
swap		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
controlled- Z		
controlled-phase		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{bmatrix}$
Toffoli		$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$
Fredkin (controlled-swap)		$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}$

7.1 1 Introduction and overview

> Science offers the boldest metaphysics of the age. It is a thoroughly human construct, driven by the faith that if we dream, press to discover, explain, and dream again, thereby plunging repeatedly into new terrain, the world will somehow come clearer and we will grasp the true strangeness of the universe. And the strangeness will all prove to be connected, and make sense.
>
> - Edward O. Wilson
>
> Information is physical.
>
> - Rolf Landauer

What are the fundamental concepts of quantum computation and quantum information? How did these concepts develop? To what uses may they be put? How will they be presented in this book? The purpose of this introductory chapter is to answer these questions by developing in broad brushstrokes a picture of the field of quantum computation and quantum information. The intent is to communicate a basic understanding of the central concepts of the field, perspective on how they have been developed, and to help you decide how to approach the rest of the book.

Our story begins in Section 1.1 with an account of the historical context in which quantum computation and quantum information has developed. Each remaining section in the chapter gives a brief introduction to one or more fundamental concepts from the field: quantum bits (Section 1.2), quantum computers, quantum gates and quantum circuits (Section 1.3), quantum algorithms (Section 1.4), experimental quantum information processing (Section 1.5), and quantum information and communication (Section 1.6).

Along the way, illustrative and easily accessible developments such as quantum teleportation and some simple quantum algorithms are given, using the basic mathematics taught in this chapter. The presentation is self-contained, and designed to be accessible even without a background in computer science or physics. As we move along, we give pointers to more in-depth discussions in later chapters, where references and suggestions for further reading may also be found.

If as you read you're finding the going rough, skip on to a spot where you feel more comfortable. At points we haven't been able to avoid using a little technical lingo which won't be completely explained until later in the book. Simply accept it for now, and come back later when you understand all the terminology in more detail. The emphasis in this first chapter is on the big picture, with the details to be filled in later.

7.1.1 1.1 Global perspectives

Quantum computation and quantum information is the study of the information processing tasks that can be accomplished using quantum mechanical systems. Sounds pretty
simple and obvious, doesn't it? Like many simple but profound ideas it was a long time before anybody thought of doing information processing using quantum mechanical systems. To see why this is the case, we must go back in time and look in turn at each of the fields which have contributed fundamental ideas to quantum computation and quantum information - quantum mechanics, computer science, information theory, and cryptography. As we take our short historical tour of these fields, think of yourself first as a physicist, then as a computer scientist, then as an information theorist, and finally as a cryptographer, in order to get some feel for the disparate perspectives which have come together in quantum computation and quantum information.

7.1.2 1.1.1 History of quantum computation and quantum information

Our story begins at the turn of the twentieth century when an unheralded revolution was underway in science. A series of crises had arisen in physics. The problem was that the theories of physics at that time (now dubbed classical physics) were predicting absurdities such as the existence of an 'ultraviolet catastrophe' involving infinite energies, or electrons spiraling inexorably into the atomic nucleus. At first such problems were resolved with the addition of ad hoc hypotheses to classical physics, but as a better understanding of atoms and radiation was gained these attempted explanations became more and more convoluted. The crisis came to a head in the early 1920s after a quarter century of turmoil, and resulted in the creation of the modern theory of quantum mechanics. Quantum mechanics has been an indispensable part of science ever since, and has been applied with enormous success to everything under and inside the Sun, including the structure of the atom, nuclear fusion in stars, superconductors, the structure of DNA, and the elementary particles of Nature.

What is quantum mechanics? Quantum mechanics is a mathematical framework or set of rules for the construction of physical theories. For example, there is a physical theory known as quantum electrodynamics which describes with fantastic accuracy the interaction of atoms and light. Quantum electrodynamics is built up within the framework of quantum mechanics, but it contains specific rules not determined by quantum mechanics. The relationship of quantum mechanics to specific physical theories like quantum electrodynamics is rather like the relationship of a computer's operating system to specific applications software - the operating system sets certain basic parameters and modes of operation, but leaves open how specific tasks are accomplished by the applications.

The rules of quantum mechanics are simple but even experts find them counterintuitive, and the earliest antecedents of quantum computation and quantum information may be found in the long-standing desire of physicists to better understand quantum mechanics. The best known critic of quantum mechanics, Albert Einstein, went to his grave unreconciled with the theory he helped invent. Generations of physicists since have wrestled with quantum mechanics in an effort to make its predictions more palatable. One of the goals of quantum computation and quantum information is to develop tools which sharpen our intuition about quantum mechanics, and make its predictions more transparent to human minds.

For example, in the early 1980s, interest arose in whether it might be possible to use quantum effects to signal faster than light - a big no-no according to Einstein's theory of relativity. The resolution of this problem turns out to hinge on whether it is possible to clone an unknown quantum state, that is, construct a copy of a quantum state. If cloning were possible, then it would be possible to signal faster than light using quantum effects.

However, cloning - so easy to accomplish with classical information (consider the words in front of you, and where they came from!) - turns out not to be possible in general in quantum mechanics. This no-cloning theorem, discovered in the early 1980s, is one of the earliest results of quantum computation and quantum information. Many refinements of the no-cloning theorem have since been developed, and we now have conceptual tools which allow us to understand how well a (necessarily imperfect) quantum cloning device might work. These tools, in turn, have been applied to understand other aspects of quantum mechanics.

A related historical strand contributing to the development of quantum computation and quantum information is the interest, dating to the 1970s, of obtaining complete control over single quantum systems. Applications of quantum mechanics prior to the 1970s typically involved a gross level of control over a bulk sample containing an enormous number of quantum mechanical systems, none of them directly accessible. For example, superconductivity has a superb quantum mechanical explanation. However, because a superconductor involves a huge

(compared to the atomic scale) sample of conducting metal, we can only probe a few aspects of its quantum mechanical nature, with the individual quantum systems constituting the superconductor remaining inaccessible. Systems such as particle accelerators do allow limited access to individual quantum systems, but again provide little control over the constituent systems.

Since the 1970s many techniques for controlling single quantum systems have been developed. For example, methods have been developed for trapping a single atom in an 'atom trap', isolating it from the rest of the world and allowing us to probe many different aspects of its behavior with incredible precision. The scanning tunneling microscope has been used to move single atoms around, creating designer arrays of atoms at will. Electronic devices whose operation involves the transfer of only single electrons have been demonstrated.

Why all this effort to attain complete control over single quantum systems? Setting aside the many technological reasons and concentrating on pure science, the principal answer is that researchers have done this on a hunch. Often the most profound insights in science come when we develop a method for probing a new regime of Nature. For example, the invention of radio astronomy in the 1930s and 1940s led to a spectacular sequence of discoveries, including the galactic core of the Milky Way galaxy, pulsars, and quasars. Low temperature physics has achieved its amazing successes by finding ways to lower the temperatures of different systems. In a similar way, by obtaining complete control over single quantum systems, we are exploring untouched regimes of Nature in the hope of discovering new and unexpected phenomena. We are just now taking our first steps along these lines, and already a few interesting surprises have been discovered in this regime. What else shall we discover as we obtain more complete control over single quantum systems, and extend it to more complex systems?

Quantum computation and quantum information fit naturally into this program. They provide a useful series of challenges at varied levels of difficulty for people devising methods to better manipulate single quantum systems, and stimulate the development of new experimental techniques and provide guidance as to the most interesting directions in which to take experiment. Conversely, the ability to control single quantum systems is essential if we are to harness the power of quantum mechanics for applications to quantum computation and quantum information.

Despite this intense interest, efforts to build quantum information processing systems have resulted in modest success to date. Small quantum computers, capable of doing dozens of operations on a few quantum bits (or qubits) represent the state of the art in quantum computation. Experimental prototypes for doing quantum cryptography - a way of communicating in secret across long distances - have been demonstrated, and are even at the level where they may be useful for some real-world applications. However, it remains a great challenge to physicists and engineers of the future to develop techniques for making large-scale quantum information processing a reality.

Let us turn our attention from quantum mechanics to another of the great intellectual triumphs of the twentieth century, computer science. The origins of computer science are lost in the depths of history. For example, cuneiform tablets indicate that by the time of Hammurabi (circa 1750 B.C.) the Babylonians had developed some fairly sophisticated algorithmic ideas, and it is likely that many of those ideas date to even earlier times.

The modern incarnation of computer science was announced by the great mathematician Alan Turing in a remarkable 1936 paper. Turing developed in detail an abstract notion of what we would now call a programmable computer, a model for computation now known as the Turing machine, in his honor. Turing showed that there is a Universal Turing Machine that can be used to simulate any other Turing machine. Furthermore, he claimed that the Universal Turing Machine completely captures what it means to perform a task by algorithmic means. That is, if an algorithm can be performed on any piece of hardware (say, a modern personal computer), then there is an equivalent algorithm for a Universal Turing Machine which performs exactly

the same task as the algorithm running on the personal computer. This assertion, known as the Church-Turing thesis in honor of Turing and another pioneer of computer science, Alonzo Church, asserts the equivalence between the physical concept of what class of algorithms can be performed on some physical device with the rigorous mathematical concept of a Universal Turing Machine. The broad acceptance of this thesis laid the foundation for the development of a rich theory of computer science.

Not long after Turing's paper, the first computers constructed from electronic components were developed. John von Neumann developed a simple theoretical model for how to put together in a practical fashion all the components necessary for a computer to be fully as capable as a Universal Turing Machine. Hardware development truly took off, though, in 1947, when John Bardeen, Walter Brattain, and Will Shockley developed the transistor. Computer hardware has grown in power at an amazing pace ever since, so much so that the growth was codified by Gordon Moore in 1965 in what has come to be known as Moore's law, which states that computer power will double for constant cost roughly once every two years.

Amazingly enough, Moore's law has approximately held true in the decades since the 1960s. Nevertheless, most observers expect that this dream run will end some time during the first two decades of the twenty-first century. Conventional approaches to the fabrication of computer technology are beginning to run up against fundamental difficulties of size. Quantum effects are beginning to interfere in the functioning of electronic devices as they are made smaller and smaller.

One possible solution to the problem posed by the eventual failure of Moore's law is to move to a different computing paradigm. One such paradigm is provided by the theory of quantum computation, which is based on the idea of using quantum mechanics to perform computations, instead of classical physics. It turns out that while an ordinary computer can be used to simulate a quantum computer, it appears to be impossible to
perform the simulation in an efficient fashion. Thus quantum computers offer an essential speed advantage over classical computers. This speed advantage is so significant that many researchers believe that no conceivable amount of progress in classical computation would be able to overcome the gap between the power of a classical computer and the power of a quantum computer.

What do we mean by 'efficient' versus 'inefficient' simulations of a quantum computer? Many of the key notions needed to answer this question were actually invented before the notion of a quantum computer had even arisen. In particular, the idea of efficient and inefficient algorithms was made mathematically precise by the field of computational complexity. Roughly speaking, an efficient algorithm is one which runs in time polynomial in the size of the problem solved. In contrast, an inefficient algorithm requires superpolynomial (typically exponential) time. What was noticed in the late 1960s and early 1970s was that it seemed as though the Turing machine model of computation was at least as powerful as any other model of computation, in the sense that a problem which could be solved efficiently in some model of computation could also be solved efficiently in the Turing machine model, by using the Turing machine to simulate the other model of computation. This observation was codified into a strengthened version of the ChurchTuring thesis:

Any algorithmic process can be simulated efficiently using a Turing machine.
The key strengthening in the strong Church-Turing thesis is the word efficiently. If the strong Church-Turing thesis is correct, then it implies that no matter what type of machine we use to perform our algorithms, that machine can be simulated efficiently using a standard Turing machine. This is an important strengthening, as it implies that for the purposes of analyzing whether a given computational task can be accomplished efficiently, we may restrict ourselves to the analysis of the Turing machine model of computation.

One class of challenges to the strong Church-Turing thesis comes from the field of analog

computation. In the years since Turing, many different teams of researchers have noticed that certain types of analog computers can efficiently solve problems believed to have no efficient solution on a Turing machine. At first glance these analog computers appear to violate the strong form of the Church-Turing thesis. Unfortunately for analog computation, it turns out that when realistic assumptions about the presence of noise in analog computers are made, their power disappears in all known instances; they cannot efficiently solve problems which are not efficiently solvable on a Turing machine. This lesson - that the effects of realistic noise must be taken into account in evaluating the efficiency of a computational model - was one of the great early challenges of quantum computation and quantum information, a challenge successfully met by the development of a theory of quantum error-correcting codes and fault-tolerant quantum computation. Thus, unlike analog computation, quantum computation can in principle tolerate a finite amount of noise and still retain its computational advantages.

The first major challenge to the strong Church-Turing thesis arose in the mid 1970s, when Robert Solovay and Volker Strassen showed that it is possible to test whether an integer is prime or composite using a randomized algorithm. That is, the Solovay-Strassen test for primality used randomness as an essential part of the algorithm. The algorithm did not determine whether a given integer was prime or composite with certainty. Instead, the algorithm could determine that a number was probably prime or else composite with
certainty. By repeating the Solovay-Strassen test a few times it is possible to determine with near certainty whether a number is prime or composite. The Solovay-Strassen test was of especial significance at the time it was proposed as no deterministic test for primality was then known, nor is one known at the time of this writing. Thus, it seemed as though computers with access to a random number generator would be able to efficiently perform computational tasks with no efficient solution on a conventional deterministic Turing machine. This discovery inspired a search for other randomized algorithms which has paid off handsomely, with the field blossoming into a thriving area of research.

Randomized algorithms pose a challenge to the strong Church-Turing thesis, suggesting that there are efficiently soluble problems which, nevertheless, cannot be efficiently solved on a deterministic Turing machine. This challenge appears to be easily resolved by a simple modification of the strong Church-Turing thesis:

Any algorithmic process can be simulated efficiently using a probabilistic Turing machine.

This ad hoc modification of the strong Church-Turing thesis should leave you feeling rather queasy. Might it not turn out at some later date that yet another model of computation allows one to efficiently solve problems that are not efficiently soluble within Turing's model of computation? Is there any way we can find a single model of computation which is guaranteed to be able to efficiently simulate any other model of computation?

Motivated by this question, in 1985 David Deutsch asked whether the laws of physics could be use to derive an even stronger version of the Church-Turing thesis. Instead of adopting ad hoc hypotheses, Deutsch looked to physical theory to provide a foundation for the Church-Turing thesis that would be as secure as the status of that physical theory. In particular, Deutsch attempted to define a computational device that would be capable of efficiently simulating an arbitrary physical system. Because the laws of physics are ultimately quantum mechanical, Deutsch was naturally led to consider computing devices based upon the principles of quantum mechanics. These devices, quantum analogues of the machines defined forty-nine years earlier by Turing, led ultimately to the modern conception of a quantum computer used in this book.

At the time of writing it is not clear whether Deutsch's notion of a Universal Quantum Computer is sufficient to efficiently simulate an arbitrary physical system. Proving or refuting this conjecture is one of the great open problems of the field of quantum computation and

quantum information. It is possible, for example, that some effect of quantum field theory or an even more esoteric effect based in string theory, quantum gravity or some other physical theory may take us beyond Deutsch's Universal Quantum Computer, giving us a still more powerful model for computation. At this stage, we simply don't know.

What Deutsch's model of a quantum computer did enable was a challenge to the strong form of the Church-Turing thesis. Deutsch asked whether it is possible for a quantum computer to efficiently solve computational problems which have no efficient solution on a classical computer, even a probabilistic Turing machine. He then constructed a simple example suggesting that, indeed, quantum computers might have computational powers exceeding those of classical computers.

This remarkable first step taken by Deutsch was improved in the subsequent decade by many people, culminating in Peter Shor's 1994 demonstration that two enormously important problems - the problem of finding the prime factors of an integer, and the so-called 'discrete logarithm' problem - could be solved efficiently on a quantum computer. This attracted widespread interest because these two problems were and still are widely believed to have no efficient solution on a classical computer. Shor's results are a powerful indication that quantum computers are more powerful than Turing machines, even probabilistic Turing machines. Further evidence for the power of quantum computers came in 1995 when Lov Grover showed that another important problem - the problem of conducting a search through some unstructured search space - could also be sped up on a quantum computer. While Grover's algorithm did not provide as spectacular a speedup as Shor's algorithms, the widespread applicability of search-based methodologies has excited considerable interest in Grover's algorithm.

At about the same time as Shor's and Grover's algorithms were discovered, many people were developing an idea Richard Feynman had suggested in 1982. Feynman had pointed out that there seemed to be essential difficulties in simulating quantum mechanical systems on classical computers, and suggested that building computers based on the principles of quantum mechanics would allow us to avoid those difficulties. In the 1990s several teams of researchers began fleshing this idea out, showing that it is indeed possible to use quantum computers to efficiently simulate systems that have no known efficient simulation on a classical computer. It is likely that one of the major applications of quantum computers in the future will be performing simulations of quantum mechanical systems too difficult to simulate on a classical computer, a problem with profound scientific and technological implications.

What other problems can quantum computers solve more quickly than classical computers? The short answer is that we don't know. Coming up with good quantum algorithms seems to be hard. A pessimist might think that's because there's nothing quantum computers are good for other than the applications already discovered! We take a different view. Algorithm design for quantum computers is hard because designers face two difficult problems not faced in the construction of algorithms for classical computers. First, our human intuition is rooted in the classical world. If we use that intuition as an aid to the construction of algorithms, then the algorithmic ideas we come up with will be classical ideas. To design good quantum algorithms one must 'turn off' one's classical intuition for at least part of the design process, using truly quantum effects to achieve the desired algorithmic end. Second, to be truly interesting it is not enough to design an algorithm that is merely quantum mechanical. The algorithm must be better than any existing classical algorithm! Thus, it is possible that one may find an algorithm which makes use of truly quantum aspects of quantum mechanics, that is nevertheless not of widespread interest because classical algorithms with comparable performance characteristics exist. The combination of these two problems makes the construction of new quantum algorithms a challenging problem for the future.

Even more broadly, we can ask if there are any generalizations we can make about the power of quantum computers versus classical computers. What is it that makes quantum computers

more powerful than classical computers - assuming that this is indeed the case? What class of problems can be solved efficiently on a quantum computer, and how does that class compare to the class of problems that can be solved efficiently on a classical computer? One of the most exciting things about quantum computation and quantum information is how little is known about the answers to these questions! It is a great challenge for the future to understand these questions better.

Having come up to the frontier of quantum computation, let's switch to the history of another strand of thought contributing to quantum computation and quantum information: information theory. At the same time computer science was exploding in the 1940s, another revolution was taking place in our understanding of communication. In 1948 Claude Shannon published a remarkable pair of papers laying the foundations for the modern theory of information and communication.

Perhaps the key step taken by Shannon was to mathematically define the concept of information. In many mathematical sciences there is considerable flexibility in the choice of fundamental definitions. Try thinking naively for a few minutes about the following question: how would you go about mathematically defining the notion of an information source? Several different answers to this problem have found widespread use; however, the definition Shannon came up with seems to be far and away the most fruitful in terms of increased understanding, leading to a plethora of deep results and a theory with a rich structure which seems to accurately reflect many (though not all) real-world communications problems.

Shannon was interested in two key questions related to the communication of information over a communications channel. First, what resources are required to send information over a communications channel? For example, telephone companies need to know how much information they can reliably transmit over a given telephone cable. Second, can information be transmitted in such a way that it is protected against noise in the communications channel?

Shannon answered these two questions by proving the two fundamental theorems of information theory. The first, Shannon's noiseless channel coding theorem, quantifies the physical resources required to store the output from an information source. Shannon's second fundamental theorem, the noisy channel coding theorem, quantifies how much information it is possible to reliably transmit through a noisy communications channel. To achieve reliable transmission in the presence of noise, Shannon showed that error-correcting codes could be used to protect the information being sent. Shannon's noisy channel coding theorem gives an upper limit on the protection afforded by errorcorrecting codes. Unfortunately, Shannon's theorem does not explicitly give a practically useful set of error-correcting codes to achieve that limit. From the time of Shannon's papers until today, researchers have constructed more and better classes of error-correcting codes in their attempts to come closer to the limit set by Shannon's theorem. A sophisticated theory of error-correcting codes now exists offering the user a plethora of choices in their quest to design a good error-correcting code. Such codes are used in a multitude of places including, for example, compact disc players, computer modems, and satellite communications systems.

Quantum information theory has followed with similar developments. In 1995, Ben Schumacher provided an analogue to Shannon's noiseless coding theorem, and in the process defined the 'quantum bit' or 'qubit' as a tangible physical resource. However, no analogue to Shannon's noisy channel coding theorem is yet known for quantum information. Nevertheless, in analogy to their classical counterparts, a theory of quantum error-correction has been developed which, as already mentioned, allows quantum computers to compute effectively in the presence of noise, and also allows communication over noisy quantum channels to take place reliably.

Indeed, classical ideas of error-correction have proved to be enormously important in developing and understanding quantum error-correcting codes. In 1996, two groups working independently, Robert Calderbank and Peter Shor, and Andrew Steane, discov-

ered an important class of quantum codes now known as CSS codes after their initials. This work has since been subsumed by the stabilizer codes, independently discovered by Robert Calderbank, Eric Rains, Peter Shor and Neil Sloane, and by Daniel Gottesman. By building upon the basic ideas of classical linear coding theory, these discoveries greatly facilitated a rapid understanding of quantum error-correcting codes and their application to quantum computation and quantum information.

The theory of quantum error-correcting codes was developed to protect quantum states against noise. What about transmitting ordinary classical information using a quantum channel? How efficiently can this be done? A few surprises have been discovered in this arena. In 1992 Charles Bennett and Stephen Wiesner explained how to transmit two classical bits of information, while only transmitting one quantum bit from sender to receiver, a result dubbed superdense coding.

Even more interesting are the results in distributed quantum computation. Imagine you have two computers networked, trying to solve a particular problem. How much communication is required to solve the problem? Recently it has been shown that quantum computers can require exponentially less communication to solve certain problems than would be required if the networked computers were classical! Unfortunately, as yet these problems are not especially important in a practical setting, and suffer from some undesirable technical restrictions. A major challenge for the future of quantum computation and quantum information is to find problems of real-world importance for which distributed quantum computation offers a substantial advantage over distributed classical computation.

Let's return to information theory proper. The study of information theory begins with the properties of a single communications channel. In applications we often do not deal with a single communications channel, but rather with networks of many channels. The subject of networked information theory deals with the information carrying properties of such networks of communications channels, and has been developed into a rich and intricate subject.

By contrast, the study of networked quantum information theory is very much in its infancy. Even for very basic questions we know little about the information carrying abilities of networks of quantum channels. Several rather striking preliminary results have been found in the past few years; however, no unifying theory of networked information theory exists for quantum channels. One example of networked quantum information theory should suffice to convince you of the value such a general theory would have. Imagine that we are attempting to send quantum information from Alice to Bob through a noisy quantum channel. If that channel has zero capacity for quantum information, then it is impossible to reliably send any information from Alice to Bob. Imagine instead that we consider two copies of the channel, operating in synchrony. Intuitively it is clear (and can be rigorously justified) that such a channel also has zero capacity to send quantum information. However, if we instead reverse the direction of one of the channels, as illustrated in Figure 1.1, it turns out that sometimes we can obtain a non-zero capacity for the transmission of information from Alice to Bob! Counter-intuitive properties like this illustrate the strange nature of quantum information. Better understanding the information carrying properties of networks of quantum channels is a major open problem of quantum computation and quantum information.

Let's switch fields one last time, moving to the venerable old art and science of cryptography. Broadly speaking, cryptography is the problem of doing communication or

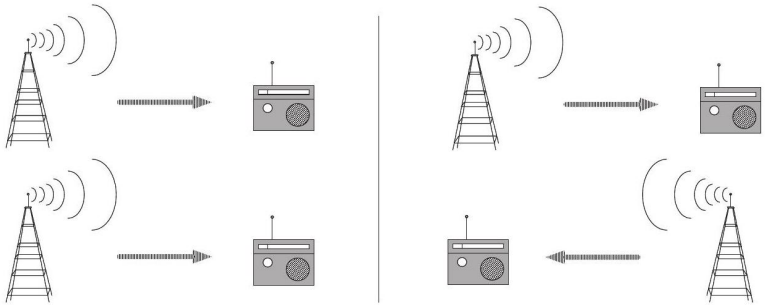


Figure 1.1. Classically, if we have two very noisy channels of zero capacity running side by side, then the combined channel has zero capacity to send information. Not surprisingly, if we reverse the direction of one of the channels, we still have zero capacity to send information. Quantum mechanically, reversing one of the zero capacity channels can actually allow us to send information!

computation involving two or more parties who may not trust one another. The best known cryptographic problem is the transmission of secret messages. Suppose two parties wish to communicate in secret. For example, you may wish to give your credit card number to a merchant in exchange for goods, hopefully without any malevolent third party intercepting your credit card number. The way this is done is to use a cryptographic protocol. We'll describe in detail how cryptographic protocols work later in the book, but for now it will suffice to make a few simple distinctions. The most important distinction is between private key cryptosystems and public key cryptosystems.

The way a private key cryptosystem works is that two parties, 'Alice' and 'Bob', wish to communicate by sharing a private key, which only they know. The exact form of the key doesn't matter at this point - think of a string of zeroes and ones. The point is that this key is used by Alice to encrypt the information she wishes to send to Bob. After Alice encrypts she sends the encrypted information to Bob, who must now recover the original information. Exactly how Alice encrypts the message depends upon the private *key*, so that to recover the original message Bob needs to know the private key, in order to undo the transformation Alice applied.

Unfortunately, private key cryptosystems have some severe problems in many contexts. The most basic problem is how to distribute the keys? In many ways, the key distribution problem is just as difficult as the original problem of communicating in private - a malevolent third party may be eavesdropping on the key distribution, and then use the intercepted key to decrypt some of the message transmission.

One of the earliest discoveries in quantum computation and quantum information was that quantum mechanics can be used to do key distribution in such a way that Alice and Bob's security can not be compromised. This procedure is known as quantum cryptography or quantum key distribution. The basic idea is to exploit the quantum mechanical principle that observation in general disturbs the system being observed. Thus, if there is an eavesdropper listening in as Alice and Bob attempt to transmit their key, the presence of the eavesdropper will be visible as a disturbance of the communications channel Alice and Bob are using to establish the key. Alice and Bob can then throw out the key bits established while the eavesdropper was listening in, and start over. The first quantum cryptographic ideas were proposed by Stephen Wiesner in the late 1960s, but unfortunately were not accepted for publication! In 1984 Charles Bennett and Gilles Brassard, building on Wiesner's earlier work, proposed a protocol using quantum mechanics to distribute keys between Alice and Bob, without any possibility of a compromise. Since then numerous quantum cryptographic protocols have been proposed, and experimental prototypes developed. At the time of this writing, the experimental prototypes are nearing the stage where they may be

useful in limited-scale real-world applications.

The second major type of cryptosystem is the public key cryptosystem. Public key cryptosystems don't rely on Alice and Bob sharing a secret key in advance. Instead, Bob simply publishes a 'public key', which is made available to the general public. Alice can make use of this public key to encrypt a message which she sends to Bob. What is interesting is that a third party cannot use Bob's public key to decrypt the message! Strictly speaking, we shouldn't say cannot. Rather, the encryption transformation is chosen in a very clever and non-trivial way so that it is extremely difficult (though not impossible) to invert, given only knowledge of the public key. To make inversion easy, Bob has a secret key matched to his public key, which together enable him to easily perform the decryption. This secret key is not known to anybody other than Bob, who can therefore be confident that only he can read the contents of Alice's transmission, to the extent that it is unlikely that anybody else has the computational power to invert the encryption, given only the public key. Public key cryptosystems solve the key distribution problem by making it unnecessary for Alice and Bob to share a private key before communicating.

Rather remarkably, public key cryptography did not achieve widespread use until the mid-1970s, when it was proposed independently by Whitfield Diffie and Martin Hellman, and by Ralph Merkle, revolutionizing the field of cryptography. A little later, Ronald Rivest, Adi Shamir, and Leonard Adleman developed the RSA cryptosystem, which at the time of writing is the most widely deployed public key cryptosystem, believed to offer a fine balance of security and practical usability. In 1997 it was disclosed that these ideas - public key cryptography, the Diffie-Hellman and RSA cryptosystems - were actually invented in the late 1960s and early 1970s by researchers working at the British intelligence agency GCHQ.

The key to the security of public key cryptosystems is that it should be difficult to invert the encryption stage if only the public key is available. For example, it turns out that inverting the encryption stage of RSA is a problem closely related to factoring. Much of the presumed security of RSA comes from the belief that factoring is a problem hard to solve on a classical computer. However, Shor's fast algorithm for factoring on a quantum computer could be used to break RSA! Similarly, there are other public key cryptosystems which can be broken if a fast algorithm for solving the discrete logarithm problem - like Shor's quantum algorithm for discrete logarithm - were known. This practical application of quantum computers to the breaking of cryptographic codes has excited much of the interest in quantum computation and quantum information.

We have been looking at the historical antecedents for quantum computation and quantum information. Of course, as the field has grown and matured, it has sprouted its own subfields of research, whose antecedents lie mainly within quantum computation and quantum information.

Perhaps the most striking of these is the study of quantum entanglement. Entanglement is a uniquely quantum mechanical resource that plays a key role in many of the most interesting applications of quantum computation and quantum information; entanglement is iron to the classical world's bronze age. In recent years there has been a
tremendous effort trying to better understand the properties of entanglement considered as a fundamental resource of Nature, of comparable importance to energy, information, entropy, or any other fundamental resource. Although there is as yet no complete theory of entanglement, some progress has been made in understanding this strange property of quantum mechanics. It is hoped by many researchers that further study of the properties of entanglement will yield insights that facilitate the development of new applications in quantum computation and quantum information.

7.1.3 1.1.2 Future directions

We've looked at some of the history and present status of quantum computation and quantum information. What of the future? What can quantum computation and quantum information offer to science, to technology, and to humanity? What benefits does quantum computation and quantum information confer upon its parent fields of computer science, information theory, and physics? What are the key open problems of quantum computation and quantum information? We will make a few very brief remarks about these overarching questions before moving onto more detailed investigations.

Quantum computation and quantum information has taught us to think physically about computation, and we have discovered that this approach yields many new and exciting capabilities for information processing and communication. Computer scientists and information theorists have been gifted with a new and rich paradigm for exploration. Indeed, in the broadest terms we have learned that any physical theory, not just quantum mechanics, may be used as the basis for a theory of information processing and communication. The fruits of these explorations may one day result in information processing devices with capabilities far beyond today's computing and communications systems, with concomitant benefits and drawbacks for society as a whole.

Quantum computation and quantum information certainly offer challenges aplenty to physicists, but it is perhaps a little subtle what quantum computation and quantum information offers to physics in the long term. We believe that just as we have learned to think physically about computation, we can also learn to think computationally about physics. Whereas physics has traditionally been a discipline focused on understanding 'elementary' objects and simple systems, many interesting aspects of Nature arise only when things become larger and more complicated. Chemistry and engineering deal with such complexity to some extent, but most often in a rather ad hoc fashion. One of the messages of quantum computation and information is that new tools are available for traversing the gulf between the small and the relatively complex: computation and algorithms provide systematic means for constructing and understanding such systems. Applying ideas from these fields is already beginning to yield new insights into physics. It is our hope that this perspective will blossom in years to come into a fruitful way of understanding all aspects of physics.

We've briefly examined some of the key motivations and ideas underlying quantum computation and quantum information. Over the remaining sections of this chapter we give a more technical but still accessible introduction to these motivations and ideas, with the hope of giving you a bird's-eye view of the field as it is presently poised.

7.1.4 1.2 Quantum bits

The bit is the fundamental concept of classical computation and classical information. Quantum computation and quantum information are built upon an analogous concept, the quantum bit, or qubit for short. In this section we introduce the properties of single and multiple qubits, comparing and contrasting their properties to those of classical bits.

What is a qubit? We're going to describe qubits as mathematical objects with certain specific properties. 'But hang on', you say, 'I thought qubits were physical objects.' It's true that qubits, like bits, are realized as actual physical systems, and in Section 1.5 and Chapter 7 we describe in detail how this connection between the abstract mathematical point of view and real systems is made. However, for the most part we treat qubits as abstract mathematical objects. The beauty of treating qubits as abstract entities is that it gives us the freedom to construct a general theory of quantum computation and quantum information which does not depend upon a specific system for its realization.

What then is a qubit? Just as a classical bit has a state - either 0 or 1 - a qubit also has a state. Two possible states for a qubit are the states $|0\rangle$ and $|1\rangle$, which as you might guess correspond to the states 0 and 1 for a classical bit. Notation like ' $\rangle$ ' is called the Dirac notation, and we'll be seeing it often, as it's the standard notation for states in quantum mechanics. The difference between bits and qubits is that a qubit can be in a state other than $|0\rangle$ or $|1\rangle$. It is also possible to form linear combinations of states, often called superpositions:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle. \tag{1.1}$$

The numbers α and β are complex numbers, although for many purposes not much is lost by thinking of them as real numbers. Put another way, the state of a qubit is a vector in a two-dimensional complex vector space. The special states $|0\rangle$ and $|1\rangle$ are known as computational basis states, and form an orthonormal basis for this vector space.

We can examine a bit to determine whether it is in the state 0 or 1 . For example, computers do this all the time when they retrieve the contents of their memory. Rather remarkably, we cannot examine a qubit to determine its quantum state, that is, the values of α and β. Instead, quantum mechanics tells us that we can only acquire much more restricted information about the quantum state. When we measure a qubit we get either the result 0 , with probability $|\alpha|^2$, or the result 1 , with probability $|\beta|^2$. Naturally, $|\alpha|^2 + |\beta|^2 = 1$, since the probabilities must sum to one. Geometrically, we can interpret this as the condition that the qubit's state be normalized to length 1 . Thus, in general a qubit's state is a unit vector in a two-dimensional complex vector space.

This dichotomy between the unobservable state of a qubit and the observations we can make lies at the heart of quantum computation and quantum information. In most of our abstract models of the world, there is a direct correspondence between elements of the abstraction and the real world, just as an architect's plans for a building are in correspondence with the final building. The lack of this direct correspondence in quantum mechanics makes it difficult to intuit the behavior of quantum systems; however, there is an indirect correspondence, for qubit states can be manipulated and transformed in ways which lead to measurement outcomes which depend distinctly on the different properties of the state. Thus, these quantum states have real, experimentally verifiable consequences, which we shall see are essential to the power of quantum computation and quantum information.

The ability of a qubit to be in a superposition state runs counter to our 'common sense' understanding of the physical world around us. A classical bit is like a coin: either heads or tails up. For imperfect coins, there may be intermediate states like having it balanced on an edge, but those can be disregarded in the ideal case. By contrast, a qubit can exist in a continuum of states between $|0\rangle$ and $|1\rangle$ - until it is observed. Let us emphasize again that when a qubit is measured, it only ever gives ' 0 ' or ' 1 ' as the measurement result - probabilistically. For example, a qubit can be in the state

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, \tag{1.2}$$

which, when measured, gives the result 0 fifty percent $\left(|1/\sqrt{2}|^2\right)$ of the time, and the result 1 fifty percent of the time. We will return often to this state, which is sometimes denoted $|+\rangle$.

Despite this strangeness, qubits are decidedly real, their existence and behavior extensively validated by experiments (discussed in Section 1.5 and Chapter 7), and many different physical systems can be used to realize qubits. To get a concrete feel for how a qubit can be realized it may be helpful to list some of the ways this realization may occur: as the two different polarizations of a photon; as the alignment of a nuclear spin in a uniform magnetic field; as two states of an electron orbiting a single atom such as shown in Figure 1.2. In the atom model, the electron can exist in either the so-called 'ground' or 'excited' states, which we'll call $|0\rangle$ and

$|1\rangle$, respectively. By shining light on the atom, with appropriate energy and for an appropriate length of time, it is possible to move the electron from the $|0\rangle$ state to the $|1\rangle$ state and vice versa. But more interestingly, by reducing the time we shine the light, an electron initially in the state $|0\rangle$ can be moved 'halfway' between $|0\rangle$ and $|1\rangle$, into the $|+\rangle$ state.

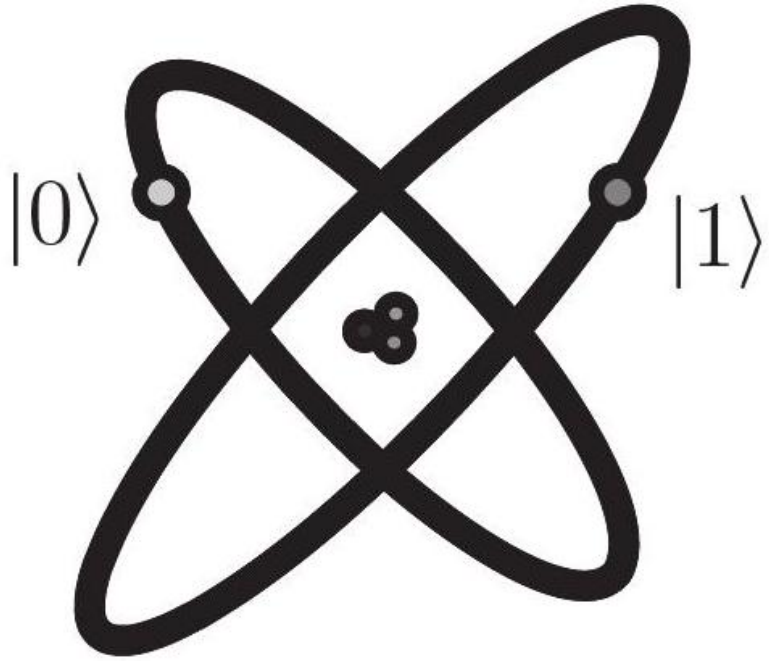


Figure 1.2. Qubit represented by two electronic levels in an atom.

Naturally, a great deal of attention has been given to the 'meaning' or 'interpretation' that might be attached to superposition states, and of the inherently probabilistic nature of observations on quantum systems. However, by and large, we shall not concern ourselves with such discussions in this book. Instead, our intent will be to develop mathematical and conceptual pictures which are predictive.

One picture useful in thinking about qubits is the following geometric representation.

Because $|\alpha|^2 + |\beta|^2 = 1$, we may rewrite Equation (1.1) as

$$|\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right), \tag{1.3}$$

where θ, φ and γ are real numbers. In Chapter 2 we will see that we can ignore the factor of $e^{i\gamma}$ out the front, because it has no observable effects, and for that reason we can effectively write

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle. \tag{1.4}$$

The numbers θ and φ define a point on the unit three-dimensional sphere, as shown in Figure 1.3. This sphere is often called the Bloch sphere; it provides a useful means of visualizing the state of a single qubit, and often serves as an excellent testbed for ideas about quantum computation and quantum information. Many of the operations on single qubits which we describe later in this chapter are neatly described within the Bloch sphere picture. However, it must be kept in mind that this intuition is limited because there is no simple generalization of the Bloch sphere known for multiple qubits.

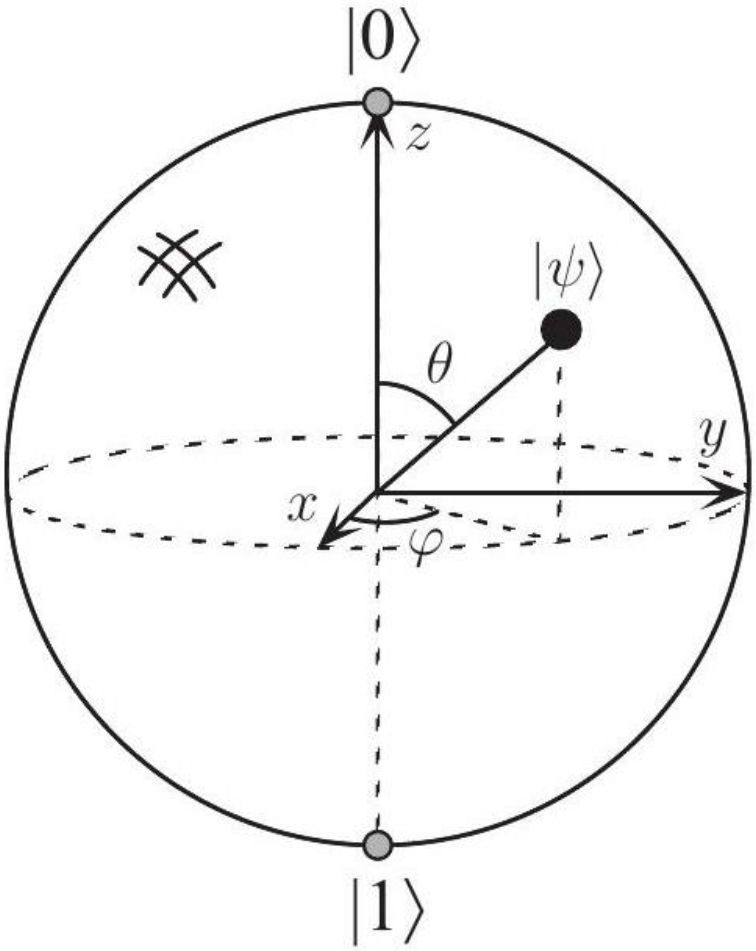


Figure 1.3. Bloch sphere representation of a qubit.

How much information is represented by a qubit? Paradoxically, there are an infinite number of points on the unit sphere, so that in principle one could store an entire text of Shakespeare in the infinite binary expansion of θ. However, this conclusion turns out to be misleading, because of the behavior of a qubit when observed. Recall that measurement of a qubit will give only either 0 or 1 . Furthermore, measurement changes the state of a qubit, collapsing it from its superposition of $|0\rangle$ and $|1\rangle$ to the specific state consistent with the measurement result. For example, if measurement of $|+\rangle$ gives 0 , then the post-measurement state of the qubit will be $|0\rangle$. Why does this type of collapse occur? Nobody knows. As discussed in Chapter 2, this behavior is simply one of the fundamental postulates of quantum mechanics. What is relevant for our purposes is that from a single measurement one obtains only a single bit of information about the state of the qubit, thus resolving the apparent paradox. It turns out that only if infinitely many
identically prepared qubits were measured would one be able to determine α and β for a qubit in the state given in Equation (1.1).

But an even more interesting question to ask might be: how much information is represented by a qubit if we do not measure it? This is a trick question, because how can one quantify information if it cannot be measured? Nevertheless, there is something conceptually important here, because when Nature evolves a closed quantum system of qubits, not performing any 'measurements', she apparently does keep track of all the continuous variables describing the state, like α and β. In a sense, in the state of a qubit, Nature conceals a great deal of 'hidden information'. And even more interestingly, we will see shortly that the potential amount of this extra 'information' grows exponentially with the number of qubits. Understanding this hidden

quantum information is a question that we grapple with for much of this book, and which lies at the heart of what makes quantum mechanics a powerful tool for information processing.

7.1.5 1.2.1 Multiple qubits

Hilbert space is a big place.

- Carlton Caves

Suppose we have two qubits. If these were two classical bits, then there would be four possible states, $00, 01, 10$, and 11 . Correspondingly, a two qubit system has four computational basis states denoted $|00\rangle, |01\rangle, |10\rangle, |11\rangle$. A pair of qubits can also exist in superpositions of these four states, so the quantum state of two qubits involves associating a complex coefficient - sometimes called an amplitude - with each computational basis state, such that the state vector describing the two qubits is

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle. \tag{1.5}$$

Similar to the case for a single qubit, the measurement result $x(= 00, 01, 10 \text{ or } 11)$ occurs with probability $|\alpha_x|^2$, with the state of the qubits after the measurement being $|x\rangle$. The condition that probabilities sum to one is therefore expressed by the normalization condition that $\sum_{x\in\{0,1\}^2} |\alpha_x|^2 = 1$, where the notation ' $\{0,1\}^{2'}$ means 'the set of strings of length two with each letter being either zero or one'. For a two qubit system, we could measure just a subset of the qubits, say the first qubit, and you can probably guess how this works: measuring the first qubit alone gives 0 with probability $|\alpha_{00}|^2 + |\alpha_{01}|^2$, leaving the post-measurement state

$$|\psi'\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}. \tag{1.6}$$

Note how the post-measurement state is re-normalized by the factor $\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}$ so that it still satisfies the normalization condition, just as we expect for a legitimate quantum state.

An important two qubit state is the Bell state or EPR pair,

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}. \tag{1.7}$$

This innocuous-looking state is responsible for many surprises in quantum computation and quantum information. It is the key ingredient in quantum teleportation and superdense coding, which we'll come to in Section 1.3.7 and Section 2.3, respectively, and the prototype for many other interesting quantum states. The Bell state has the property that upon measuring the first qubit, one obtains two possible results: 0 with probability $1/2$, leaving the post-measurement state $|\varphi'\rangle = |00\rangle$, and 1 with probability $1/2$, leaving $|\varphi'\rangle = |11\rangle$. As a result, a measurement of the second qubit always gives the same result as the measurement of the first qubit. That is, the measurement outcomes are correlated. Indeed, it turns out that other types of measurements can be performed on the Bell state, by first applying some operations to the first or second qubit, and that interesting correlations still exist between the result of a measurement on the first and second qubit. These correlations have been the subject of intense interest ever since a famous paper by Einstein, Podolsky and Rosen, in which they first pointed out the strange properties of states like the Bell state. EPR's insights were taken up and greatly improved by John Bell, who proved an amazing result: the measurement correlations in the Bell state are stronger than could ever exist between classical systems. These results, described

in detail in Section 2.6, were the first intimation that quantum mechanics allows information processing beyond what is possible in the classical world.

More generally, we may consider a system of n qubits. The computational basis states of this system are of the form $|x_1 x_2 \ldots x_n\rangle$, and so a quantum state of such a system is specified by 2^n amplitudes. For $n = 500$ this number is larger than the estimated number of atoms in the Universe! Trying to store all these complex numbers would not be possible on any conceivable classical computer. Hilbert space is indeed a big place. In principle, however, Nature manipulates such enormous quantities of data, even for systems containing only a few hundred atoms. It is as if Nature were keeping 2^{500} hidden pieces of scratch paper on the side, on which she performs her calculations as the system evolves. This enormous potential computational power is something we would very much like to take advantage of. But how can we think of quantum mechanics as computation?

7.1.6 1.3 Quantum computation

Changes occurring to a quantum state can be described using the language of quantum computation. Analogous to the way a classical computer is built from an electrical circuit containing wires and logic gates, a quantum computer is built from a quantum circuit containing wires and elementary quantum gates to carry around and manipulate the quantum information. In this section we describe some simple quantum gates, and present several example circuits illustrating their application, including a circuit which teleports qubits!

7.1.7 1.3.1 Single qubit gates

Classical computer circuits consist of wires and logic gates. The wires are used to carry information around the circuit, while the logic gates perform manipulations of the information, converting it from one form to another. Consider, for example, classical single bit logic gates. The only non-trivial member of this class is the not gate, whose operation is defined by its truth table, in which $0 \rightarrow 1$ and $1 \rightarrow 0$, that is, the 0 and 1 states are interchanged.

Can an analogous quantum not gate for qubits be defined? Imagine that we had some process which took the state $|0\rangle$ to the state $|1\rangle$, and vice versa. Such a process would obviously be a good candidate for a quantum analogue to the NOT gate. However, specifying the action of the gate on the states $|0\rangle$ and $|1\rangle$ does not tell us what happens to superpositions of the states $|0\rangle$ and $|1\rangle$, without further knowledge about the properties of quantum gates. In fact, the quantum not gate acts linearly, that is, it takes the state

$$\alpha|0\rangle + \beta|1\rangle \tag{1.8}$$

to the corresponding state in which the role of $|0\rangle$ and $|1\rangle$ have been interchanged,

$$\alpha|1\rangle + \beta|0\rangle. \tag{1.9}$$

Why the quantum not gate acts linearly and not in some nonlinear fashion is a very interesting question, and the answer is not at all obvious. It turns out that this linear behavior is a general property of quantum mechanics, and very well motivated empirically; moreover, nonlinear behavior can lead to apparent paradoxes such as time travel, faster-than-light communication, and violations of the second laws of thermodynamics. We'll explore this point in more depth in later chapters, but for now we'll just take it as given.

There is a convenient way of representing the quantum not gate in matrix form, which follows directly from the linearity of quantum gates. Suppose we define a matrix X to represent the quantum not gate as follows:

$$X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{1.10}$$

(The notation X for the quantum NOT is used for historical reasons.) If the quantum state $\alpha|0\rangle + \beta|1\rangle$ is written in a vector notation as

$$\begin{bmatrix} \alpha \\ \beta \end{bmatrix}, \tag{1.11}$$

with the top entry corresponding to the amplitude for $|0\rangle$ and the bottom entry the amplitude for $|1\rangle$, then the corresponding output from the quantum not gate is

$$X \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix}. \tag{1.12}$$

Notice that the action of the NOT gate is to take the state $|0\rangle$ and replace it by the state corresponding to the first column of the matrix X. Similarly, the state $|1\rangle$ is replaced by the state corresponding to the second column of the matrix X.

So quantum gates on a single qubit can be described by two by two matrices. Are there any constraints on what matrices may be used as quantum gates? It turns out that there are. Recall that the normalization condition requires $|\alpha|^2+|\beta|^2 = 1$ for a quantum state $\alpha|0\rangle+\beta|1\rangle$. This must also be true of the quantum state $|\psi'\rangle = \alpha'|0\rangle + \beta'|1\rangle$ after the gate has acted. It turns out that the appropriate condition on the matrix representing the gate is that the matrix U describing the single qubit gate be unitary, that is $U^\dagger U = I$, where $U^\dagger$ is the adjoint of U (obtained by transposing and then complex conjugating U), and I is the two by two identity matrix. For example, for the not gate it is easy to verify that $X^\dagger X = I$.

Amazingly, this unitarity constraint is the only constraint on quantum gates. Any unitary matrix specifies a valid quantum gate! The interesting implication is that in contrast to the classical case, where only one non-trivial single bit gate exists - the NOT

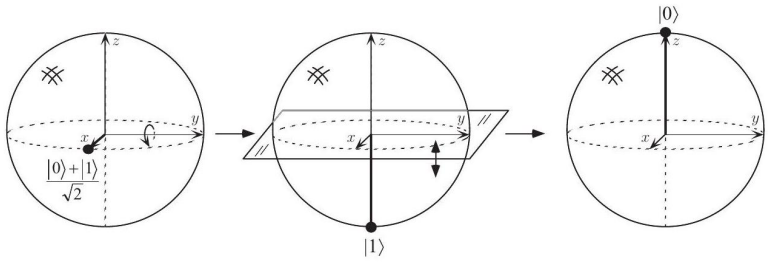


Figure 1.4. Visualization of the Hadamard gate on the Bloch sphere, acting on the input state $(|0\rangle+|1\rangle) / \sqrt{2}$.

gate - there are many non-trivial single qubit gates. Two important ones which we shall use later are the Z gate:

$$Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \tag{1.13}$$

which leaves $|0\rangle$ unchanged, and flips the sign of $|1\rangle$ to give $-|1\rangle$, and the Hadamard gate,

$$H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{1.14}$$

This gate is sometimes described as being like a 'square-root of not' gate, in that it turns a $|0\rangle$ into $(|0\rangle + |1\rangle)/\sqrt{2}$ (first column of H), 'halfway' between $|0\rangle$ and $|1\rangle$, and turns $|1\rangle$ into $(|0\rangle - |1\rangle)/\sqrt{2}$ (second column of H), which is also 'halfway' between $|0\rangle$ and $|1\rangle$. Note, however, that H^2 is not a nOT gate, as simple algebra shows that $H^2 = I$, and thus applying H twice to a state does nothing to it.

The Hadamard gate is one of the most useful quantum gates, and it is worth trying to visualize its operation by considering the Bloch sphere picture. In this picture, it turns out that single qubit gates correspond to rotations and reflections of the sphere. The Hadamard operation is just a rotation of the sphere about the $\hat{y}$ axis by 90°, followed by a rotation about the $\hat{x}$ axis by 180°, as illustrated in Figure 1.4. Some important single qubit gates are shown in Figure 1.5, and contrasted with the classical case.

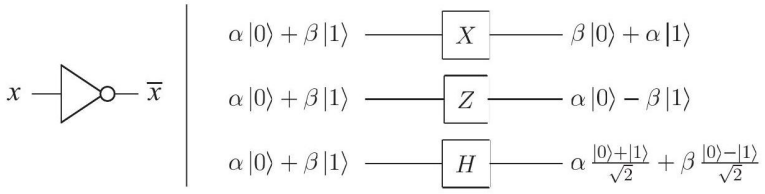


Figure 1.5. Single bit (left) and qubit (right) logic gates.

There are infinitely many two by two unitary matrices, and thus infinitely many single qubit gates. However, it turns out that the properties of the complete set can be understood from the properties of a much smaller set. For example, as explained in Box 1.1, an arbitrary single qubit unitary gate can be decomposed as a product of rotations

$$\begin{bmatrix} \cos\frac{\gamma}{2} & -\sin\frac{\gamma}{2} \\ \sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{bmatrix}, \tag{1.15}$$

and a gate which we'll later understand as being a rotation about the $\hat{z}$ axis,

$$\begin{bmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{bmatrix} \tag{1.16}$$

together with a (global) phase shift-a constant multiplier of the form $e^{i\alpha}$. These gates can be broken down further - we don't need to be able to do these gates for arbitrary α, β and γ, but can build arbitrarily good approximations to such gates using only certain special fixed values of α, β and γ. In this way it is possible to build up an arbitrary single qubit gate using a finite set of quantum gates. More generally, an arbitrary quantum computation on any number of qubits can be generated by a finite set of gates that is said to be universal for quantum computation. To obtain such a universal set we first need to introduce some quantum gates involving multiple qubits.

Box 1.1: Decomposing single qubit operations

In Section 4.2 starting on page 174 we prove that an arbitrary 2×2 unitary matrix may be decomposed as

$$U = e^{i\alpha} \begin{bmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{bmatrix} \begin{bmatrix} \cos\frac{\gamma}{2} & -\sin\frac{\gamma}{2} \\ \sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{bmatrix} \begin{bmatrix} e^{-i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{bmatrix}, \tag{1.17}$$

where α, β, γ, and δ are real-valued. Notice that the second matrix is just an ordinary rotation. It turns out that the first and last matrices can also be understood as rotations in a

different plane. This decomposition can be used to give an exact prescription for performing an arbitrary single qubit quantum logic gate.

7.1.8 1.3.2 Multiple qubit gates

Now let us generalize from one to multiple qubits. Figure 1.6 shows five notable multiple bit classical gates, the AND, OR, XOR (exclusive-OR), NAND and NOR gates. An important theoretical result is that any function on bits can be computed from the composition of NAND gates alone, which is thus known as a universal gate. By contrast, the XOR alone or even together with NOT is not universal. One way of seeing this is to note that applying an XOR gate does not change the total parity of the bits. As a result, any circuit involving only not and XOR gates will, if two inputs x and y have the same parity, give outputs with the same parity, restricting the class of functions which may be computed, and thus precluding universality.

The prototypical multi-qubit quantum logic gate is the controlled-NOT or CNOT gate. This gate has two input qubits, known as the control qubit and the target qubit, respectively. The circuit representation for the CNOT is shown in the top right of Figure 1.6; the top line represents the control qubit, while the bottom line represents the target

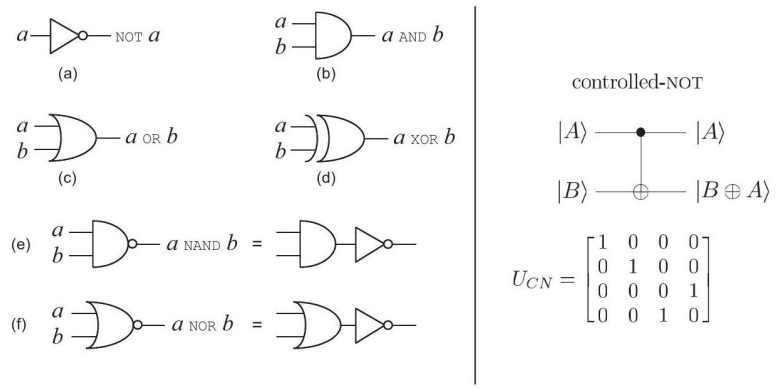


Figure 1.6. On the left are some standard single and multiple bit gates, while on the right is the prototypical multiple qubit gate, the controlled-not. The matrix representation of the controlled-not, U_{CN}, is written with respect to the amplitudes for $|00\rangle, |01\rangle, |10\rangle$, and $|11\rangle$, in that order.

qubit. The action of the gate may be described as follows. If the control qubit is set to 0 , then the target qubit is left alone. If the control qubit is set to 1 , then the target qubit is flipped. In equations:

$$|00\rangle \rightarrow |00\rangle; |01\rangle \rightarrow |01\rangle; |10\rangle \rightarrow |11\rangle; |11\rangle \rightarrow |10\rangle. \tag{1.18}$$

Another way of describing the CNOT is as a generalization of the classical XOR gate, since the action of the gate may be summarized as $|A, B\rangle \rightarrow |A, B \oplus A\rangle$, where $\oplus$ is addition modulo two, which is exactly what the XOR gate does. That is, the control qubit and the target qubit are xored and stored in the target qubit.

Yet another way of describing the action of the CNOT is to give a matrix representation, as shown in the bottom right of Figure 1.6. You can easily verify that the first column of U_{CN} describes the transformation that occurs to $|00\rangle$, and similarly for the other computational basis states, $|01\rangle, |10\rangle$, and $|11\rangle$. As for the single qubit case, the requirement that probability be conserved is expressed in the fact that U_{CN} is a unitary matrix, that is, $U_{CN}^{\dagger} U_{CN} = I$.

We noticed that the CNOT can be regarded as a type of generalized-XOR gate. Can other classical gates such as the NAND or the regular XOR gate be understood as unitary gates in a sense similar to the way the quantum NOT gate represents the classical NOT gate? It turns out that this is not possible. The reason is because the XOR and NAND gates are essentially irreversible or non-invertible. For example, given the output $A \oplus B$ from an XOR gate, it is not possible to determine what the inputs A and B were; there is an irretrievable loss of information associated with the irreversible action of the XOR gate. On the other hand, unitary quantum gates are always invertible, since the inverse of a unitary matrix is also a unitary matrix, and thus a quantum gate can always be inverted by another quantum gate. Understanding how to do classical logic in this reversible or invertible sense will be a crucial step in understanding how to harness the power of
quantum mechanics for computation. We'll explain the basic idea of how to do reversible computation in Section 1.4.1.

Of course, there are many interesting quantum gates other than the controlled-not. However, in a sense the controlled-NOT and single qubit gates are the prototypes for all other gates because of the following remarkable universality result: Any multiple qubit logic gate may be composed from CNOT and single qubit gates. The proof is given in Section 4.5, and is the quantum parallel of the universality of the NAND gate.

7.1.9 1.3.3 Measurements in bases other than the computational basis

We've described quantum measurements of a single qubit in the state $\alpha|0\rangle + \beta|1\rangle$ as yielding the result 0 or 1 and leaving the qubit in the corresponding state $|0\rangle$ or $|1\rangle$, with respective probabilities $|\alpha|^2$ and $|\beta|^2$. In fact, quantum mechanics allows somewhat more versatility in the class of measurements that may be performed, although certainly nowhere near enough to recover α and β from a single measurement!

Note that the states $|0\rangle$ and $|1\rangle$ represent just one of many possible choices of basis states for a qubit. Another possible choice is the set $|+\rangle \equiv (|0\rangle + |1\rangle)/\sqrt{2}$ and $|-\rangle \equiv (|0\rangle - |1\rangle)/\sqrt{2}$. An arbitrary state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ can be re-expressed in terms of the states $|+\rangle$ and $|-\rangle$:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \alpha\frac{|+\rangle + |-\rangle}{\sqrt{2}} + \beta\frac{|+\rangle - |-\rangle}{\sqrt{2}} = \frac{\alpha+\beta}{\sqrt{2}}|+\rangle + \frac{\alpha-\beta}{\sqrt{2}}|-\rangle. \tag{1.19}$$

It turns out that it is possible to treat the $|+\rangle$ and $|-\rangle$ states as though they were the computational basis states, and measure with respect to this new basis. Naturally, measuring with respect to the $|+\rangle, |-\rangle$ basis results in the result ' + ' with probability $|\alpha+\beta|^2/2$ and the result '-' with probability $|\alpha-\beta|^2/2$, with corresponding post-measurement states $|+\rangle$ and $|-\rangle$, respectively.

More generally, given any basis states $|a\rangle$ and $|b\rangle$ for a qubit, it is possible to express an arbitrary state as a linear combination $\alpha|a\rangle + \beta|b\rangle$ of those states. Furthermore, provided the states are orthonormal, it is possible to perform a measurement with respect to the $|a\rangle, |b\rangle$ basis, giving the result a with probability $|\alpha|^2$ and b with probability $|\beta|^2$. The orthonormality constraint is necessary in order that $|\alpha|^2 + |\beta|^2 = 1$ as we expect for probabilities. In an analogous way it is possible in principle to measure a quantum system of many qubits with respect to an arbitrary orthonormal basis. However, just because it is possible in principle does not mean that such a measurement can be done easily, and we return later to the question of how efficiently a measurement in an arbitrary basis can be performed.

There are many reasons for using this extended formalism for quantum measurements, but ultimately the best one is this: the formalism allows us to describe observed experimental results, as we will see in our discussion of the Stern-Gerlach experiment in Section 1.5.1. An

even more sophisticated and convenient (but essentially equivalent) formalism for describing quantum measurements is described in the next chapter, in Section 2.2.3.

7.1.10 1.3.4 Quantum circuits

We've already met a few simple quantum circuits. Let's look in a little more detail at the elements of a quantum circuit. A simple quantum circuit containing three quantum gates is shown in Figure 1.7. The circuit is to be read from left-to-right. Each line
in the circuit represents a wire in the quantum circuit. This wire does not necessarily correspond to a physical wire; it may correspond instead to the passage of time, or perhaps to a physical particle such as a photon - a particle of light - moving from one location to another through space. It is conventional to assume that the state input to the circuit is a computational basis state, usually the state consisting of all $|0\rangle$s. This rule is broken frequently in the literature on quantum computation and quantum information, but it is considered polite to inform the reader when this is the case.

The circuit in Figure 1.7 accomplishes a simple but useful task - it swaps the states of the two qubits. To see that this circuit accomplishes the swap operation, note that the sequence of gates has the following sequence of effects on a computational basis state $|a, b\rangle$,

$$\begin{aligned} |a, b\rangle &\longrightarrow |a, a \oplus b\rangle \\ &\longrightarrow |a \oplus (a \oplus b), a \oplus b\rangle = |b, a \oplus b\rangle \\ &\longrightarrow |b, (a \oplus b) \oplus b\rangle = |b, a\rangle, \end{aligned} \tag{1.20}$$

where all additions are done modulo 2 . The effect of the circuit, therefore, is to interchange the state of the two qubits.

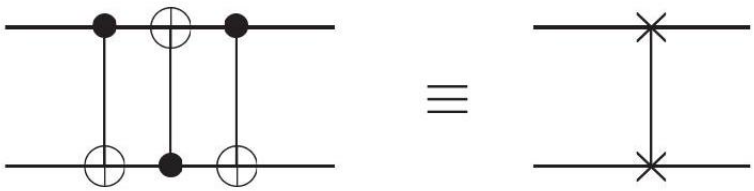


Figure 1.7. Circuit swapping two qubits, and an equivalent schematic symbol notation for this common and useful circuit.

There are a few features allowed in classical circuits that are not usually present in quantum circuits. First of all, we don't allow 'loops', that is, feedback from one part of the quantum circuit to another; we say the circuit is acyclic. Second, classical circuits allow wires to be 'joined' together, an operation known as FANIN, with the resulting single wire containing the bitwise OR of the inputs. Obviously this operation is not reversible and therefore not unitary, so we don't allow FANIN in our quantum circuits. Third, the inverse operation, FANOUT, whereby several copies of a bit are produced is also not allowed in quantum circuits. In fact, it turns out that quantum mechanics forbids the copying of a qubit, making the fanout operation impossible! We'll see an example of this in the next section when we attempt to design a circuit to copy a qubit.

As we proceed we'll introduce new quantum gates as needed. It's convenient to introduce another convention about quantum circuits at this point. This convention is illustrated in Figure 1.8. Suppose U is any unitary matrix acting on some number n of qubits, so U can be

regarded as a quantum gate on those qubits. Then we can define a controlled- U gate which is a natural extension of the controlled-not gate. Such a gate has a single control qubit, indicated by the line with the black dot, and n target qubits, indicated by the boxed U. If the control qubit is set to 0 then nothing happens to the target qubits. If the control qubit is set to 1 then the gate U is applied to the target qubits. The prototypical example of the controlled- U gate is the controlled-NOT gate, which is a controlled- U gate with $U = X$, as illustrated in Figure 1.9.

Another important operation is measurement, which we represent by a 'meter' symbol,

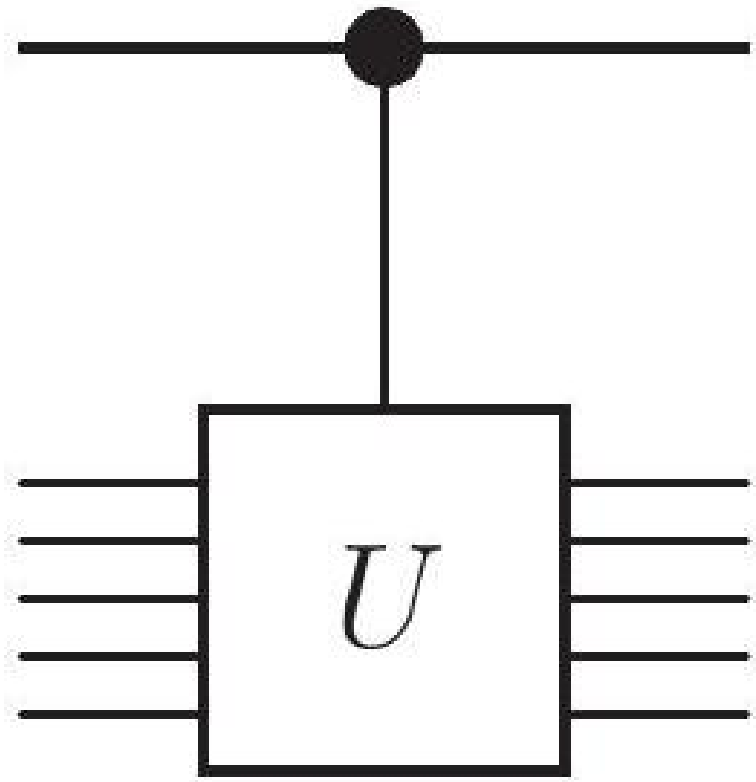


Figure 1.8. Controlled- U gate.

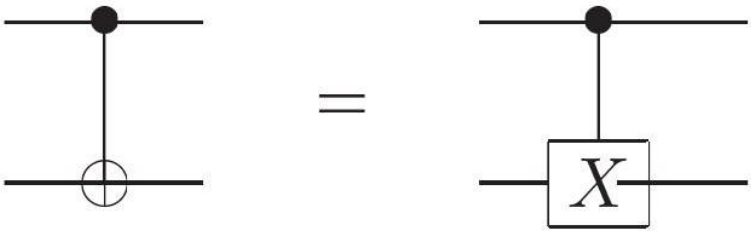


Figure 1.9. Two different representations for the controlled-not.

as shown in Figure 1.10. As previously described, this operation converts a single qubit state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ into a probabilistic classical bit M (distinguished from a qubit by drawing it as a double-line wire), which is 0 with probability $|\alpha|^2$, or 1 with probability $|\beta|^2$.

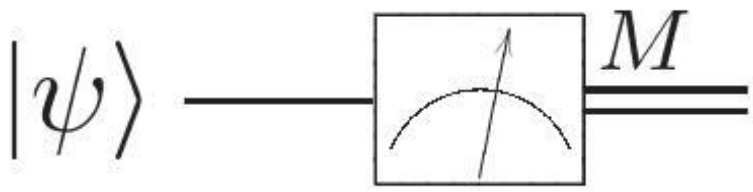


Figure 1.10. Quantum circuit symbol for measurement.

We shall find quantum circuits useful as models of all quantum processes, including but not limited to computation, communication, and even quantum noise. Several simple examples illustrate this below.

7.1.11 1.3.5 Qubit copying circuit?

The CNOT gate is useful for demonstrating one particularly fundamental property of quantum information. Consider the task of copying a classical bit. This may be done using a classical CNOT gate, which takes in the bit to copy (in some unknown state x) and a 'scratchpad' bit initialized to zero, as illustrated in Figure 1.11. The output is two bits, both of which are in the same state x.

Suppose we try to copy a qubit in the unknown state $|\psi\rangle = a|0\rangle + b|1\rangle$ in the same manner by using a CNOT gate. The input state of the two qubits may be written as

$$[a|0\rangle + b|1\rangle]|0\rangle = a|00\rangle + b|10\rangle, \tag{1.21}$$

The function of CNOT is to negate the second qubit when the first qubit is 1 , and thus the output is simply $a|00\rangle + b|11\rangle$. Have we successfully copied $|\psi\rangle$? That is, have we created the state $|\psi\rangle|\psi\rangle$? In the case where $|\psi\rangle = |0\rangle$ or $|\psi\rangle = |1\rangle$ that is indeed what this circuit does; it is possible to use quantum circuits to copy classical information encoded as a $|0\rangle$ or a $|1\rangle$. However, for a general state $|\psi\rangle$ we see that

$$|\psi\rangle|\psi\rangle = a^2|00\rangle + ab|01\rangle + ab|10\rangle + b^2|11\rangle. \tag{1.22}$$

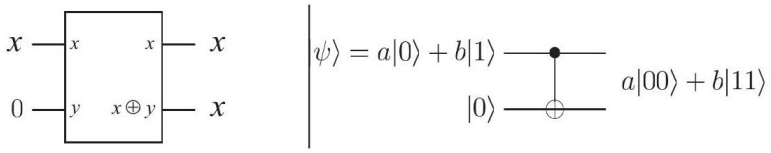


Figure 1.11. Classical and quantum circuits to 'copy' an unknown bit or qubit.

Comparing with $a|00\rangle + b|11\rangle$, we see that unless $ab = 0$ the 'copying circuit' above does not copy the quantum state input. In fact, it turns out to be impossible to make a copy of an unknown quantum state. This property, that qubits cannot be copied, is known as the no-cloning theorem, and it is one of the chief differences between quantum and classical information. The no-cloning theorem is discussed at more length in Box 12.1 on page 532; the proof is very simple, and we encourage you to skip ahead and read the proof now.

There is another way of looking at the failure of the circuit in Figure 1.11, based on the intuition that a qubit somehow contains 'hidden' information not directly accessible to measurement. Consider what happens when we measure one of the qubits of the state $a|00\rangle + b|11\rangle$. As previously described, we obtain either 0 or 1 with probabilities $|a|^2$ and $|b|^2$. However, once

one qubit is measured, the state of the other one is completely determined, and no additional information can be gained about a and b. In this sense, the extra hidden information carried in the original qubit $|\psi\rangle$ was lost in the first measurement, and cannot be regained. If, however, the qubit had been copied, then the state of the other qubit should still contain some of that hidden information. Therefore, a copy cannot have been created.

7.1.12 1.3.6 Example: Bell states

Let's consider a slightly more complicated circuit, shown in Figure 1.12, which has a Hadamard gate followed by a CNOT, and transforms the four computational basis states according to the table given. As an explicit example, the Hadamard gate takes the input $|00\rangle$ to $(|0\rangle + |1\rangle)|0\rangle/\sqrt{2}$, and then the CNOT gives the output state $(|00\rangle + |11\rangle)/\sqrt{2}$. Note how this works: first, the Hadamard transform puts the top qubit in a superposition; this then acts as a control input to the CNOT, and the target gets inverted only when the control is 1 . The output states

$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}; \tag{1.23}$$

$$|\beta_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}; \tag{1.24}$$

$$|\beta_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}; \text{ and} \tag{1.25}$$

$$|\beta_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}; \tag{1.26}$$

are known as the Bell states, or sometimes the EPR states or EPR pairs, after some of the people - Bell, and Einstein, Podolsky, and Rosen - who first pointed out the strange properties of states like these. The mnemonic notation $|\beta_{00}\rangle, |\beta_{01}\rangle, |\beta_{10}\rangle, |\beta_{11}\rangle$ may be understood via the equations

$$|\beta_{xy}\rangle \equiv \frac{|0, y\rangle + (-1)^x |1, \bar{y}\rangle}{\sqrt{2}} \tag{1.27}$$

where $\bar{y}$ is the negation of y.

In	Out		
$\|00\rangle$	$(\|00\rangle + \|11\rangle)/\sqrt{2} \equiv \|\beta_{00}\rangle$	$x -$ $H-$	$\|\beta_{xy}\rangle$
$\|01\rangle$	$(\|01\rangle + \|10\rangle)/\sqrt{2} \equiv \|\beta_{01}\rangle$		
$\|10\rangle$	$(\|00\rangle - \|11\rangle)/\sqrt{2} \equiv \|\beta_{10}\rangle$	$y-$	
$\|11\rangle$	$(\|01\rangle - \|10\rangle)/\sqrt{2} \equiv \|\beta_{11}\rangle$		

Figure 1.12. Quantum circuit to create Bell states, and its input-ouput quantum 'truth table'.

7.1.13 1.3.7 Example: quantum teleportation

We will now apply the techniques of the last few pages to understand something nontrivial, surprising, and a lot of fun - quantum teleportation! Quantum teleportation is a technique for moving quantum states around, even in the absence of a quantum communications channel linking the sender of the quantum state to the recipient.

Here's how quantum teleportation works. Alice and Bob met long ago but now live far apart. While together they generated an EPR pair, each taking one qubit of the EPR pair when they separated. Many years later, Bob is in hiding, and Alice's mission, should she choose to accept it, is to deliver a qubit $|\psi\rangle$ to Bob. She does not know the state of the qubit, and moreover can only send classical information to Bob. Should Alice accept the mission?

Intuitively, things look pretty bad for Alice. She doesn't know the state $|\psi\rangle$ of the qubit she has to send to Bob, and the laws of quantum mechanics prevent her from determining the state when she only has a single copy of $|\psi\rangle$ in her possession. What's worse, even if she did know the state $|\psi\rangle$, describing it precisely takes an infinite amount of classical information since $|\psi\rangle$ takes values in a continuous space. So even if she did know $|\psi\rangle$, it would take forever for Alice to describe the state to Bob. It's not looking good for Alice. Fortunately for Alice, quantum teleportation is a way of utilizing the entangled EPR pair in order to send $|\psi\rangle$ to Bob, with only a small overhead of classical communication.

In outline, the steps of the solution are as follows: Alice interacts the qubit $|\psi\rangle$ with her half of the EPR pair, and then measures the two qubits in her possession, obtaining one of four possible classical results, $00, 01, 10$, and 11 . She sends this information to Bob. Depending on Alice's classical message, Bob performs one of four operations on his half of the EPR pair. Amazingly, by doing this he can recover the original state $|\psi\rangle$!

The quantum circuit shown in Figure 1.13 gives a more precise description of quantum teleportation. The state to be teleported is $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where α and β are unknown amplitudes. The state input into the circuit $|\psi_0\rangle$ is

$$|\psi_0\rangle = |\psi\rangle\,|\beta_{00}\rangle \tag{1.28}$$

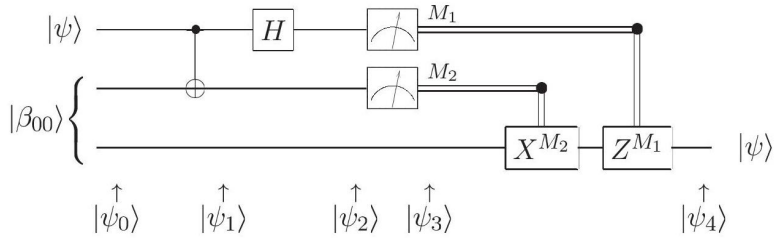


Figure 1.13. Quantum circuit for teleporting a qubit. The two top lines represent Alice's system, while the bottom line is Bob's system. The meters represent measurement, and the double lines coming out of them carry classical bits (recall that single lines denote qubits).

$$= \frac{1}{\sqrt{2}}[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)], \tag{1.29}$$

where we use the convention that the first two qubits (on the left) belong to Alice, and the third qubit to Bob. As we explained previously, Alice's second qubit and Bob's qubit start out in an EPR state. Alice sends her qubits through a CNOT gate, obtaining

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle)]. \tag{1.30}$$

She then sends the first qubit through a Hadamard gate, obtaining

$$|\psi_2\rangle = \frac{1}{2}[\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)]. \tag{1.31}$$

This state may be re-written in the following way, simply by regrouping terms:

$$|\psi_2\rangle = \frac{1}{2}[|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)]. \quad (1.32)$$

This expression naturally breaks down into four terms. The first term has Alice's qubits in the state $|00\rangle$, and Bob's qubit in the state $\alpha|0\rangle + \beta|1\rangle -$ which is the original state $|\psi\rangle$. If Alice performs a measurement and obtains the result 00 then Bob's system will be in the state $|\psi\rangle$. Similarly, from the previous expression we can read off Bob's postmeasurement state, given the result of Alice's measurement:

$$00 \longmapsto |\psi_3(00)\rangle \equiv [\alpha|0\rangle + \beta|1\rangle] \quad (1.33)$$
$$01 \longmapsto |\psi_3(01)\rangle \equiv [\alpha|1\rangle + \beta|0\rangle] \quad (1.34)$$
$$10 \longmapsto |\psi_3(10)\rangle \equiv [\alpha|0\rangle - \beta|1\rangle] \quad (1.35)$$
$$11 \longmapsto |\psi_3(11)\rangle \equiv [\alpha|1\rangle - \beta|0\rangle]. \quad (1.36)$$

Depending on Alice's measurement outcome, Bob's qubit will end up in one of these four possible states. Of course, to know which state it is in, Bob must be told the result of Alice's measurement - we will show later that it is this fact which prevents teleportation
from being used to transmit information faster than light. Once Bob has learned the measurement outcome, Bob can 'fix up' his state, recovering $|\psi\rangle$, by applying the appropriate quantum gate. For example, in the case where the measurement yields 00 , Bob doesn't need to do anything. If the measurement is 01 then Bob can fix up his state by applying the X gate. If the measurement is 10 then Bob can fix up his state by applying the Z gate. If the measurement is 11 then Bob can fix up his state by applying first an X and then a Z gate. Summing up, Bob needs to apply the transformation $Z^{M_1}X^{M_2}$ (note how time goes from left to right in circuit diagrams, but in matrix products terms on the right happen first) to his qubit, and he will recover the state $|\psi\rangle$.

There are many interesting features of teleportation, some of which we shall return to later in the book. For now we content ourselves with commenting on a couple of aspects. First, doesn't teleportation allow one to transmit quantum states faster than light? This would be rather peculiar, because the theory of relativity implies that faster than light information transfer could be used to send information backwards in time. Fortunately, quantum teleportation does not enable faster than light communication, because to complete the teleportation Alice must transmit her measurement result to Bob over a classical communications channel. We will show in Section 2.4.3 that without this classical communication, teleportation does not convey any information at all. The classical channel is limited by the speed of light, so it follows that quantum teleportation cannot be accomplished faster than the speed of light, resolving the apparent paradox.

A second puzzle about teleportation is that it appears to create a copy of the quantum state being teleported, in apparent violation of the no-cloning theorem discussed in Section 1.3.5. This violation is only illusory since after the teleportation process only the target qubit is left in the state $|\psi\rangle$, and the original data qubit ends up in one of the computational basis states $|0\rangle$ or $|1\rangle$, depending upon the measurement result on the first qubit.

What can we learn from quantum teleportation? Quite a lot! It's much more than just a neat trick one can do with quantum states. Quantum teleportation emphasizes the interchangeability of different resources in quantum mechanics, showing that one shared EPR pair together with two classical bits of communication is a resource at least the equal of one qubit of communication. Quantum computation and quantum information has revealed a plethora of methods

for interchanging resources, many built upon quantum teleportation. In particular, in Chapter 10 we explain how teleportation can be used to build quantum gates which are resistant to the effects of noise, and in Chapter 12 we show that teleportation is intimately connected with the properties of quantum error-correcting codes. Despite these connections with other subjects, it is fair to say that we are only beginning to understand why it is that quantum teleportation is possible in quantum mechanics; in later chapters we endeavor to explain some of the insights that make such an understanding possible.

7.1.14 1.4 Quantum algorithms

What class of computations can be performed using quantum circuits? How does that class compare with the computations which can be performed using classical logical circuits? Can we find a task which a quantum computer may perform better than a classical computer? In this section we investigate these questions, explaining how to perform classical computations on quantum computers, giving some examples of problems for
which quantum computers offer an advantage over classical computers, and summarizing the known quantum algorithms.

7.1.15 1.4.1 Classical computations on a quantum computer

Can we simulate a classical logic circuit using a quantum circuit? Not surprisingly, the answer to this question turns out to be yes. It would be very surprising if this were not the case, as physicists believe that all aspects of the world around us, including classical logic circuits, can ultimately be explained using quantum mechanics. As pointed out earlier, the reason quantum circuits cannot be used to directly simulate classical circuits is because unitary quantum logic gates are inherently reversible, whereas many classical logic gates such as the NAND gate are inherently irreversible.

Any classical circuit can be replaced by an equivalent circuit containing only reversible elements, by making use of a reversible gate known as the Toffoli gate. The Toffoli gate has three input bits and three output bits, as illustrated in Figure 1.14. Two of the bits are control bits that are unaffected by the action of the Toffoli gate. The third bit is a target bit that is flipped if both control bits are set to 1 , and otherwise is left alone. Note that applying the Toffoli gate twice to a set of bits has the effect $(a, b, c) \rightarrow (a, b, c \oplus ab) \rightarrow (\ a, b, c\ )$, and thus the Toffoli gate is a reversible gate, since it has an inverse - itself.

Inputs			Outputs		
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

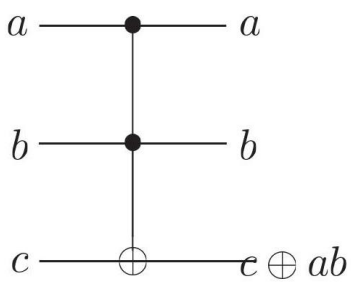


Figure 1.14. Truth table for the Toffoli gate, and its circuit representation.

The Toffoli gate can be used to simulate NAND gates, as shown in Figure 1.15, and can also be used to do fanout, as shown in Figure 1.16. With these two operations it becomes possible

to simulate all other elements in a classical circuit, and thus an arbitrary classical circuit can be simulated by an equivalent reversible circuit.

The Toffoli gate has been described as a classical gate, but it can also be implemented as a quantum logic gate. By definition, the quantum logic implementation of the Toffoli gate simply permutes computational basis states in the same way as the classical Toffoli gate. For example, the quantum Toffoli gate acting on the state $|110\rangle$ flips the third qubit because the first two are set, resulting in the state $|111\rangle$. It is tedious but not difficult to write this transformation out as an 8 by 8 matrix, U, and verify explicitly that U is a unitary matrix, and thus the Toffoli gate is a legitimate quantum gate. The quantum Toffoli gate can be used to simulate irreversible classical logic gates, just as the classical

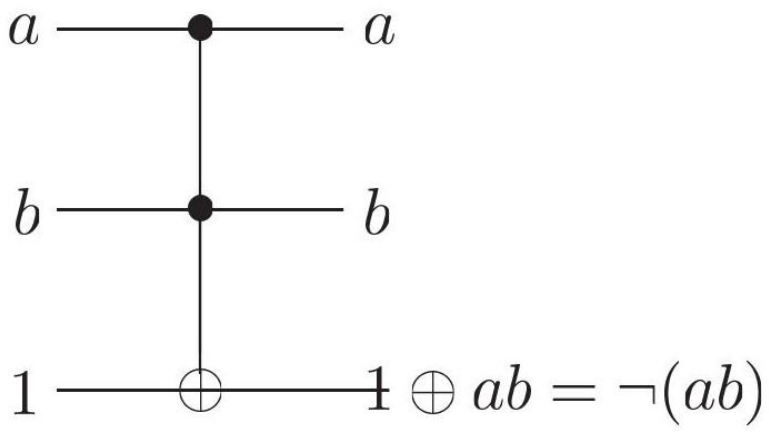


Figure 1.15. Classical circuit implementing a NAND gate using a Toffoli gate. The top two bits represent the input to the NAND, while the third bit is prepared in the standard state 1 , sometimes known as an ancilla state. The output from the NAND is on the third bit.

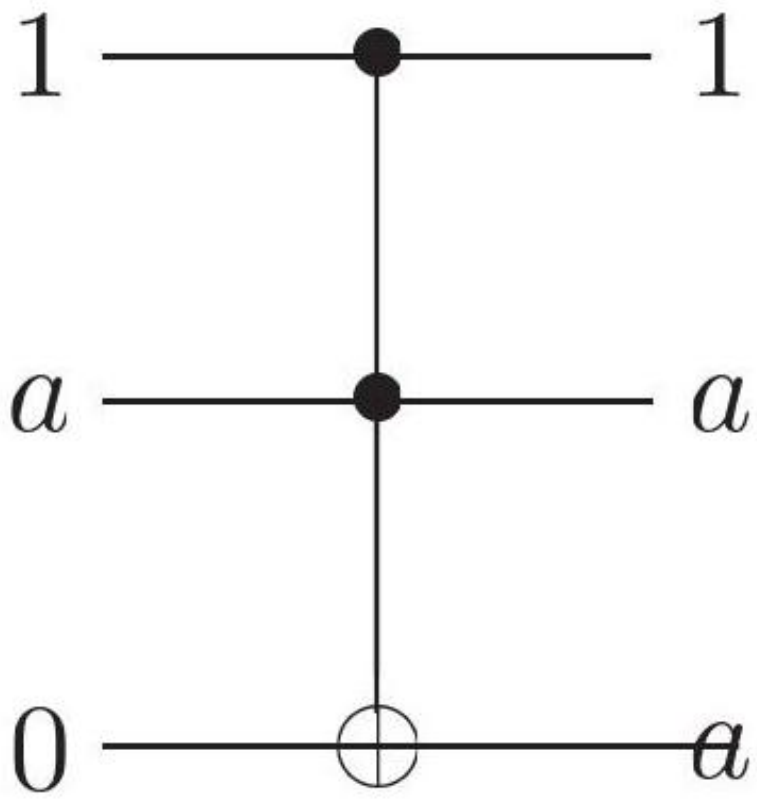


Figure 1.16. fanout with the Toffoli gate, with the second bit being the input to the fanout (and the other two bits standard ancilla states), and the output from fanout appearing on the second and third bits.

Toffoli gate was, and ensures that quantum computers are capable of performing any computation which a classical (deterministic) computer may do.

What if the classical computer is non-deterministic, that is, has the ability to generate random bits to be used in the computation? Not surprisingly, it is easy for a quantum computer to simulate this. To perform such a simulation it turns out to be sufficient to produce random fair coin tosses, which can be done by preparing a qubit in the state $|0\rangle$, sending it through a Hadamard gate to produce $(|0\rangle + |1\rangle)/\sqrt{2}$, and then measuring the state. The result will be $|0\rangle$ or $|1\rangle$ with 50/50 probability. This provides a quantum computer with the ability to efficiently simulate a non-deterministic classical computer.

Of course, if the ability to simulate classical computers were the only feature of quantum computers there would be little point in going to all the trouble of exploiting quantum effects! The advantage of quantum computing is that much more powerful functions may be computed using qubits and quantum gates. In the next few sections we explain how to do this, culminating in the Deutsch-Jozsa algorithm, our first example of a quantum algorithm able to solve a problem faster than any classical algorithm.

7.1.16 1.4.2 Quantum parallelism

Quantum parallelism is a fundamental feature of many quantum algorithms. Heuristically, and at the risk of over-simplifying, quantum parallelism allows quantum computers to evaluate a function $f(x)$ for many different values of x simultaneously. In this section we explain how quantum parallelism works, and some of its limitations.

Suppose $f(x) : \{0,1\} \rightarrow \{0,1\}$ is a function with a one-bit domain and range. A convenient way of computing this function on a quantum computer is to consider a two qubit

quantum computer which starts in the state $|x, y\rangle$. With an appropriate sequence of logic gates it is possible to transform this state into $|x, y \oplus f(x)\rangle$, where $\oplus$ indicates addition modulo 2; the first register is called the 'data' register, and the second register the 'target' register. We give the transformation defined by the map $|x, y\rangle \to |x, y \oplus f(x)\rangle$ a name, U_f, and note that it is easily shown to be unitary. If $y = 0$, then the final state of the second qubit is just the value $f(x)$. (In Section 3.2.5 we show that given a classical circuit for computing f there is a quantum circuit of comparable efficiency which computes the transformation U_f on a quantum computer. For our purposes it can be considered to be a black box.)

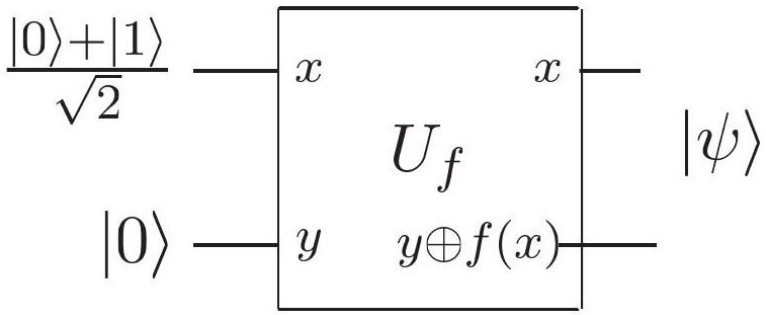


Figure 1.17. Quantum circuit for evaluating $f(0)$ and $f(1)$ simultaneously. $U_{f $ is the quantum circuit which takes inputs like $|x, y\rangle$ to $|x, y \oplus f(x)\rangle$.}

Consider the circuit shown in Figure 1.17, which applies U_f to an input not in the computational basis. Instead, the data register is prepared in the superposition $(|0\rangle + |1\rangle)/\sqrt{2}$, which can be created with a Hadamard gate acting on $|0\rangle$. Then we apply U_f, resulting in the state:

$$\frac{|0, f(0)\rangle + |1, f(1)\rangle}{\sqrt{2}}. \tag{1.37}$$

This is a remarkable state! The different terms contain information about both $f(0)$ and $f(1)$; it is almost as if we have evaluated $f(x)$ for two values of x simultaneously, a feature known as 'quantum parallelism'. Unlike classical parallelism, where multiple circuits each built to compute $f(x)$ are executed simultaneously, here a single $f(x)$ circuit is employed to evaluate the function for multiple values of x simultaneously, by exploiting the ability of a quantum computer to be in superpositions of different states.

This procedure can easily be generalized to functions on an arbitrary number of bits, by using a general operation known as the Hadamard transform, or sometimes the WalshHadamard transform. This operation is just n Hadamard gates acting in parallel on n qubits. For example, shown in Figure 1.18 is the case $n = 2$ with qubits initially prepared as $|0\rangle$, which gives

$$\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) = \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2} \tag{1.38}$$

as output. We write $H^{\otimes 2}$ to denote the parallel action of two Hadamard gates, and read ' $\otimes$ ' as 'tensor'. More generally, the result of performing the Hadamard transform on n qubits initially in the all $|0\rangle$ state is

$$\frac{1}{\sqrt{2^n}} \sum_x |x\rangle, \tag{1.39}$$

where the sum is over all possible values of x, and we write $H^{\otimes n}$ to denote this action. That is, the Hadamard transform produces an equal superposition of all computational basis states.

Moreover, it does this extremely efficiently, producing a superposition of 2^n states using just n gates.

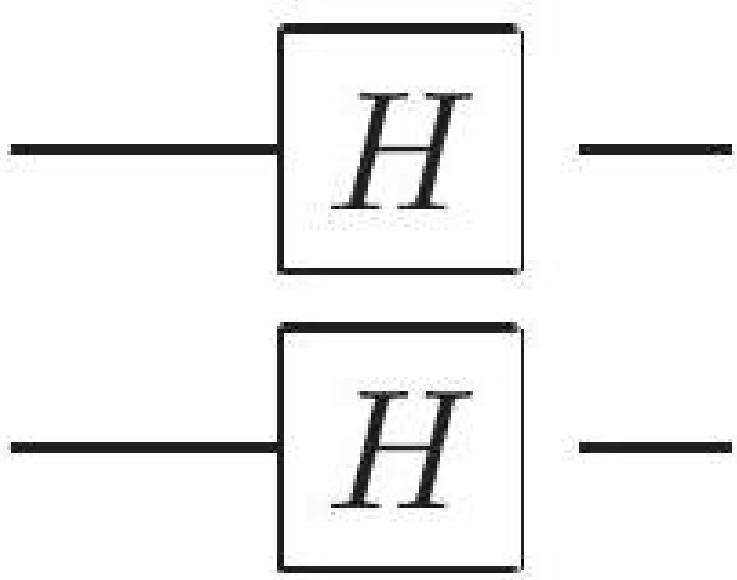


Figure 1.18. The Hadamard transform $H^{\otimes 2
$ on two qubits.}

Quantum parallel evaluation of a function with an n bit input x and 1 bit output, $f(x)$, can thus be performed in the following manner. Prepare the $n+1$ qubit state $|0\rangle^{\otimes n}|0\rangle$, then apply the Hadamard transform to the first n qubits, followed by the quantum circuit implementing U_f. This produces the state

$$\frac{1}{\sqrt{2^n}} \sum_x |x\rangle|f(x)\rangle. \tag{1.40}$$

In some sense, quantum parallelism enables all possible values of the function f to be evaluated simultaneously, even though we apparently only evaluated f once. However, this parallelism is not immediately useful. In our single qubit example, measurement of the state gives only either $|0, f(0)\rangle$ or $|1, f(1)\rangle$! Similarly, in the general case, measurement of the state $\sum_x |x, f(x)\rangle$ would give only $f(x)$ for a single value of x. Of course, a classical computer can do this easily! Quantum computation requires something more than just quantum parallelism to be useful; it requires the ability to extract information about more than one value of $f(x)$ from superposition states like $\sum_x |x, f(x)\rangle$. Over the next two sections we investigate examples of how this may be done.

7.1.17 1.4.3 Deutsch's algorithm

A simple modification of the circuit in Figure 1.17 demonstrates how quantum circuits can outperform classical ones by implementing Deutsch's algorithm (we actually present a simplified and improved version of the original algorithm; see 'History and further reading' at the end of the chapter). Deutsch's algorithm combines quantum parallelism with a property of quantum mechanics known as interference. As before, let us use the Hadamard gate to prepare the first qubit as the superposition $(|0\rangle + |1\rangle)/\sqrt{2}$, but now let us prepare the second qubit y as the superposition $(|0\rangle - |1\rangle)/\sqrt{2}$, using a Hadamard gate applied to the state $|1\rangle$. Let us follow the states along to see what happens in this circuit, shown in Figure 1.19.

The input state

$$|\psi_0\rangle = |01\rangle \tag{1.41}$$

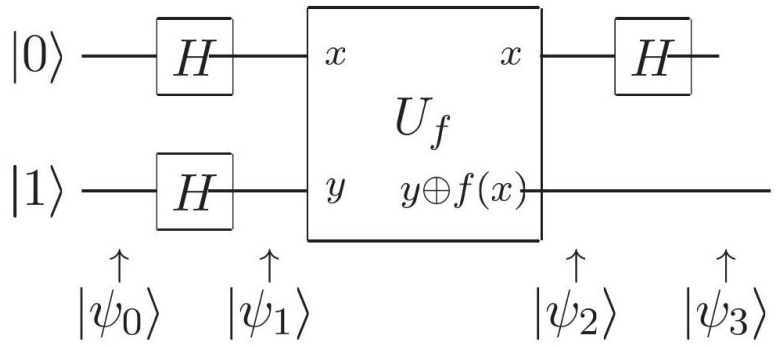


Figure 1.19. Quantum circuit implementing Deutsch's algorithm.

is sent through two Hadamard gates to give

$$|\psi_1\rangle = \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]. \tag{1.42}$$

A little thought shows that if we apply U_f to the state $|x\rangle(|0\rangle - |1\rangle)/\sqrt{2}$ then we obtain the state $(-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle)/\sqrt{2}$. Applying U_f to $|\psi_1\rangle$ therefore leaves us with one of two possibilities:

$$|\psi_2\rangle = \begin{cases} \pm\left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & \text{if } f(0) = f(1) \\ \pm\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & \text{if } f(0) \neq f(1). \end{cases} \tag{1.43}$$

The final Hadamard gate on the first qubit thus gives us

$$|\psi_3\rangle = \begin{cases} \pm|0\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & \text{if } f(0) = f(1) \\ \pm|1\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & \text{if } f(0) \neq f(1). \end{cases} \tag{1.44}$$

Realizing that $f(0) \oplus f(1)$ is 0 if $f(0) = f(1)$ and 1 otherwise, we can rewrite this result concisely as

$$|\psi_3\rangle = \pm|f(0) \oplus f(1)\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right], \tag{1.45}$$

so by measuring the first qubit we may determine $f(0) \oplus f(1)$. This is very interesting indeed: the quantum circuit has given us the ability to determine a global property of $f(x)$, namely $f(0) \oplus f(1)$, using only one evaluation of $f(x)$! This is faster than is possible with a classical apparatus, which would require at least two evaluations.

This example highlights the difference between quantum parallelism and classical randomized algorithms. Naively, one might think that the state $|0\rangle|f(0)\rangle + |1\rangle|f(1)\rangle$ corresponds rather closely to a probabilistic classical computer that evaluates $f(0)$ with probability one-half, or $f(1)$ with probability one-half. The difference is that in a classical computer these two alternatives forever exclude one another; in a quantum computer it is
possible for the two alternatives to interfere with one another to yield some global property of the function f, by using something like the Hadamard gate to recombine the different alternatives, as was done in Deutsch's algorithm. The essence of the design of many quantum

algorithms is that a clever choice of function and final transformation allows efficient determination of useful global information about the function - information which cannot be attained quickly on a classical computer.

7.1.18 1.4.4 The Deutsch-Jozsa algorithm

Deutsch's algorithm is a simple case of a more general quantum algorithm, which we shall refer to as the Deutsch-Jozsa algorithm. The application, known as Deutsch's problem, may be described as the following game. Alice, in Amsterdam, selects a number x from 0 to $2^n - 1$, and mails it in a letter to Bob, in Boston. Bob calculates some function $f(x)$ and replies with the result, which is either 0 or 1 . Now, Bob has promised to use a function f which is of one of two kinds; either $f(x)$ is constant for all values of x, or else $f(x)$ is balanced, that is, equal to 1 for exactly half of all the possible x, and 0 for the other half. Alice's goal is to determine with certainty whether Bob has chosen a constant or a balanced function, corresponding with him as little as possible. How fast can she succeed?

In the classical case, Alice may only send Bob one value of x in each letter. At worst, Alice will need to query Bob at least $2^n/2 + 1$ times, since she may receive $2^n/20$ s before finally getting a 1 , telling her that Bob's function is balanced. The best deterministic classical algorithm she can use therefore requires $2^n/2 + 1$ queries. Note that in each letter, Alice sends Bob n bits of information. Furthermore, in this example, physical distance is being used to artificially elevate the cost of calculating $f(x)$, but this is not needed in the general problem, where $f(x)$ may be inherently difficult to calculate.

If Bob and Alice were able to exchange qubits, instead of just classical bits, and if Bob agreed to calculate $f(x)$ using a unitary transform U_f, then Alice could achieve her goal in just one correspondence with Bob, using the following algorithm.

Analogously to Deutsch's algorithm, Alice has an n qubit register to store her query in, and a single qubit register which she will give to Bob, to store the answer in. She begins by preparing both her query and answer registers in a superposition state. Bob will evaluate $f(x)$ using quantum parallelism and leave the result in the answer register. Alice then interferes states in the superposition using a Hadamard transform on the query register, and finishes by performing a suitable measurement to determine whether f was constant or balanced.

The specific steps of the algorithm are depicted in Figure 1.20. Let us follow the states through this circuit. The input state

$$|\psi_0\rangle = |0\rangle^{\otimes n}|1\rangle \tag{1.46}$$

is similar to that of Equation (1.41), but here the query register describes the state of n qubits all prepared in the $|0\rangle$ state. After the Hadamard transform on the query register and the Hadamard gate on the answer register we have

$$|\psi_1\rangle = \sum_{x\in\{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]. \tag{1.47}$$

The query register is now a superposition of all values, and the answer register is in an

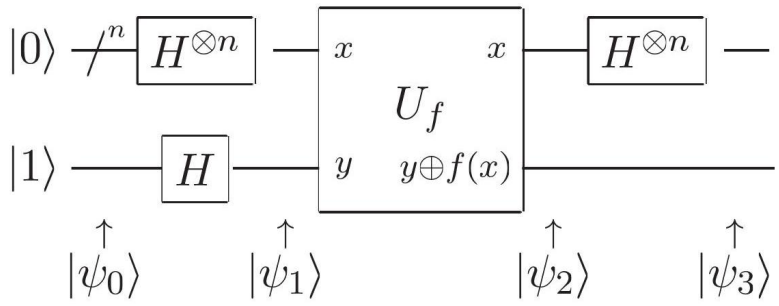


Figure 1.20. Quantum circuit implementing the general Deutsch-Jozsa algorithm. The wire with a '/' through it represents a set of n qubits, similar to the common engineering notation.

evenly weighted superposition of 0 and 1 . Next, the function f is evaluated (by Bob) using $U_f : |x, y\rangle \rightarrow |x, y \oplus f(x)\rangle$, giving

$$|\psi_2\rangle = \sum_x \frac{(-1)^{f(x)}|x\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]. \tag{1.48}$$

Alice now has a set of qubits in which the result of Bob's function evaluation is stored in the amplitude of the qubit superposition state. She now interferes terms in the superposition using a Hadamard transform on the query register. To determine the result of the Hadamard transform it helps to first calculate the effect of the Hadamard transform on a state $|x\rangle$. By checking the cases $x = 0$ and $x = 1$ separately we see that for a single qubit $H|x\rangle = \sum_z (-1)^{xz}|z\rangle/\sqrt{2}$. Thus

$$H^{\otimes n}\,|x_1, \ldots, x_n\rangle = \frac{\sum_{z_1,\ldots,z_n}(-1)^{x_1 z_1 + \cdots + x_n z_n}\,|z_1, \ldots, z_n\rangle}{\sqrt{2^n}}. \tag{1.49}$$

This can be summarized more succinctly in the very useful equation

$$H^{\otimes n}|x\rangle = \frac{\sum_z (-1)^{x\cdot z}|z\rangle}{\sqrt{2^n}}, \tag{1.50}$$

where $x \cdot z$ is the bitwise inner product of x and z, modulo 2 . Using this equation and (1.48) we can now evaluate $|\psi_3\rangle$,

$$|\psi_3\rangle = \sum_z \sum_x \frac{(-1)^{x\cdot z + f(x)}|z\rangle}{2^n} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]. \tag{1.51}$$

Alice now observes the query register. Note that the amplitude for the state $|0\rangle^{\otimes n}$ is $\sum_x (-1)^{f(x)}/2^n$. Let's look at the two possible cases $-f$ constant and f balanced - to discern what happens. In the case where f is constant the amplitude for $|0\rangle^{\otimes n}$ is $+1$ or -1 , depending on the constant value $f(x)$ takes. Because $|\psi_3\rangle$ is of unit length it follows that all the other amplitudes must be zero, and an observation will yield 0 s for all qubits in the query register. If f is balanced then the positive and negative contributions to the amplitude for $|0\rangle^{\otimes n}$ cancel, leaving an amplitude of zero, and a measurement must yield a result other than 0 on at least one qubit in the query register. Summarizing, if Alice
measures all 0 s then the function is constant; otherwise the function is balanced. The Deutsch-Jozsa algorithm is summarized below.

Algorithm: Deutsch-Jozsa

Inputs: (1) A black box U_f which performs the transformation $|x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$, for $x \in \{0, \ldots, 2^n - 1\}$ and $f(x) \in \{0, 1\}$. It is promised that $f(x)$ is either constant for all values

of x, or else $f(x)$ is balanced, that is, equal to 1 for exactly half of all the possible x, and 0 for the other half.

Outputs: 0 if and only if f is constant.
Runtime: One evaluation of U_f. Always succeeds.

Procedure:

1. $|0\rangle^{\otimes n}|1\rangle$
   initialize state
2. $\rightarrow \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$
   create superposition using
   Hadamard gates
3. $\rightarrow \sum_x (-1)^{f(x)}|x\rangle \left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$
   calculate function f using U_f
4. $\rightarrow \sum_z \sum_x \frac{(-1)^{x\cdot z+f(x)}|z\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$
   perform Hadamard transform
5. $\rightarrow z$
   measure to obtain final output z
   We've shown that a quantum computer can solve Deutsch's problem with one evaluation of the function f compared to the classical requirement for $2^n/2 + 1$ evaluations. This appears impressive, but there are several important caveats. First, Deutsch's problem is not an especially important problem; it has no known applications. Second, the comparison between classical and quantum algorithms is in some ways an apples and oranges comparison, as the method for evaluating the function is quite different in the two cases. Third, if Alice is allowed to use a probabilistic classical computer, then by asking Bob to evaluate $f(x)$ for a few randomly chosen x she can very quickly determine with high probability whether f is constant or balanced. This probabilistic scenario is perhaps more realistic than the deterministic scenario we have been considering. Despite these caveats, the Deutsch-Jozsa algorithm contains the seeds for more impressive quantum algorithms, and it is enlightening to attempt to understand the principles behind its operation.

Exercise 1.1: (Probabilistic classical algorithm) Suppose that the problem is not to distinguish between the constant and balanced functions with certainty, but rather, with some probability of error $\epsilon < 1/2$. What is the performance of the best classical algorithm for this problem?

7.1.19 1.4.5 Quantum algorithms summarized

The Deutsch-Jozsa algorithm suggests that quantum computers may be capable of solving some computational problems much more efficiently than classical computers. Unfortunately, the problem it solves is of little practical interest. Are there more interesting
problems whose solution may be obtained more efficiently using quantum algorithms? What are the principles underlying such algorithms? What are the ultimate limits of a quantum computer's computational power?

Broadly speaking, there are three classes of quantum algorithms which provide an advantage over known classical algorithms. First, there is the class of algorithms based upon quantum versions of the Fourier transform, a tool which is also widely used in classical algorithms. The

Deutsch-Jozsa algorithm is an example of this type of algorithm, as are Shor's algorithms for factoring and discrete logarithm. The second class of algorithms is quantum search algorithms. The third class of algorithms is quantum simulation, whereby a quantum computer is used to simulate a quantum system. We now briefly describe each of these classes of algorithms, and then summarize what is known or suspected about the computational power of quantum computers.

Quantum algorithms based upon the Fourier transform

The discrete Fourier transform is usually described as transforming a set $x_0, \ldots, x_{N-1}$ of N complex numbers into a set of complex numbers $y_0, \ldots, y_{N-1}$ defined by

$$y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi ijk/N} x_j \tag{1.52}$$

Of course, this transformation has an enormous number of applications in many branches of science; the Fourier transformed version of a problem is often easier than the original problem, enabling a solution.

The Fourier transform has proved so useful that a beautiful generalized theory of Fourier transforms has been developed which goes beyond the definition (1.52). This general theory involves some technical ideas from the character theory of finite groups, and we will not attempt to describe it here. What is important is that the Hadamard transform used in the Deutsch-Jozsa algorithm is an example of this generalized class of Fourier transforms. Moreover, many of the other important quantum algorithms also involve some type of Fourier transform.

The most important quantum algorithms known, Shor's fast algorithms for factoring and discrete logarithm, are two examples of algorithms based upon the Fourier transform defined in Equation (1.52). The Equation (1.52) does not appear terribly quantum mechanical in the form we have written it. Imagine, however, that we define a linear transformation U on n qubits by its action on computational basis states $|j\rangle$, where $0 \leq j \leq 2^n - 1$,

$$|j\rangle \longrightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi ijk/2^n} |k\rangle. \tag{1.53}$$

It can be checked that this transformation is unitary, and in fact can be realized as a quantum circuit. Moreover, if we write out its action on superpositions,

$$\sum_{j=0}^{2^n-1} x_j |j\rangle \longrightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \left[\sum_{j=0}^{2^n-1} e^{2\pi ijk/2^n} x_j \right] |k\rangle = \sum_{k=0}^{2^n-1} y_k |k\rangle, \tag{1.54}$$

we see that it corresponds to a vector notation for the Fourier transform (1.52) for the case $N = 2^n$.

How quickly can we perform the Fourier transform? Classically, the fast Fourier transform takes roughly $N \log(N) = n2^n$ steps to Fourier transform $N = 2^n$ numbers. On a quantum computer, the Fourier transform can be accomplished using about $\log^2(N) = n^2$ steps, an exponential saving! The quantum circuit to do this is explained in Chapter 5.

This result seems to indicate that quantum computers can be used to very quickly compute the Fourier transform of a vector of 2^n complex numbers, which would be fantastically useful in a wide range of applications. However, that is not exactly the case; the Fourier transform is being performed on the information 'hidden' in the amplitudes of the quantum state. This information is not directly accessible to measurement. The catch, of course, is that if the output state is measured, it will collapse each qubit into the state $|0\rangle$ or $|1\rangle$, preventing us from

learning the transform result y_k directly. This example speaks to the heart of the conundrum of devising a quantum algorithm. On the one hand, we can perform certain calculations on the 2^n amplitudes associated with n qubits far more efficiently than would be possible on a classical computer. But on the other hand, the results of such a calculation are not available to us if we go about it in a straightforward manner. More cleverness is required in order to harness the power of quantum computation.

Fortunately, it does turn out to be possible to utilize the quantum Fourier transform to efficiently solve several problems that are believed to have no efficient solution on a classical computer. These problems include Deutsch's problem, and Shor's algorithms for discrete logarithm and factoring. This line of thought culminated in Kitaev's discovery of a method to solve the Abelian stabilizer problem, and the generalization to the hidden subgroup problem,

> Let f be a function from a finitely generated group G to a finite set X such that f is constant on the cosets of a subgroup K, and distinct on each coset. Given a quantum black box for performing the unitary transform $U|g\rangle|h\rangle = |g\rangle|h \oplus f(g)\rangle$, for $g \in G, h \in X$, and $\oplus$ an appropriately chosen binary operation on X, find a generating set for K.

The Deutsch-Jozsa algorithm, Shor's algorithms, and related 'exponentially fast' quantum algorithms can all be viewed as special cases of this algorithm. The quantum Fourier transform and its applications are described in Chapter 5.

Quantum search algorithms

A completely different class of algorithms is represented by the quantum search algorithm, whose basic principles were discovered by Grover. The quantum search algorithm solves the following problem: Given a search space of size N, and no prior knowledge about the structure of the information in it, we want to find an element of that search space satisfying a known property. How long does it take to find an element satisfying that property? Classically, this problem requires approximately N operations, but the quantum search algorithm allows it to be solved using approximately $\sqrt{N}$ operations.

The quantum search algorithm offers only a quadratic speedup, as opposed to the more impressive exponential speedup offered by algorithms based on the quantum Fourier transform. However, the quantum search algorithm is still of great interest, since searching heuristics have a wider range of application than the problems solved using the quantum Fourier transform, and adaptations of the quantum search algorithm may have utility
for a very wide range of problems. The quantum search algorithm and its applications are described in Chapter 6.

Quantum simulation

Simulating naturally occurring quantum mechanical systems is an obvious candidate for a task at which quantum computers may excel, yet which is believed to be difficult on a classical computer. Classical computers have difficulty simulating general quantum systems for much the same reasons they have difficulty simulating quantum computers the number of complex numbers needed to describe a quantum system generally grows exponentially with the size of the system, rather than linearly, as occurs in classical systems. In general, storing the quantum state of a system with n distinct components takes something like c^n bits of memory on a classical computer, where c is a constant which depends upon details of the system being simulated, and the desired accuracy of the simulation.

By contrast, a quantum computer can perform the simulation using kn qubits, where k is again a constant which depends upon the details of the system being simulated. This allows

quantum computers to efficiently perform simulations of quantum mechanical systems that are believed not to be efficiently simulatable on a classical computer. A significant caveat is that even though a quantum computer can simulate many quantum systems far more efficiently than a classical computer, this does not mean that the fast simulation will allow the desired information about the quantum system to be obtained. When measured, a kn qubit simulation will collapse into a definite state, giving only kn bits of information; the c^n bits of 'hidden information' in the wavefunction is not entirely accessible. Thus, a crucial step in making quantum simulations useful is development of systematic means by which desired answers can be efficiently extracted; how to do this is only partially understood.

Despite this caveat, quantum simulation is likely to be an important application of quantum computers. The simulation of quantum systems is an important problem in many fields, notably quantum chemistry, where the computational constraints imposed by classical computers make it difficult to accurately simulate the behavior of even moderately sized molecules, much less the very large molecules that occur in many important biological systems. Obtaining faster and more accurate simulations of such systems may therefore have the welcome effect of enabling advances in other fields in which quantum phenomena are important.

In the future we may discover a physical phenomenon in Nature which cannot be efficiently simulated on a quantum computer. Far from being bad news, this would be wonderful! At the least, it will stimulate us to extend our models of computation to encompass the new phenomenon, and increase the power of our computational models beyond the existing quantum computing model. It also seems likely that very interesting new physical effects will be associated with any such phenomenon!

Another application for quantum simulation is as a general method to obtain insight into other quantum algorithms; for example, in Section 6.2 we explain how the quantum search algorithm can be viewed as the solution to a problem of quantum simulation. By approaching the problem in this fashion it becomes much easier to understand the origin of the quantum search algorithm.

Finally, quantum simulation also gives rise to an interesting and optimistic 'quantum corollary' to Moore's law. Recall that Moore's law states that the power of classical computers will double once every two years or so, for constant cost. However, suppose we are simulating a quantum system on a classical computer, and want to add a single qubit (or a larger system) to the system being simulated. This doubles or more the memory requirements needed for a classical computer to store a description of the state of the quantum system, with a similar or greater cost in the time needed to simulate the dynamics. The quantum corollary to Moore's law follows from this observation, stating that quantum computers are keeping pace with classical computers provided a single qubit is added to the quantum computer every two years. This corollary should not be taken too seriously, as the exact nature of the gain, if any, of quantum computation over classical is not yet clear. Nevertheless, this heuristic statement helps convey why we should be interested in quantum computers, and hopeful that they will one day be able to outperform the most powerful classical computers, at least for some applications.

The power of quantum computation

How powerful are quantum computers? What gives them their power? Nobody yet knows the answers to these questions, despite the suspicions fostered by examples such as factoring, which strongly suggest that quantum computers are more powerful than classical computers. It is still possible that quantum computers are no more powerful than classical computers, in the sense that any problem which can be efficiently solved on a quantum computer can also be efficiently solved on a classical computer. On the other hand, it may eventually be proved that quantum computers are much more powerful than classical computers. We now take a brief look at what is known about the power of quantum computation.

Computational complexity theory is the subject of classifying the difficulty of various computational problems, both classical and quantum, and to understand the power of quantum computers we will first examine some general ideas from computational complexity. The most basic idea is that of a complexity class. A complexity class can be thought of as a collection of computational problems, all of which share some common feature with respect to the computational resources needed to solve those problems.

Two of the most important complexity classes go by the names **P** and NP. Roughly speaking, **P** is the class of computational problems that can be solved quickly on a classical computer. NP is the class of problems which have solutions which can be quickly checked on a classical computer. To understand the distinction between **P** and **NP**, consider the problem of finding the prime factors of an integer, n. So far as is known there is no fast way of solving this problem on a classical computer, which suggests that the problem is not in **P**. On the other hand, if somebody tells you that some number p is a factor of n, then we can quickly check that this is correct by dividing p into n, so factoring is a problem in NP.

It is clear that **P** is a subset of **NP**, since the ability to solve a problem implies the ability to check potential solutions. What is not so clear is whether or not there are problems in NP that are not in P. Perhaps the most important unsolved problem in theoretical computer science is to determine whether these two classes are different:

$$\mathbf{P} \stackrel{?}{\neq} \mathbf{NP} \tag{1.55}$$

Most researchers believe that NP contains problems that are not in P. In particular, there is an important subclass of the NP problems, the NP-complete problems, that are
of especial importance for two reasons. First, there are thousands of problems, many highly important, that are known to be NP-complete. Second, any given NP-complete problem is in some sense 'at least as hard' as all other problems in NP. More precisely, an algorithm to solve a specific NP-complete problem can be adapted to solve any other problem in NP, with a small overhead. In particular, if $\mathbf{P} \neq \mathbf{NP}$, then it will follow that no NP-complete problem can be efficiently solved on a classical computer.

It is not known whether quantum computers can be used to quickly solve all the problems in NP, despite the fact that they can be used to solve some problems - like factoring - which are believed by many people to be in NP but not in P. (Note that factoring is not known to be NP-complete, otherwise we would already know how to efficiently solve all problems in NP using quantum computers.) It would certainly be very exciting if it were possible to solve all the problems in NP efficiently on a quantum computer. There is a very interesting negative result known in this direction which rules out using a simple variant of quantum parallelism to solve all the problems in NP. Specifically, one approach to the problem of solving problems in NP on a quantum computer is to try to use some form of quantum parallelism to search in parallel through all the possible solutions to the problem. In Section 6.6 we will show that no approach based upon such a search-based methodology can yield an efficient solution to all the problems in NP. While it is disappointing that this approach fails, it does not rule out that some deeper structure exists in the problems in NP that will allow them all to be solved quickly using a quantum computer.

P and NP are just two of a plethora of complexity classes that have been defined. Another important complexity class is PSPACE. Roughly speaking, PSPACE consists of those problems which can be solved using resources which are few in spatial size (that is, the computer is 'small'), but not necessarily in time ('long' computations are fine). PSPACE is believed to be strictly larger than both **P** and NP although, again, this has never been proved. Finally, the complexity class BPP is the class of problems that can be solved using randomized algorithms in polynomial time, if a bounded probability of error (say 1/4) is allowed in the solution to the problem. BPP is widely regarded as being, even more so than **P**, the class of problems which

should be considered efficiently soluble on a classical computer. We have elected to concentrate here on **P** rather than BPP because **P** has been studied in more depth, however many similar ideas and conclusions arise in connection with BPP.

What of quantum complexity classes? We can define BQP to be the class of all computational problems which can be solved efficiently on a quantum computer, where a bounded probability of error is allowed. (Strictly speaking this makes BQP more analogous to the classical complexity class BPP than to **P**, however we will ignore this subtlety for the purposes of the present discussion, and treat it as the analogue of **P**.) Exactly where BQP fits with respect to P, NP and PSPACE is as yet unknown. What is known is that quantum computers can solve all the problems in **P** efficiently, but that there are no problems outside of PSPACE which they can solve efficiently. Therefore, BQP lies somewhere between **P** and PSPACE, as illustrated in Figure 1.21. An important implication is that if it is proved that quantum computers are strictly more powerful than classical computers, then it will follow that **P** is not equal to PSPACE. Proving this latter result has been attempted without success by many computer scientists, suggesting that it may be non-trivial to prove that quantum computers are more powerful than classical computers, despite much evidence in favor of this proposition.

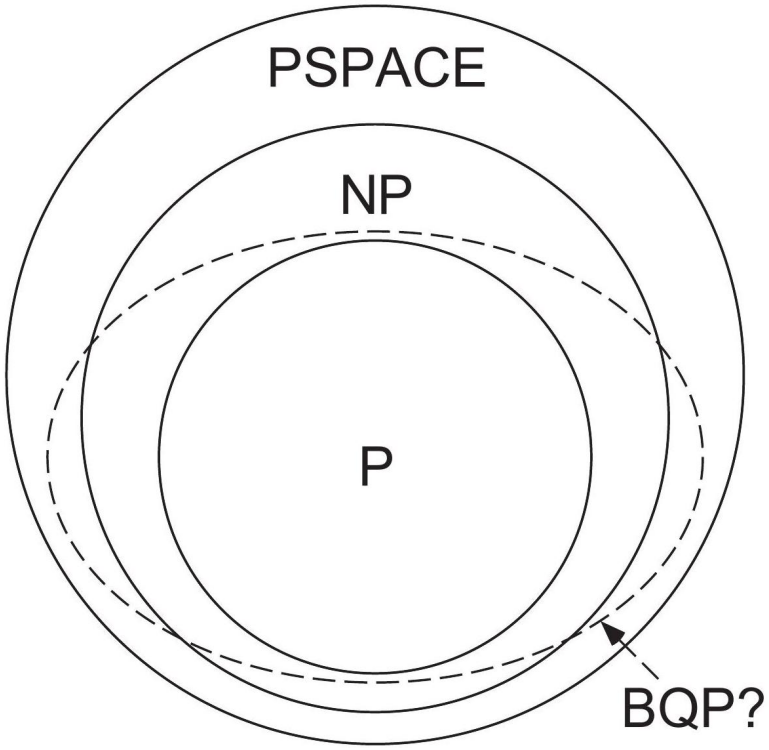


Figure 1.21. The relationship between classical and quantum complexity classes. Quantum computers can quickly solve any problem in P, and it is known that they can't solve problems outside of PSPACE quickly. Where quantum computers fit between $\mathbf{P
$ and PSPACE is not known, in part because we don't even know whether PSPACE is bigger than P!}

We won't speculate further on the ultimate power of quantum computation now, preferring to wait until after we have better understood the principles on which fast quantum algorithms are based, a topic which occupies us for most of Part II of this book. What is already clear is that the theory of quantum computation poses interesting and significant challenges to the traditional notions of computation. What makes this an important challenge is that the theoretical model of quantum computation is believed to be experimentally realizable, because - to

the best of our knowledge - this theory is consistent with the way Nature works. If this were not so then quantum computation would be just another mathematical curiosity.

7.1.20 1.5 Experimental quantum information processing

Quantum computation and quantum information is a wonderful theoretical discovery, but its central concepts, such as superpositions and entanglement, run counter to the intuition we garner from the everyday world around us. What evidence do we have that these ideas truly describe how Nature operates? Will the realization of large-scale quantum computers be experimentally feasible? Or might there be some principle of physics which fundamentally prohibits their eventual scaling? In the next two sections we address these questions. We begin with a review of the famous 'Stern-Gerlach' experiment, which provides evidence for the existence of qubits in Nature. We then widen our scope, addressing the broader problem of how to build practical quantum information processing systems.

7.1.21 1.5.1 The Stern-Gerlach experiment

The qubit is a fundamental element for quantum computation and quantum information. How do we know that systems with the properties of qubits exist in Nature? At the time of writing there is an enormous amount of evidence that this is so, but in the early days of quantum mechanics the qubit structure was not at all obvious, and people struggled with phenomena that we may now understand in terms of qubits, that is, in terms of two level quantum systems.

A decisive (and very famous) early experiment indicating the qubit structure was conceived by Stern in 1921 and performed with Gerlach in 1922 in Frankfurt. In the original Stern-Gerlach experiment, hot atoms were 'beamed' from an oven through a magnetic field which caused the atoms to be deflected, and then the position of each atom was recorded, as illustrated in Figure 1.22. The original experiment was done with silver atoms, which have a complicated structure that obscures the effects we are discussing. What we describe below actually follows a 1927 experiment done using hydrogen atoms. The same basic effect is observed, but with hydrogen atoms the discussion is easier to follow. Keep in mind, though, that this privilege wasn't available to people in the early 1920s, and they had to be very ingenious to think up explanations for the more complicated effects they observed.

Hydrogen atoms contain a proton and an orbiting electron. You can think of this electron as a little 'electric current' around the proton. This electric current causes the atom to have a magnetic field; each atom has what physicists call a'magnetic dipole moment'. As a result each atom behaves like a little bar magnet with an axis corresponding to the axis the electron is spinning around. Throwing little bar magnets through a magnetic field causes the magnets to be deflected by the field, and we expect to see a similar deflection of atoms in the Stern-Gerlach experiment.

How the atom is deflected depends upon both the atom's magnetic dipole moment the axis the electron is spinning around - and the magnetic field generated by the SternGerlach device. We won't go through the details, but suffice to say that by constructing the Stern-Gerlach device appropriately, we can cause the atom to be deflected by an amount that depends upon the $\hat{z}$ component of the atom's magnetic dipole moment, where $\hat{z}$ is some fixed external axis.

Two major surprises emerge when this experiment is performed. First, since the hot atoms exiting the oven would naturally be expected to have their dipoles oriented randomly in every direction, it would follow that there would be a continuous distribution of atoms seen at all angles exiting from the Stern-Gerlach device. Instead, what is seen is atoms emerging from a discrete set of angles. Physicists were able to explain this by assuming that the magnetic dipole moment of the atoms is quantized, that is, comes in discrete multiples of some fundamental

amount.

This observation of quantization in the Stern-Gerlach experiment was surprising to physicists of the 1920s, but not completely astonishing because evidence for quantization effects in other systems was becoming widespread at that time. What was truly surprising was the number of peaks seen in the experiment. The hydrogen atoms being used were such that they should have had zero magnetic dipole moment. Classically, this is surprising in itself, since it corresponds to no orbital motion of the electron, but based on what was known of quantum mechanics at that time this was an acceptable notion. Since the hydrogen atoms would therefore have zero magnetic moment, it was expected that only one beam of atoms would be seen, and this beam would not be deflected by the magnetic field. Instead, two beams were seen, one deflected up by the magnetic field, and the other deflected down!

This puzzling doubling was explained after considerable effort by positing that the electron in the hydrogen atom has associated with it a quantity called spin. This spin is not in any way associated to the usual rotational motion of the electron around the proton; it is an entirely new quantity to be associated with an electron. The great physicist Heisenberg labeled the idea 'brave' at the time it was suggested, and it is a brave idea, since it introduces an essentially new physical quantity into Nature. The spin of the electron is posited to make an extra contribution to the magnetic dipole moment of a hydrogen atom, in addition to the contribution due to the rotational motion of the electron.

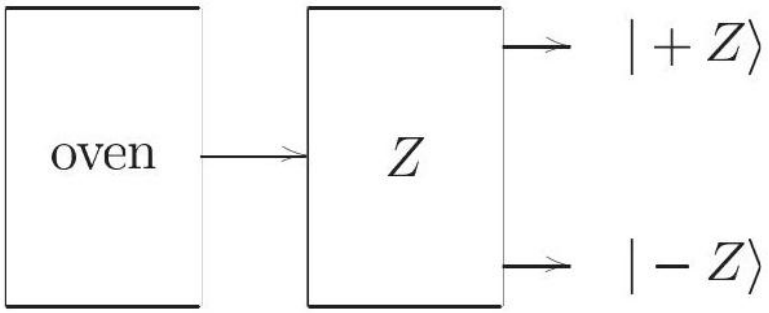


Figure 1.22. Abstract schematic of the Stern-Gerlach experiment. Hot hydrogen atoms are beamed from an oven through a magnetic field, causing a deflection either up ($|+Z\rangle$) or down ($|-Z\rangle$).

What is the proper description of the spin of the electron? As a first guess, we might hypothesize that the spin is specified by a single bit, telling the hydrogen atom to go up or down. Additional experimental results provide further useful information to determine if this guess needs refinement or replacement. Let's represent the original Stern-Gerlach apparatus as shown in Figure 1.22. Its outputs are two beams of atoms, which we shall call $|+Z\rangle$ and $|-Z\rangle$. (We're using suggestive notation which looks quantum mechanical, but of course you're free to use whatever notation you prefer.) Now suppose we cascade two Stern-Gerlach apparatus together, as shown in Figure 1.23. We arrange it so that the second apparatus is tipped sideways, so the magnetic field deflects atoms along the $\hat{x}$ axis. In our thought-experiment we'll block off the $|-Z\rangle$ output from the first Stern-Gerlach apparatus, while the $|+Z\rangle$ output is sent through a second apparatus oriented along the $\hat{x}$ axis. A detector is placed at the final output to measure the distribution of atoms along the $\hat{x}$ axis.

A classical magnetic dipole pointed in the $+\hat{z}$ direction has no net magnetic moment in the $\hat{x}$ direction, so we might expect that the final output would have one central peak. However, experimentally it is observed that there are two peaks of equal intensity! So perhaps these atoms are peculiar, and have definite magnetic moments along each axis, independently. That is, maybe each atom passing through the second apparatus can be

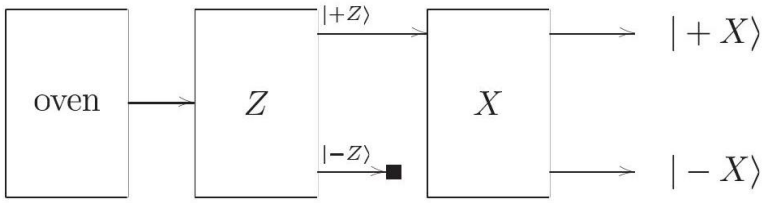


Figure 1.23. Cascaded Stern-Gerlach measurements.

described as being in a state we might write as $|+Z\rangle|+X\rangle$ or $|+Z\rangle|-X\rangle$, to indicate the two values for spin that might be observed.

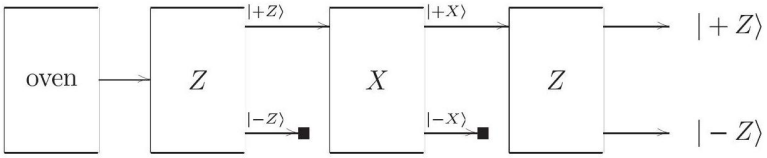


Figure 1.24. Three stage cascaded Stern-Gerlach measurements.

Another experiment, shown in Figure 1.24, can test this hypothesis by sending one beam of the previous output through a second $\hat{z}$ oriented Stern-Gerlach apparatus. If the atoms had retained their $|+Z\rangle$ orientation, then the output would be expected to have only one peak, at the $|+Z\rangle$ output. However, again two beams are observed at the final output, of equal intensity. Thus, the conclusion would seem to be that contrary to classical expectations, a$|+Z\rangle$ state consists of equal portions of $|+X\rangle$ and $|-X\rangle$ states, and a $|+X\rangle$ state consists of equal portions of $|+Z\rangle$ and $|-Z\rangle$ states. Similar conclusions can be reached if the Stern-Gerlach apparatus is aligned along some other axis, like the $\hat{y}$ axis.

The qubit model provides a simple explanation of this experimentally observed behavior. Let $|0\rangle$ and $|1\rangle$ be the states of a qubit, and make the assignments

$$|+Z\rangle \leftarrow |0\rangle \tag{1.56}$$
$$|-Z\rangle \leftarrow |1\rangle \tag{1.57}$$
$$|+X\rangle \leftarrow (|0\rangle + |1\rangle)/\sqrt{2}. \tag{1.58}$$
$$|-X\rangle \leftarrow (|0\rangle - |1\rangle)/\sqrt{2} \tag{1.59}$$

Then the results of the cascaded Stern-Gerlach experiment can be explained by assuming that the $\hat{z}$ Stern-Gerlach apparatus measures the spin (that is, the qubit) in the computational basis $|0\rangle, |1\rangle$, and the $\hat{x}$ Stern-Gerlach apparatus measures the spin with respect to the basis $(|0\rangle + |1\rangle)/\sqrt{2}, (|0\rangle - |1\rangle)/\sqrt{2}$. For example, in the cascaded $\hat{z} - \hat{x} - \hat{z}$ experiment, if we assume that the spins are in the state $|+Z\rangle = |0\rangle = (|+X\rangle + |-X\rangle)/\sqrt{2}$ after exiting the first Stern-Gerlach experiment, then the probability for obtaining $|+X\rangle$ out of the second apparatus is 1/2, and the probability for $|-X\rangle$ is 1/2. Similarly, the probability for obtaining $|+Z\rangle$ out of the third apparatus is 1/2. A qubit model thus properly predicts results from this type of cascaded Stern-Gerlach experiment.

This example demonstrates how qubits could be a believable way of modeling systems in Nature. Of course it doesn't establish beyond all doubt that the qubit model is the correct way of understanding electron spin - far more experimental corroboration is required. Nevertheless, because of many experiments like these, we now believe that electron spin is best described by

the qubit model. What is more, we believe that the qubit model (and generalizations of it to higher dimensions; quantum mechanics, in other words) is capable of describing every physical system. We now turn to the question of what systems are especially well adapted to quantum information processing.

7.1.22 1.5.2 Prospects for practical quantum information processing

Building quantum information processing devices is a great challenge for scientists and engineers of the third millennium. Will we rise to meet this challenge? Is it possible at all? Is it worth attempting? If so, how might the feat be accomplished? These are difficult and important questions, to which we essay brief answers in this section, to be expanded upon throughout the book.

The most fundamental question is whether there is any point of principle that prohibits us from doing one or more forms of quantum information processing? Two possible obstructions suggest themselves: that noise may place a fundamental barrier to useful quantum information processing; or that quantum mechanics may fail to be correct.

Noise is without a doubt a significant obstruction to the development of practical quantum information processing devices. Is it a fundamentally irremovable obstruction that will forever prevent the development of large-scale quantum information processing devices? The theory of quantum error-correcting codes strongly suggests that while quantum noise is a practical problem that needs to be addressed, it does not present a fundamental problem of principle. In particular, there is a threshold theorem for quantum computation, which states, roughly speaking, that provided the level of noise in a quantum computer can be reduced below a certain constant 'threshold' value, quantum error-correcting codes can be used to push it down even further, essentially ad infinitum, for a small overhead in the complexity of the computation. The threshold theorem makes some broad assumptions about the nature and magnitude of the noise occurring in a quantum computer, and the architecture available for performing quantum computation; however, provided those assumptions are satisfied, the effects of noise can be made essentially negligible for quantum information processing. Chapters 8,10 and 12 discuss quantum noise, quantum error-correction and the threshold theorem in detail.

A second possibility that may preclude quantum information processing is if quantum mechanics is incorrect. Indeed, probing the validity of quantum mechanics (both relativistic and non-relativistic) is one reason for being interested in building quantum information processing devices. Never before have we explored a regime of Nature in which complete control has been obtained over large-scale quantum systems, and perhaps Nature may reveal some new surprises in this regime which are not adequately explained by quantum mechanics. If this occurs, it will be a momentous discovery in the history of science, and can be expected to have considerable consequences in other areas of science and technology, as did the discovery of quantum mechanics. Such a discovery might also impact quantum computation and quantum information; however, whether the impact would enhance, detract or not affect the power of quantum information processing cannot be predicted in advance. Until and unless such effects are found we have no way of knowing how they might affect information processing, so for the remainder of this book
we go with all the evidence to date and assume that quantum mechanics is a complete and correct description of the world.

Given that there is no fundamental obstacle to building quantum information processing devices, why should we invest enormous amounts of time and money in the attempt to do so? We have already discussed several reasons for wanting to do so: practical applications such as quantum cryptography and the factoring of large composite numbers; and the desire to obtain fundamental insights into Nature and into information processing.

These are good reasons, and justify a considerable investment of time and money in the effort to build quantum information processing devices. However, it is fair to say that a clearer picture of the relative power of quantum and classical information processing is needed in order to assess their relative merits. To obtain such a picture requires further theoretical work on the foundations of quantum computation and quantum information. Of particular interest is a decisive answer to the question 'Are quantum computers more powerful than classical computers?' Even if the answer to such a question eludes us for the time being, it would be useful to have a clear path of interesting applications at varying levels of complexity to aid researchers aiming to experimentally realize quantum information processing. Historically, the advance of technology is often hastened by the use of short- to medium-term incentives as a stepping-stone to long-term goals. Consider that microprocessors were initially used as controllers for elevators and other simple devices, before graduating to be the fundamental component in personal computers (and then on to who-knows-what). Below we sketch out a path of short- to medium-term goals for people interested in achieving the long-term goal of large-scale quantum information processing.

Surprisingly many small-scale applications of quantum computation and quantum information are known. Not all are as flashy as cousins like the quantum factoring algorithm, but the relative ease of implementing small-scale applications makes them extremely important as medium-term goals in themselves.

Quantum state tomography and quantum process tomography are two elementary processes whose perfection is of great importance to quantum computation and quantum information, as well as being of independent interest in their own right. Quantum state tomography is a method for determining the quantum state of a system. To do this, it has to overcome the 'hidden' nature of the quantum state - remember, the state can't be directly determined by a measurement - by performing repeated preparations of the same quantum state, which is then measured in different ways in order to build up a complete description of the quantum state. Quantum process tomography is a more ambitious (but closely related) procedure to completely characterize the dynamics of a quantum system. Quantum process tomography can, for example, be used to characterize the performance of an alleged quantum gate or quantum communications channel, or to determine the types and magnitudes of different noise processes in a system. Beside obvious applications to quantum computation and quantum information, quantum process tomography can be expected to have significant applications as a diagnostic tool to aid in the evaluation and improvement of primitive operations in any field of science and technology where quantum effects are important. Quantum state tomography and quantum process tomography are described in more detail in Chapter 8.

Various small-scale communications primitives are also of great interest. We have already mentioned quantum cryptography and quantum teleportation. The former is likely to be useful in practical applications involving the distribution of a small amount of key
material that needs to be highly secure. The uses of quantum teleportation are perhaps more open to question. We will see in Chapter 12 that teleportation may be an extremely useful primitive for transmitting quantum states between distant nodes in a network, in the presence of noise. The idea is to focus one's efforts on distributing EPR pairs between the nodes that wish to communicate. The EPR pairs may be corrupted during communication, but special 'entanglement distillation' protocols can then be used to 'clean up' the EPR pairs, enabling them to be used to teleport quantum states from one location to another. In fact, procotols based upon entanglement distillation and teleportation offer performance superior to more conventional quantum error-correction techniques in enabling noise free communication of qubits.

What of the medium-scale? A promising medium-scale application of quantum information processing is to the simulation of quantum systems. To simulate a quantum system containing even a few dozen 'qubits' (or the equivalent in terms of some other basic system) strains the

resources of even the largest supercomputers. A simple calculation is instructive. Suppose we have a system containing 50 qubits. To describe the state of such a system requires $2^{50} \approx 10^{15}$ complex amplitudes. If the amplitudes are stored to 128 bits of precision, then it requires 256 bits or 32 bytes in order to store each amplitude, for a total of 32×10^{15} bytes of information, or about 32 thousand terabytes of information, well beyond the capacity of existing computers, and corresponding to about the storage capacity that might be expected to appear in supercomputers during the second decade of the twenty-first century, presuming that Moore's law continues on schedule. 90 qubits at the same level of precision requires 32×10^{27} bytes, which, even if implemented using single atoms to represent bits, would require kilograms (or more) of matter.

How useful will quantum simulations be? It seems likely that conventional methods will still be used to determine elementary properties of materials, such as bond strengths and basic spectroscopic properties. However, once the basic properties are well understood, it seems likely that quantum simulation will be of great utility as a laboratory for the design and testing of properties of novel molecules. In a conventional laboratory setup, many different types of 'hardware' - chemicals, detectors, and so on - may be required to test a wide variety of possible designs for a molecule. On a quantum computer, these different types of hardware can all be simulated in software, which is likely to be much less expensive and much faster. Of course, final design and testing must be performed with real physical systems; however, quantum computers may enable a much larger range of potential designs to be explored and evaluated en route to a better final design. It is interesting to note that such ab initio calculations to aid in the design of new molecules have been attempted on classical computers; however, they have met with limited success due to the enormous computational resources needed to simulate quantum mechanics on a classical computer. Quantum computers should be able to do much better in the relatively near future.

What of large-scale applications? Aside from scaling up applications like quantum simulation and quantum cryptography, relatively few large-scale applications are known: the factoring of large numbers, taking discrete logarithms, and quantum searching. Interest in the first two of these derives mainly from the negative effect they would have of limiting the viability of existing public key cryptographic systems. (They might also be of substantial practical interest to mathematicians interested in these problems simply for their own sake.) So it does not seem likely that factoring and discrete logarithm
will be all that important as applications for the long run. Quantum searching may be of tremendous use because of the wide utility of the search heuristic, and we discuss some possible applications in Chapter 6. What would really be superb are many more large-scale applications of quantum information processing. This is a great goal for the future!

Given a path of potential applications for quantum information processing, how can it be achieved in real physical systems? At the small scale of a few qubits there are already several working proposals for quantum information processing devices. Perhaps the easiest to realize are based upon optical techniques, that is, electromagnetic radiation. Simple devices like mirrors and beamsplitters can be used to do elementary manipulations of photons. Interestingly, a major difficulty has been producing single photons on demand; experimentalists have instead opted to use schemes which produce single photons 'every now and then', at random, and wait for such an event to occur. Quantum cryptography, superdense coding, and quantum teleportation have all been realized using such optical techniques. A major advantage of the optical techniques is that photons tend to be highly stable carriers of quantum mechanical information. A major disadvantage is that photons don't directly interact with one another. Instead, the interaction has to be mediated by something else, like an atom, which introduces additional noise and complications into the experiment. An effective interaction between two photons is set up, which essentially works in two steps: photon number one interacts with the

atom, which in turn interacts with the second photon, causing an overall interaction between the two photons.

An alternative scheme is based upon methods for trapping different types of atom: there is the ion trap, in which a small number of charged atoms are trapped in a confined space; and neutral atom traps, for trapping uncharged atoms in a confined space. Quantum information processing schemes based upon atom traps use the atoms to store qubits. Electromagnetic radiation also shows up in these schemes, but in a rather different way than in what we referred to as the 'optical' approach to quantum information processing. In these schemes, photons are used to manipulate the information stored in the atoms themselves, rather than as the place the information is stored. Single qubit quantum gates can be performed by applying appropriate pulses of electromagnetic radiation to individual atoms. Neighboring atoms can interact with one another via (for example) dipole forces that enable quantum gates to be accomplished. Moreover, the exact nature of the interaction between neighboring atoms can be modified by applying appropriate pulses of electromagnetic radiation to the atoms, giving the experimentalist control over what gates are performed in the system. Finally, quantum measurement can be accomplished in these systems using the long established quantum jumps technique, which implements with superb accuracy the measurements in the computational basis used for quantum computation.

Another class of quantum information processing schemes is based upon Nuclear Magnetic Resonance, often known by its initials, NMR. These schemes store quantum information in the nuclear spin of atoms in a molecule, and manipulate that information using electromagnetic radiation. Such schemes pose special difficulties, because in NMR it is not possible to directly access individual nuclei. Instead, a huge number (typically around 10^{15}) of essentially identical molecules are stored in solution. Electromagnetic pulses are applied to the sample, causing each molecule to respond in roughly the same way. You should think of each molecule as being an independent computer, and the sample as containing a huge number of computers all running in parallel (classically).

NMR quantum information processing faces three special difficulties that make it rather different from other quantum information processing schemes. First, the molecules are typically prepared by letting them equilibrate at room temperature, which is so much higher than typical spin flip energies that the spins become nearly completely randomly oriented. This fact makes the initial state rather more 'noisy' than is desirable for quantum information processing. How this noise may be overcome is an interesting story that we tell in Chapter 7. A second problem is that the class of measurements that may be performed in NMR falls well short of the most general measurements we would like to perform in quantum information processing. Nevertheless, for many instances of quantum information processing the class of measurements allowed in NMR is sufficient. Third, because molecules cannot be individually addressed in NMR you might ask how it is that individual qubits can be manipulated in an appropriate way. Fortunately, different nuclei in the molecule can have different properties that allow them to be individually addressed - or at least addressed at a sufficiently fine-grained scale to allow the operations essential for quantum computation.

Many of the elements required to perform large-scale quantum information processing can be found in existing proposals: superb state preparation and quantum measurements can be performed on a small number of qubits in the ion trap; superb dynamics can be performed in small molecules using NMR; fabrication technology in solid state systems allows designs to be scaled up tremendously. A single system having all these elements would be a long way down the road to a dream quantum computer. Unfortunately, all these systems are very different, and we are many, many years from having large-scale quantum computers. However, we believe that the existence of all these properties in existing (albeit different) systems does bode well for the long-term existence of largescale quantum information processors. Furthermore, it suggests

that there is a great deal of merit to pursuing hybrid designs which attempt to marry the best features of two or more existing technologies. For example, there is much work being done on trapping atoms inside electromagnetic cavities. This enables flexible manipulation of the atom inside the cavity via optical techniques, and makes possible real-time feedback control of single atoms in ways unavailable in conventional atom traps.

To conclude, note that it is important not to assess quantum information processing as though it were just another technology for information processing. For example, it is tempting to dismiss quantum computation as yet another technological fad in the evolution of the computer that will pass in time, much as other fads have passed - for example, the 'bubble memories' widely touted as the next big thing in memory during the early 1980s. This is a mistake, since quantum computation is an abstract paradigm for information processing that may have many different implementations in technology. One can compare two different proposals for quantum computing as regards their technological merits - it makes sense to compare a 'good' proposal to a 'bad' proposal - however even a very poor proposal for a quantum computer is of a different qualitative nature from a superb design for a classical computer.

7.1.23 1.6 Quantum information

The term 'quantum information' is used in two distinct ways in the field of quantum computation and quantum information. The first usage is as a broad catch-all for all manner of operations that might be interpreted as related to information processing
using quantum mechanics. This use encompasses subjects such as quantum computation, quantum teleportation, the no-cloning theorem, and virtually all other topics in this book.

The second use of 'quantum information' is much more specialized: it refers to the study of elementary quantum information processing tasks. It does not typically include, for example, quantum algorithm design, since the details of specific quantum algorithms are beyond the scope of 'elementary'. To avoid confusion we will use the term 'quantum information theory' to refer to this more specialized field, in parallel with the widely used term '(classical) information theory' to describe the corresponding classical field. Of course, the term 'quantum information theory' has a drawback of its own - it might be seen as implying that theoretical considerations are all that matter! Of course, this is not the case, and experimental demonstration of the elementary processes studied by quantum information theory is of great interest.

The purpose of this section is to introduce the basic ideas of quantum information theory. Even with the restriction to elementary quantum information processing tasks, quantum information theory may look like a disordered zoo to the beginner, with many apparently unrelated subjects falling under the 'quantum information theory' rubric. In part, that's because the subject is still under development, and it's not yet clear how all the pieces fit together. However, we can identify a few fundamental goals uniting work on quantum information theory:
(1) Identify elementary classes of static resources in quantum mechanics. An example is the qubit. Another example is the bit; classical physics arises as a special case of quantum physics, so it should not be surprising that elementary static resources appearing in classical information theory should also be of great relevance in quantum information theory. Yet another example of an elementary class of static resources is a Bell state shared between two distant parties.
(2) Identify elementary classes of dynamical processes in quantum mechanics. A simple example is memory, the ability to store a quantum state over some period of time. Less trivial processes are quantum information transmission between two parties, Alice and Bob; copying (or trying to copy) a quantum state, and the process of protecting quantum information processing against the effects of noise.
(3) Quantify resource tradeoffs incurred performing elementary dynamical processes. For example, what are the minimal resources required to reliably transfer quantum information between

two parties using a noisy communications channel?

Similar goals define classical information theory; however, quantum information theory is broader in scope than classical information theory, for quantum information theory includes all the static and dynamic elements of classical information theory, as well as additional static and dynamic elements.

The remainder of this section describes some examples of questions studied by quantum information theory, in each case emphasizing the fundamental static and dynamic elements under consideration, and the resource tradeoffs being considered. We begin with an example that will appear quite familiar to classical information theorists: the problem of sending classical information through a quantum channel. We then begin to branch out and explore some of the new static and dynamic processes present in quantum mechanics, such as quantum error-correction, the problem of distinguishing quantum states, and entanglement transformation. The chapter concludes with some reflections on how the
tools of quantum information theory can be applied elsewhere in quantum computation and quantum information.

7.1.24 1.6.1 Quantum information theory: example problems

Classical information through quantum channels

The fundamental results of classical information theory are Shannon's noiseless channel coding theorem and Shannon's noisy channel coding theorem. The noiseless channel coding theorem quantifies how many bits are required to store information being emitted by a source of information, while the noisy channel coding theorem quantifies how much information can be reliably transmitted through a noisy communications channel.

What do we mean by an information source? Defining this notion is a fundamental problem of classical and quantum information theory, one we'll re-examine several times. For now, let's go with a provisional definition: a classical information source is described by a set of probabilities $p_j, j = 1, 2, \ldots, d$. Each use of the source results in the 'letter' j being emitted, chosen at random with probability p_j, independently for each use of the source. For instance, if the source were of English text, then the numbers j might correspond to letters of the alphabet and punctuation, with the probabilities p_j giving the relative frequencies with which the different letters appear in regular English text. Although it is not true that the letters in English appear in an independent fashion, for our purposes it will be a good enough approximation.

Regular English text includes a considerable amount of redundancy, and it is possible to exploit that redundancy to compress the text. For example, the letter 'e' occurs much more frequently in regular English text than does the letter ' z '. A good scheme for compressing English text will therefore represent the letter 'e' using fewer bits of information than it uses to represent ' z '. Shannon's noiseless channel coding theorem quantifies exactly how well such a compression scheme can be made to work. More precisely, the noiseless channel coding theorem tells us that a classical source described by probabilities p_j can be compressed so that on average each use of the source can be represented using $H(p_j)$ bits of information, where $H(p_j) \equiv -\sum_j p_j \log(p_j)$ is a function of the source probability distribution known as the Shannon entropy. Moreover, the noiseless channel coding theorem tells us that to attempt to represent the source using fewer bits than this will result in a high probability of error when the information is decompressed. (Shannon's noiseless channel coding theorem is discussed in much greater detail in Chapter 12.)

Shannon's noiseless coding theorem provides a good example where the goals of information theory listed earlier are all met. Two static resources are identified (goal number 1): the bit and the information source. A two-stage dynamic process is identified (goal 2), compressing an information source, and then decompressing to recover the information source. Finally

a quantitative criterion for determining the resources consumed (goal 3) by an optimal data compression scheme is found.

Shannon's second major result, the noisy channel coding theorem, quantifies the amount of information that can be reliably transmitted through a noisy channel. In particular, suppose we wish to transfer the information being produced by some information source to another location through a noisy channel. That location may be at another point in space, or at another point in time - the latter is the problem of storing information in the presence of noise. The idea in both instances is to encode the information being produced using error-correcting codes, so that any noise introduced by the channel can be corrected at the other end of the channel. The way error-correcting codes achieve this
is by introducing enough redundancy into the information sent through the channel so that even after some of the information has been corrupted it is still possible to recover the original message. For example, suppose the noisy channel is for the transmission of single bits, and the noise in the channel is such that to achieve reliable transmission each bit produced by the source must be encoded using two bits before being sent through the channel. We say that such a channel has a capacity of half a bit, since each use of the channel can be used to reliably convey roughly half a bit of information. Shannon's noisy channel coding theorem provides a general procedure for calculating the capacity of an arbitrary noisy channel.

Shannon's noisy channel coding theorem also achieves the three goals of information theory we stated earlier. Two types of static resources are involved (goal 1), the information source, and the bits being sent through the channel. Three dynamical processes are involved (goal 2). The primary process is the noise in the channel. To combat this noise we perform the dual processes of encoding and decoding the state in an error-correcting code. For a fixed noise model, Shannon's theorem tells us how much redundancy must be introduced by an optimal error-correction scheme if reliable information transmission is to be achieved (goal 3).

For both the noiseless and noisy channel coding theorems Shannon restricted himself to storing the output from an information source in classical systems - bits and the like. A natural question for quantum information theory is what happens if the storage medium is changed so that classical information is transmitted using quantum states as the medium. For example, it may be that Alice wishes to compress some classical information produced by an information source, transmitting the compressed information to Bob, who then decompresses it. If the medium used to store the compressed information is a quantum state, then Shannon's noiseless channel coding theorem cannot be used to determine the optimal compression and decompression scheme. One might wonder, for example, if using qubits allows a better compression rate than is possible classically. We'll study this question in Chapter 12, and prove that, in fact, qubits do not allow any significant saving in the amount of communication required to transmit information over a noiseless channel.

Naturally, the next step is to investigate the problem of transmitting classical information through a noisy quantum channel. Ideally, what we'd like is a result that quantifies the capacity of such a channel for the transmission of information. Evaluating the capacity is a very tricky job for several reasons. Quantum mechanics gives us a huge variety of noise models, since it takes place in a continuous space, and it is not at all obvious how to adapt classical error-correction techniques to combat the noise. Might it be advantageous, for example, to encode the classical information using entangled states, which are then transmitted one piece at a time through the noisy channel? Or perhaps it will be advantageous to decode using entangled measurements? In Chapter 12 we'll prove the HSW (Holevo-Schumacher-Westmoreland) theorem, which provides a lower bound on the capacity of such a channel. Indeed, it is widely believed that the HSW theorem provides an exact evaluation of the capacity, although a complete proof of this is not yet known! What remains at issue is whether or not encoding using entangled states can be used to raise the capacity beyond the lower bound provided by the HSW theorem. All evidence

to date suggests that this doesn't help raise the capacity, but it is still a fascinating open problem of quantum information theory to determine the truth or falsity of this conjecture.

Quantum information through quantum channels

Classical information is, of course, not the only static resource available in quantum mechanics. Quantum states themselves are a natural static resource, even more natural than classical information. Let's look at a different quantum analogue of Shannon's coding theorems, this time involving the compression and decompression of quantum states.

To begin, we need to define some quantum notion of an information source, analogous to the classical definition of an information source. As in the classical case, there are several different ways of doing this, but for the sake of definiteness let's make the provisional definition that a quantum source is described by a set of probabilities p_j and corresponding quantum states $|\psi_j\rangle$. Each use of the source produces a state $|\psi_j\rangle$ with probability p_j, with different uses of the source being independent of one another.

Is it possible to compress the output from such a quantum mechanical source? Consider the case of a qubit source which outputs the state $|0\rangle$ with probability p and the state $|1\rangle$ with probability $1-p$. This is essentially the same as a classical source emitting single bits, either 0 with probability p, or 1 with probability $1-p$, so it is not surprising that similar techniques can be used to compress the source so that only $H(p, 1-p)$ qubits are required to store the compressed source, where $H(\cdot)$ is again the Shannon entropy function.

What if the source had instead been producing the state $|0\rangle$ with probability p, and the state $(|0\rangle + |1\rangle)/\sqrt{2}$ with probability $1-p$? The standard techniques of classical data compression no longer apply, since in general it is not possible for us to distinguish the states $|0\rangle$ and $(|0\rangle + |1\rangle)/\sqrt{2}$. Might it still be possible to perform some type of compression operation?

It turns out that a type of compression is still possible, even in this instance. What is interesting is that the compression may no longer be error-free, in the sense that the quantum states being produced by the source may be slightly distorted by the compressiondecompression procedure. Nevertheless, we require that this distortion ought to become very small and ultimately negligible in the limit of large blocks of source output being compressed. To quantify the distortion we introduce a fidelity measure for the compression scheme, which measures the average distortion introduced by the compression scheme. The idea of quantum data compression is that the compressed data should be recovered with very good fidelity. Think of the fidelity as being analogous to the probability of doing the decompression correctly - in the limit of large block lengths, it should tend towards the no error limit of 1 .

Schumacher's noiseless channel coding theorem quantifies the resources required to do quantum data compression, with the restriction that it be possible to recover the source with fidelity close to 1 . In the case of a source producing orthogonal quantum states $|\psi_j\rangle$ with probabilities p_j Schumacher's theorem reduces to telling us that the source may be compressed down to but not beyond the classical limit $H(p_j)$. However, in the more general case of non-orthogonal states being produced by the source, Schumacher's theorem tells us how much a quantum source may be compressed, and the answer is not the Shannon entropy $H(p_j)$! Instead, a new entropic quantity, the von Neumann entropy, turns out to be the correct answer. In general, the von Neumann entropy agrees with the Shannon entropy if and only if the states $|\psi_j\rangle$ are orthogonal. Otherwise, the von Neumann entropy for the source $p_j, |\psi_j\rangle$ is in general strictly smaller than the Shannon entropy $H(p_j)$. Thus, for example, a source producing the state $|0\rangle$ with probability p
and $(|0\rangle + |1\rangle)/\sqrt{2}$ with probability $1-p$ can be reliably compressed using fewer than $H(p, 1-p)$ qubits per use of the source!

The basic intuition for this decrease in resources required can be understood quite easily. Suppose the source emitting states $|0\rangle$ with probability p and $(|0\rangle + |1\rangle)/\sqrt{2}$ with probability

$1-p$ is used a large number n times. Then by the law of large numbers, with high probability the source emits about np copies of $|0\rangle$ and $n(1-p)$ copies of $(|0\rangle+|1\rangle)/\sqrt{2}$. That is, it has the form

$$|0\rangle^{\otimes np}\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)^{\otimes n(1-p)} \tag{1.60}$$

up to re-ordering of the systems involved. Suppose we expand the product of $|0\rangle+|1\rangle$ terms on the right hand side. Since $n(1-p)$ is large, we can again use the law of large numbers to deduce that the terms in the product will be roughly one-half $|0\rangle$s and onehalf $|1\rangle$s. That is, the $|0\rangle+|1\rangle$ product can be well approximated by a superposition of states of the form

$$|0\rangle^{\otimes n(1-p)/2}|1\rangle^{\otimes n(1-p)/2} \tag{1.61}$$

Thus the state emitted by the source can be approximated as a superposition of terms of the form

$$|0\rangle^{\otimes n(1+p)/2}|1\rangle^{\otimes n(1-p)/2} \tag{1.62}$$

How many states of this form are there? Roughly n choose $n(1+p)/2$, which by Stirling's approximation is equal to $N \equiv 2^{nH[(1+p)/2,(1-p)/2]}$. A simple compression method then is to label all states of the form (1.62) $|c_1\rangle$ through $|c_N\rangle$. It is possible to perform a unitary transform on the n qubits emitted from the source that takes $|c_j\rangle$ to $|j\rangle|0\rangle^{\otimes n-nH[(1+p)/2,(1-p)/2]}$, since j is an $nH[(1+p)/2,(1-p)/2]$ bit number. The compression operation is to perform this unitary transformation, and then drop the final $n-nH[(1+p)/2,(1-p)/2]$ qubits, leaving a compressed state of $nH[(1+p)/2,(1-p)/2]$ qubits. To decompress we append the state $|0\rangle^{\otimes n-nH[(1+p)/2,(1-p)/2]}$ to the compressed state, and perform the inverse unitary transformation.

This procedure for quantum data compression and decompression results in a storage requirement of $H[(1+p)/2,(1-p)/2]$ qubits per use of the source, which whenever $p \geq 1/3$ is an improvement over the $H(p,1-p)$ qubits we might naively have expected from Shannon's noiseless channel coding theorem. In fact, Schumacher's noiseless channel coding theorem allows us to do somewhat better even than this, as we will see in Chapter 12; however, the essential reason in that construction is the same as the reason we were able to compress here: we exploited the fact that $|0\rangle$ and $(|0\rangle+|1\rangle)/\sqrt{2}$ are not orthogonal. Intuitively, the states contain some redundancy since both have a component in the $|0\rangle$ direction, which results in more physical similarity than would be obtained from orthogonal states. It is this redundancy that we have exploited in the coding scheme just described, and which is used in the full proof of Schumacher's noiseless channel coding theorem. Note that the restriction $p \geq 1/3$ arises because when $p < 1/3$ this particular scheme doesn't exploit the redundancy in the states: we end up effectively increasing the redundancy present in the problem! Of course, this is an artifact of the particular scheme we have chosen, and the general solution exploits the redundancy in a much more sensible way to achieve data compression.

Schumacher's noiseless channel coding theorem is an analogue of Shannon's noiseless channel coding theorem for the compression and decompression of quantum states. Can we find an analogue of Shannon's noisy channel coding theorem? Considerable progress on this important question has been made, using the theory of quantum error-correcting codes; however, a fully satisfactory analogue has not yet been found. We review some of what is known about the quantum channel capacity in Chapter 12.

Quantum distinguishability

Thus far all the dynamical processes we have considered - compression, decompression, noise, encoding and decoding error-correcting codes - arise in both classical and quantum information

theory. However, the introduction of new types of information, such as quantum states, enlarges the class of dynamical processes beyond those considered in classical information theory. A good example is the problem of distinguishing quantum states. Classically, we are used to being able to distinguish different items of information, at least in principle. In practice, of course, a smudged letter 'a' written on a page may be very difficult to distinguish from a letter 'o', but in principle it is possible to distinguish between the two possibilities with perfect certainty.

On the other hand, quantum mechanically it is not always possible to distinguish between arbitrary states. For example, there is no process allowed by quantum mechanics that will reliably distinguish between the states $|0\rangle$ and $(|0\rangle + |1\rangle)/\sqrt{2}$. Proving this rigorously requires tools we don't presently have available (it is done in Chapter 2), but by considering examples it's pretty easy to convince oneself that it is not possible. Suppose, for example, that we try to distinguish the two states by measuring in the computational basis. Then, if we have been given the state $|0\rangle$, the measurement will yield 0 with probability 1 . However, when we measure $(|0\rangle + |1\rangle)/\sqrt{2}$ the measurement yields 0 with probability 1/2 and 1 with probability 1/2. Thus, while a measurement result of 1 implies that state must have been $(|0\rangle + |1\rangle)/\sqrt{2}$, since it couldn't have been $|0\rangle$, we can't infer anything about the identity of the quantum state from a measurement result of 0 .

This indistinguishability of non-orthogonal quantum states is at the heart of quantum computation and quantum information. It is the essence of our assertion that a quantum state contains hidden information that is not accessible to measurement, and thus plays a key role in quantum algorithms and quantum cryptography. One of the central problems of quantum information theory is to develop measures quantifying how well non-orthogonal quantum states may be distinguished, and much of Chapters 9 and 12 is concerned with this goal. In this introduction we'll limit ourselves to pointing out two interesting aspects of indistinguishability - a connection with the possibility of faster-than-light communication, and an application to 'quantum money.'

Imagine for a moment that we could distinguish between arbitrary quantum states. We'll show that this implies the ability to communicate faster than light, using entanglement. Suppose Alice and Bob share an entangled pair of qubits in the state $(|00\rangle+|11\rangle)/\sqrt{2}$. Then, if Alice measures in the computational basis, the post-measurement states will be $|00\rangle$ with probability 1/2, and $|11\rangle$ with probability 1/2. Thus Bob's system is either in the state $|0\rangle$, with probability 1/2, or in the state $|1\rangle$, with probability 1/2. Suppose, however, that Alice had instead measured in the $|+\rangle, |-\rangle$ basis. Recall that $|0\rangle = (|+\rangle + |-\rangle)/\sqrt{2}$ and $|1\rangle = (|+\rangle - |-\rangle)/\sqrt{2}$. A little algebra shows that the initial state of Alice and Bob's system may be rewritten as $(|++\rangle + |--\rangle)/\sqrt{2}$. Therefore, if Alice measures in the $|+\rangle, |-\rangle$ basis, the state of Bob's system after the measurement
will be $|+\rangle$ or $|-\rangle$ with probability 1/2 each. So far, this is all basic quantum mechanics. But if Bob had access to a device that could distinguish the four states $|0\rangle, |1\rangle, |+\rangle, |-\rangle$ from one another, then he could tell whether Alice had measured in the computational basis, or in the $|+\rangle, |-\rangle$ basis. Moreover, he could get that information instantaneously, as soon as Alice had made the measurement, providing a means by which Alice and Bob could achieve faster-than-light communication! Of course, we know that it is not possible to distinguish non-orthogonal quantum states; this example shows that this restriction is also intimately tied to other physical properties which we expect the world to obey.

The indistinguishability of non-orthogonal quantum states need not always be a handicap. Sometimes it can be a boon. Imagine that a bank produces banknotes imprinted with a (classical) serial number, and a sequence of qubits each in either the state $|0\rangle$ or $(|0\rangle + |1\rangle)/\sqrt{2}$. Nobody but the bank knows what sequence of these two states is embedded in the note, and the bank maintains a list matching serial numbers to embedded states. The note is impossible to counterfeit exactly, because it is impossible for a would-be counterfeiter to determine with

certainty the state of the qubits in the original note, without destroying them. When presented with the banknote a merchant (of certifiable repute) can verify that it is not a counterfeit by calling the bank, telling them the serial number, and then asking what sequence of states were embedded in the note. They can then check that the note is genuine by measuring the qubits in the $|0\rangle, |1\rangle$ or $(|0\rangle + |1\rangle)/\sqrt{2}, (|0\rangle - |1\rangle)/\sqrt{2}$ basis, as directed by the bank. With probability which increases exponentially to one with the number of qubits checked, any would-be counterfeiter will be detected at this stage! This idea is the basis for numerous other quantum cryptographic protocols, and demonstrates the utility of the indistinguishability of non-orthogonal quantum states.

Exercise 1.2: Explain how a device which, upon input of one of two non-orthogonal quantum states $|\psi\rangle$ or $|\varphi\rangle$ correctly identified the state, could be used to build a device which cloned the states $|\psi\rangle$ and $|\varphi\rangle$, in violation of the no-cloning theorem. Conversely, explain how a device for cloning could be used to distinguish non-orthogonal quantum states.

Creation and transformation of entanglement

Entanglement is another elementary static resource of quantum mechanics. Its properties are amazingly different from those of the resources most familiar from classical information theory, and they are not yet well understood; we have at best an incomplete collage of results related to entanglement. We don't yet have all the language needed to understand the solutions, but let's at least look at two information-theoretic problems related to entanglement.

Creating entanglement is a simple dynamical process of interest in quantum information theory. How many qubits must two parties exchange if they are to create a particular entangled state shared between them, given that they share no prior entanglement? A second dynamical process of interest is transforming entanglement from one form into another. Suppose, for example, that Alice and Bob share between them a Bell state, and wish to transform it into some other type of entangled state. What resources do they need to accomplish this task? Can they do it without communicating? With classical communication only? If quantum communication is required then how much quantum communication is required?

Answering these and more complex questions about the creation and transformation of entanglement forms a fascinating area of study in its own right, and also promises to give insight into tasks such as quantum computation. For example, a distributed quantum computation may be viewed as simply a method for generating entanglement between two or more parties; lower bounds on the amount of communication that must be done to perform such a distributed quantum computation then follow from lower bounds on the amount of communication that must be performed to create appropriate entangled states.

7.1.25 1.6.2 Quantum information in a wider context

We have given but the barest glimpse of quantum information theory. Part III of this book discusses quantum information theory in much greater detail, especially Chapter 11, which deals with fundamental properties of entropy in quantum and classical information theory, and Chapter 12, which focuses on pure quantum information theory.

Quantum information theory is the most abstract part of quantum computation and quantum information, yet in some sense it is also the most fundamental. The question driving quantum information theory, and ultimately all of quantum computation and quantum information, is what makes quantum information processing tick? What is it that separates the quantum and the classical world? What resources, unavailable in a classical world, are being utilized in a quantum computation? Existing answers to these questions are foggy and incomplete; it is our hope that the fog may yet lift in the years to come, and we will obtain a clear appreciation for the possibilities and limitations of quantum information processing.

Problem 1.1: (Feynman-Gates conversation) Construct a friendly imaginary discussion of about 2000 words between Bill Gates and Richard Feynman, set in the present, on the future of computation. (Comment: You might like to try waiting until you've read the rest of the book before attempting this question. See the 'History and further reading' below for pointers to one possible answer for this question.)

Problem 1.2: What is the most significant discovery yet made in quantum computation and quantum information? Write an essay of about 2000 words for an educated lay audience about the discovery. (Comment: As for the previous problem, you might like to try waiting until you've read the rest of the book before attempting this question.)

History and further reading

Most of the material in this chapter is revisited in more depth in later chapters. Therefore the historical references and further reading below are limited to material which does not recur in later chapters.

Piecing together the historical context in which quantum computation and quantum information have developed requires a broad overview of the history of many fields. We have tried to tie this history together in this chapter, but inevitably much background material was omitted due to limited space and expertise. The following recommendations attempt to redress this omission.

The history of quantum mechanics has been told in many places. We recommend especially the outstanding works of Pais [Pai82, Pai86, Pai91] . Of these three, [Pai86] is most directly concerned with the development of quantum mechanics; however, Pais' biographies of Einstein [Pai82] and of Bohr [Pai91] also contain much material of interest, at a less intense level. The rise of technologies based upon quantum mechanics has been described by Milburn [Mi197, Mil98]. Turing's marvelous paper on the foundations of computer science [Tur36] is well worth reading. It can be found in the valuable historical collection of Davis [Dav65] . Hofstadter [Hof79] and Penrose [Pen89] contain entertaining and informative discussions of the foundations of computer science. Shasha and Lazere's biography of fifteen leading computer scientists [*SL*98] gives considerable insight into many different facets of the history of computer science. Finally, Knuth's awesome series of books[Knu97, Knu98a, Knu98b] contain an amazing amount of historical information. Shannon's brilliant papers founding information theory make excellent reading[Sha48] (also reprinted in [*SW*49]). MacWilliams and Sloane [MS77] is not only an excellent text on error-correcting codes, but also contains an enormous amount of useful historical information. Similarly, Cover and Thomas [CT91] is an excellent text on information theory, with extensive historical information. Shannon's collected works, together with many useful historical items have been collected in a large volume [SW93] edited by Sloane and Wyner. Slepian has also collected a useful set of reprints on information theory [*Sle*74]. Cryptography is an ancient art with an intricate and often interesting history. Kahn [[Kah96] is a huge history of cryptography containing a wealth of information. For more recent developments we recommend the books by Menezes, van Oorschot, and Vanstone[MvOV96], Schneier [*Sch*96*a*], and by Diffie and Landau[DL98].

Quantum teleportation was discovered by Bennett, Brassard, Crépeau, Jozsa, Peres, and Wootters [BBC$^+$93], and later experimentally realized in various different forms by Boschi, Branca, De Martini, Hardy and Popescu [BBM$^+$98] using optical techniques, by Bouwmeester, Pan, Mattle, Eibl, Weinfurter, and Zeilinger [BPM$^+$97] using photon polarization, by Furusawa, Sørensen, Braunstein, Fuchs, Kimble, and Polzik using 'squeezed' states of light [FSB$^+$98], and by Nielsen, Knill, and Laflamme using NMR[NKL98].

Deutsch's problem was posed by Deutsch [Deu85], and a one-bit solution was given in the same paper. The extension to the general n-bit case was given by Deutsch and Jozsa [DJ92] .

The algorithms in these early papers have been substantially improved subsequently by Cleve, Ekert, Macchiavello, and Mosca[CEMM98], and independently in unpublished work by Tapp. In this chapter we have given the improved version of the algorithm, which fits very nicely into the hidden subgroup problem framework that will later be discussed in Chapter 5. The original algorithm of Deutsch only worked probabilistically; Deutsch and Jozsa improved this to obtain a deterministic algorithm, but their method required two function evaluations, in contrast to the improved algorithms presented in this chapter. Nevertheless, it is still conventional to refer to these algorithms as Deutsch's algorithm and the Deutsch-Jozsa algorithm in honor of two huge leaps forward: the concrete demonstration by Deutsch that a quantum computer could do something faster than a classical computer; and the extension by Deutsch and Jozsa which demonstrated for the first time a similar gap for the scaling of the time required to solve a problem.

Excellent discussions of the Stern-Gerlach experiment can be found in standard quantum mechanics textbooks such as the texts by Sakurai [Sak95] , Volume III of Feynman, Leighton and Sands [FLS65a], and Cohen-Tannoudji, Diu and Laloë[CTDl77a, CTDl77b].

Problem 1.1 was suggested by the lovely article of Rahim [Rah99].

7.2 2 Introduction to quantum mechanics

Quantum mechanics is the most accurate and complete description of the world known. It is also the basis for an understanding of quantum computation and quantum information. This chapter provides all the necessary background knowledge of quantum mechanics needed for a thorough grasp of quantum computation and quantum information. No prior knowledge of quantum mechanics is assumed.

Quantum mechanics is easy to learn, despite its reputation as a difficult subject. The reputation comes from the difficulty of some applications, like understanding the structure of complicated molecules, which aren't fundamental to a grasp of the subject; we won't be discussing such applications. The only prerequisite for understanding is some familiarity with elementary linear algebra. Provided you have this background you can begin working out simple problems in a few hours, even with no prior knowledge of the subject.

Readers already familiar with quantum mechanics can quickly skim through this chapter, to become familiar with our (mostly standard) notational conventions, and to assure themselves of familiarity with all the material. Readers with little or no prior knowledge should work through the chapter in detail, pausing to attempt the exercises. If you have difficulty with an exercise, move on, and return later to make another attempt.

The chapter begins with a review of some material from linear algebra in Section 2.1. This section assumes familiarity with elementary linear algebra, but introduces the notation used by physicists to describe quantum mechanics, which is different to that used in most introductions to linear algebra. Section 2.2 describes the basic postulates of quantum mechanics. Upon completion of the section, you will have understood all of the fundamental principles of quantum mechanics. This section contains numerous simple exercises designed to help consolidate your grasp of this material. The remaining sections of the chapter, and of this book, elucidate upon this material, without introducing fundamentally new physical principles. Section 2.3 explains superdense coding, a surprising and illuminating example of quantum information processing which combines many of the postulates of quantum mechanics in a simple setting. Sections 2.4 and 2.5 develop powerful mathematical tools - the density operator, purifications, and the Schmidt decomposition - which are especially useful in the study of quantum computation and quantum information. Understanding these tools will also help you consolidate your understanding of elementary quantum mechanics. Finally, Section 2.6 examines the question of how quantum mechanics goes beyond the usual 'classical' understanding of the way the world works.

7.2.1 2.1 Linear algebra

This book is written as much to disturb and annoy as to instruct.

- The first line of About Vectors, by Banesh Hoffmann.

Life is complex - it has both real and imaginary parts.

- Anonymous

Linear algebra is the study of vector spaces and of linear operations on those vector spaces. A good understanding of quantum mechanics is based upon a solid grasp of elementary linear algebra. In this section we review some basic concepts from linear algebra, and describe the standard notations which are used for these concepts in the study of quantum mechanics. These notations are summarized in Figure 2.1 on page 62, with the quantum notation in the left column, and the linear-algebraic description in the right column. You may like to glance at the table, and see how many of the concepts in the right column you recognize.

In our opinion the chief obstacle to assimilation of the postulates of quantum mechanics is not the postulates themselves, but rather the large body of linear algebraic notions required to understand them. Coupled with the unusual Dirac notation adopted by physicists for quantum mechanics, it can appear (falsely) quite fearsome. For these reasons, we advise the reader not familiar with quantum mechanics to quickly read through the material which follows, pausing mainly to concentrate on understanding the absolute basics of the notation being used. Then proceed to a careful study of the main topic of the chapter - the postulates of quantum mechanics - returning to study the necessary linear algebraic notions and notations in more depth, as required.

The basic objects of linear algebra are vector spaces. The vector space of most interest to us is $\mathbf{C}^n$, the space of all n-tuples of complex numbers, $(z_1, \ldots, z_n)$. The elements of a vector space are called vectors, and we will sometimes use the column matrix notation

$$\begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix} \tag{2.1}$$

to indicate a vector. There is an addition operation defined which takes pairs of vectors to other vectors. In $\mathbf{C}^n$ the addition operation for vectors is defined by

$$\begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix} + \begin{bmatrix} z'_1 \\ \vdots \\ z'_n \end{bmatrix} \equiv \begin{bmatrix} z_1 + z'_1 \\ \vdots \\ z_n + z'_n \end{bmatrix} \tag{2.2}$$

where the addition operations on the right are just ordinary additions of complex numbers. Furthermore, in a vector space there is a multiplication by a scalar operation. In $\mathbf{C}^n$ this operation is defined by

$$z \begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix} \equiv \begin{bmatrix} z z_1 \\ \vdots \\ z z_n \end{bmatrix} \tag{2.3}$$

where z is a scalar, that is, a complex number, and the multiplications on the right are ordinary multiplication of complex numbers. Physicists sometimes refer to complex numbers as c-numbers.

Quantum mechanics is our main motivation for studying linear algebra, so we will use the standard notation of quantum mechanics for linear algebraic concepts. The standard quantum mechanical notation for a vector in a vector space is the following:

$$|\psi\rangle. \tag{2.4}$$

ψ is a label for the vector (any label is valid, although we prefer to use simple labels like ψ and φ). The $|\cdot\rangle$ notation is used to indicate that the object is a vector. The entire object $|\psi\rangle$ is sometimes called a ket, although we won't use that terminology often.

A vector space also contains a special zero vector, which we denote by 0 . It satisfies the property that for any other vector $|v\rangle, |v\rangle + 0 = |v\rangle$. Note that we do not use the ket notation for the zero vector - it is the only exception we shall make. The reason for making the exception is because it is conventional to use the 'obvious' notation for the zero vector, $|0\rangle$, to mean something else entirely. The scalar multiplication operation is such that $z0 = 0$ for any complex number z. For convenience, we use the notation $(z_1, \ldots, z_n)$ to denote a column matrix with entries $z_1, \ldots, z_n$. In $\mathbf{C}^n$ the zero element is $(0, 0, \ldots, 0)$. A vector subspace of a vector space V is a subset W of V such that W is also a vector space, that is, W must be closed under scalar multiplication and addition.

Notation	Description
z^*	Complex conjugate of the complex number z. $(1+i)^* = 1-i$
$\|\psi\rangle$	Vector. Also known as a ket.
$\langle\psi\|$	Vector dual to $\|\psi\rangle$. Also known as a bra.
$\langle\varphi \mid \psi\rangle$	Inner product between the vectors $\|\varphi\rangle$ and $\|\psi\rangle$.
$\|\varphi\rangle \otimes \|\psi\rangle$	Tensor product of $\|\varphi\rangle$ and $\|\psi\rangle$.
$\|\varphi\rangle\|\psi\rangle$	Abbreviated notation for tensor product of $\|\varphi\rangle$ and $\|\psi\rangle$.
A^*	Complex conjugate of the A matrix.
A^T	Transpose of the A matrix.
$A^\dagger$	Hermitian conjugate or adjoint of the A matrix, $A^\dagger = \left(A^T\right)^*$.
	$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^\dagger = \begin{bmatrix} a^* & c^* \\ b^* & d^* \end{bmatrix}$.
$\langle\varphi\|A\|\psi\rangle$	Inner product between $\|\varphi\rangle$ and $A\|\psi\rangle$.
	Equivalently, inner product between $A^\dagger\|\varphi\rangle$ and $\|\psi\rangle$.

Figure 2.1. Summary of some standard quantum mechanical notation for notions from linear algebra. This style of notation is known as the Dirac notation.

7.2.2 2.1.1 Bases and linear independence

A spanning set for a vector space is a set of vectors $|v_1\rangle, \ldots, |v_n\rangle$ such that any vector $|v\rangle$ in the vector space can be written as a linear combination $|v\rangle = \sum_i a_i |v_i\rangle$ of vectors in that set. For example, a spanning set for the vector space $\mathbf{C}^2$ is the set

$$|v_1\rangle \equiv \begin{bmatrix} 1 \\ 0 \end{bmatrix}; \quad |v_2\rangle \equiv \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{2.5}$$

since any vector

$$|v\rangle = \begin{bmatrix} a_1 \\ a_2 \end{bmatrix} \tag{2.6}$$

in $\mathbf{C}^2$ can be written as a linear combination $|v\rangle = a_1 |v_1\rangle + a_2 |v_2\rangle$ of the vectors $|v_1\rangle$ and $|v_2\rangle$. We say that the vectors $|v_1\rangle$ and $|v_2\rangle$ span the vector space $\mathbf{C}^2$.

Generally, a vector space may have many different spanning sets. A second spanning set for the vector space $\mathbf{C}^2$ is the set

$$|v_1\rangle \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}; \quad |v_2\rangle \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} \tag{2.7}$$

since an arbitrary vector $|v\rangle = (a_1, a_2)$ can be written as a linear combination of $|v_1\rangle$ and $|v_2\rangle$,

$$|v\rangle = \frac{a_1 + a_2}{\sqrt{2}} |v_1\rangle + \frac{a_1 - a_2}{\sqrt{2}} |v_2\rangle . \tag{2.8}$$

A set of non-zero vectors $|v_1\rangle, \ldots, |v_n\rangle$ are linearly dependent if there exists a set of complex numbers $a_1, \ldots, a_n$ with $a_i \neq 0$ for at least one value of i, such that

$$a_1 |v_1\rangle + a_2 |v_2\rangle + \cdots + a_n |v_n\rangle = 0. \tag{2.9}$$

A set of vectors is linearly independent if it is not linearly dependent. It can be shown that any two sets of linearly independent vectors which span a vector space V contain the same number of elements. We call such a set a basis for V. Furthermore, such a basis set always exists. The number of elements in the basis is defined to be the dimension of V. In this book we will only be interested in finite dimensional vector spaces. There are many interesting and often difficult questions associated with infinite dimensional vector spaces. We won't need to worry about these questions.

Exercise 2.1: (Linear dependence: example) Show that $(1, -1), (1, 2)$ and $(2, 1)$ are linearly dependent.

7.2.3 2.1.2 Linear operators and matrices

A linear operator between vector spaces V and W is defined to be any function $A : V \rightarrow W$ which is linear in its inputs,

$$A \left(\sum_i a_i |v_i\rangle \right) = \sum_i a_i A \left(|v_i\rangle \right) . \tag{2.10}$$

Usually we just write $A|v\rangle$ to denote $A(|v\rangle)$. When we say that a linear operator A is defined on a vector space, V, we mean that A is a linear operator from V to V. An important linear operator on any vector space V is the identity operator, I_V, defined by the equation $I_V|v\rangle \equiv |v\rangle$ for all vectors $|v\rangle$. Where no chance of confusion arises we drop the subscript V and just write I to denote the identity operator. Another important linear operator is the zero operator, which we denote 0 . The zero operator maps all vectors to
the zero vector, $0|v\rangle \equiv 0$. It is clear from (2.10) that once the action of a linear operator A on a basis is specified, the action of A is completely determined on all inputs.

Suppose V, W, and X are vector spaces, and $A : V \rightarrow W$ and $B : W \rightarrow X$ are linear operators. Then we use the notation BA to denote the composition of B with A, defined by $(BA)(|v\rangle) \equiv B(A(|v\rangle))$. Once again, we write $BA|v\rangle$ as an abbreviation for $(BA)(|v\rangle)$.

The most convenient way to understand linear operators is in terms of their matrix representations. In fact, the linear operator and matrix viewpoints turn out to be completely equivalent. The matrix viewpoint may be more familiar to you, however. To see the connection, it helps to first understand that an m by n complex matrix A with entries A_{ij} is in fact a linear operator sending vectors in the vector space $\mathbf{C}^n$ to the vector space $\mathbf{C}^m$, under matrix

multiplication of the matrix A by a vector in $\mathbf{C}^n$. More precisely, the claim that the matrix A is a linear operator just means that

$$A\left(\sum_i a_i |v_i\rangle\right) = \sum_i a_i A |v_i\rangle \tag{2.11}$$

is true as an equation where the operation is matrix multiplication of A by column vectors. Clearly, this is true!

We've seen that matrices can be regarded as linear operators. Can linear operators be given a matrix representation? In fact they can, as we now explain. This equivalence between the two viewpoints justifies our interchanging terms from matrix theory and operator theory throughout the book. Suppose $A : V \rightarrow W$ is a linear operator between vector spaces V and W. Suppose $|v_1\rangle, \ldots, |v_m\rangle$ is a basis for V and $|w_1\rangle, \ldots, |w_n\rangle$ is a basis for W. Then for each j in the range $1, \ldots, m$, there exist complex numbers A_{1j} through A_{nj} such that

$$A |v_j\rangle = \sum_i A_{ij} |w_i\rangle \tag{2.12}$$

The matrix whose entries are the values A_{ij} is said to form a matrix representation of the operator A. This matrix representation of A is completely equivalent to the operator A, and we will use the matrix representation and abstract operator viewpoints interchangeably. Note that to make the connection between matrices and linear operators we must specify a set of input and output basis states for the input and output vector spaces of the linear operator.

Exercise 2.2: (Matrix representations: example) Suppose V is a vector space with basis vectors $|0\rangle$ and $|1\rangle$, and A is a linear operator from V to V such that $A|0\rangle = |1\rangle$ and $A|1\rangle = |0\rangle$. Give a matrix representation for A, with respect to the input basis $|0\rangle, |1\rangle$, and the output basis $|0\rangle, |1\rangle$. Find input and output bases which give rise to a different matrix representation of A.

Exercise 2.3: (Matrix representation for operator products) Suppose A is a linear operator from vector space V to vector space W, and B is a linear operator from vector space W to vector space X. Let $|v_i\rangle, |w_j\rangle$, and $|x_k\rangle$ be bases for the vector spaces V, W, and X, respectively. Show that the matrix representation for the linear transformation BA is the matrix product of the matrix representations for B and A, with respect to the appropriate bases.

Exercise 2.4: (Matrix representation for identity) Show that the identity operator on a vector space V has a matrix representation which is one along the diagonal and zero everywhere else, if the matrix representation is taken with respect to the same input and output bases. This matrix is known as the identity matrix.

7.2.4 2.1.3 The Pauli matrices

Four extremely useful matrices which we shall often have occasion to use are the Pauli matrices. These are 2 by 2 matrices, which go by a variety of notations. The matrices, and their corresponding notations, are depicted in Figure 2.2. The Pauli matrices are so useful in the study of quantum computation and quantum information that we encourage you to memorize them by working through in detail the many examples and exercises based upon them in subsequent sections.

$$\sigma_0 \equiv I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \sigma_1 \equiv \sigma_x \equiv X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$
$$\sigma_2 \equiv \sigma_y \equiv Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \sigma_3 \equiv \sigma_z \equiv Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Figure 2.2. The Pauli matrices. Sometimes I is omitted from the list with just X, Y and Z known as the Pauli matrices.

7.2.5 2.1.4 Inner products

An inner product is a function which takes as input two vectors $|v\rangle$ and $|w\rangle$ from a vector space and produces a complex number as output. For the time being, it will be convenient to write the inner product of $|v\rangle$ and $|w\rangle$ as $(\ |v\rangle, |w\rangle\ )$. This is not the standard quantum mechanical notation; for pedagogical clarity the $(\ \cdot, \cdot\ )$ notation will be useful occasionally in this chapter. The standard quantum mechanical notation for the inner product $(|v\rangle, |w\rangle)$ is $\langle v \mid w\rangle$, where $|v\rangle$ and $|w\rangle$ are vectors in the inner product space, and the notation $\langle v|$ is used for the dual vector to the vector $|v\rangle$; the dual is a linear operator from the inner product space V to the complex numbers $\mathbf{C}$, defined by $\langle v|(|w\rangle) \equiv \langle v \mid w\rangle \equiv (|v\rangle, |w\rangle)$. We will see shortly that the matrix representation of dual vectors is just a row vector.

A function $(\ \cdot, \cdot\ )$ from $V \times V$ to $\mathbf{C}$ is an inner product if it satisfies the requirements that: (1) $(\cdot, \cdot)$ is linear in the second argument,

$$\left(|v\rangle, \sum_i \lambda_i |w_i\rangle\right) = \sum_i \lambda_i \left(|v\rangle, |w_i\rangle\right). \tag{2.13}$$

(2) $(|v\rangle, |w\rangle) = (|w\rangle, |v\rangle)^*$.
(3) $(|v\rangle, |v\rangle) \geq 0$ with equality if and only if $|v\rangle = 0$.

For example, $\mathbf{C}^n$ has an inner product defined by

$$((y_1, \ldots, y_n), (z_1, \ldots, z_n)) \equiv \sum_i y_i^* z_i = [y_1^* \ldots y_n^*] \begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix}. \tag{2.14}$$

We call a vector space equipped with an inner product an inner product space.
Exercise 2.5: Verify that $(\ \cdot, \cdot\ )$ just defined is an inner product on $\mathbf{C}^n$.
Exercise 2.6: Show that any inner product $(\ \cdot, \cdot\ )$ is conjugate-linear in the first argument,

$$\left(\sum_i \lambda_i |w_i\rangle, |v\rangle\right) = \sum_i \lambda_i^* \left(|w_i\rangle, |v\rangle\right). \tag{2.15}$$

Discussions of quantum mechanics often refer to Hilbert space. In the finite dimensional complex vector spaces that come up in quantum computation and quantum information, a Hilbert space is exactly the same thing as an inner product space. From now on we use the two terms interchangeably, preferring the term Hilbert space. In infinite dimensions Hilbert spaces satisfy additional technical restrictions above and beyond inner product spaces, which we will not need to worry about.

Vectors $|w\rangle$ and $|v\rangle$ are orthogonal if their inner product is zero. For example, $|w\rangle \equiv (1, 0)$ and $|v\rangle \equiv (0, 1)$ are orthogonal with respect to the inner product defined by (2.14). We define the norm of a vector $|v\rangle$ by

$$\||v\rangle\| \equiv \sqrt{\langle v \mid v\rangle} \tag{2.16}$$

A unit vector is a vector $|v\rangle$ such that $\||v\rangle\| = 1$. We also say that $|v\rangle$ is normalized if $\||v\rangle\| = 1$. It is convenient to talk of normalizing a vector by dividing by its norm; thus $|v\rangle / \||v\rangle\|$ is the normalized form of $|v\rangle$, for any non-zero vector $|v\rangle$. A set $|i\rangle$ of vectors with index i is orthonormal if each vector is a unit vector, and distinct vectors in the set are orthogonal, that is, $\langle i \mid j\rangle = \delta_{ij}$, where i and j are both chosen from the index set.

Exercise 2.7: Verify that $|w\rangle \equiv (1, 1)$ and $|v\rangle \equiv (1, -1)$ are orthogonal. What are the normalized forms of these vectors?

Suppose $|w_1\rangle, \ldots, |w_d\rangle$ is a basis set for some vector space V with an inner product. There is a useful method, the Gram-Schmidt procedure, which can be used to produce an orthonormal

basis set $|v_1\rangle, \ldots, |v_d\rangle$ for the vector space V. Define $|v_1\rangle \equiv |w_1\rangle / \| |w_1\rangle \|$, and for $1 \leq k \leq d-1$ define $|v_{k+1}\rangle$ inductively by

$$|v_{k+1}\rangle \equiv \frac{|w_{k+1}\rangle - \sum_{i=1}^{k} \langle v_i \mid w_{k+1}\rangle |v_i\rangle}{\| |w_{k+1}\rangle - \sum_{i=1}^{k} \langle v_i \mid w_{k+1}\rangle |v_i\rangle \|} \tag{2.17}$$

It is not difficult to verify that the vectors $|v_1\rangle, \ldots, |v_d\rangle$ form an orthonormal set which is also a basis for V. Thus, any finite dimensional vector space of dimension d has an orthonormal basis, $|v_1\rangle, \ldots, |v_d\rangle$.

Exercise 2.8: Prove that the Gram-Schmidt procedure produces an orthonormal basis for V.

From now on, when we speak of a matrix representation for a linear operator, we mean a matrix representation with respect to orthonormal input and output bases. We also use the convention that if the input and output spaces for a linear operator are the same, then the input and output bases are the same, unless noted otherwise.

With these conventions, the inner product on a Hilbert space can be given a convenient matrix representation. Let $|w\rangle = \sum_i w_i |i\rangle$ and $|v\rangle = \sum_j v_j |j\rangle$ be representations of vectors $|w\rangle$ and $|v\rangle$ with respect to some orthonormal basis $|i\rangle$. Then, since $\langle i \mid j\rangle = \delta_{ij}$,

$$\langle v \mid w\rangle = \left(\sum_i v_i |i\rangle, \sum_j w_j |j\rangle \right) = \sum_{ij} v_i^* w_j \delta_{ij} = \sum_i v_i^* w_i \tag{2.18}$$

$$= [v_1^* \ldots v_n^*] \begin{bmatrix} w_1 \\ \vdots \\ w_n \end{bmatrix}. \tag{2.19}$$

That is, the inner product of two vectors is equal to the vector inner product between two matrix representations of those vectors, provided the representations are written with respect to the same orthonormal basis. We also see that the dual vector $\langle v|$ has a nice interpretation as the row vector whose components are complex conjugates of the corresponding components of the column vector representation of $|v\rangle$.

There is a useful way of representing linear operators which makes use of the inner product, known as the outer product representation. Suppose $|v\rangle$ is a vector in an inner product space V, and $|w\rangle$ is a vector in an inner product space W. Define $|w\rangle\langle v|$ to be the linear operator from V to W whose action is defined by

$$(|w\rangle\langle v|)\,(|v'\rangle) \equiv |w\rangle \langle v \mid v'\rangle = \langle v \mid v'\rangle\, |w\rangle \tag{2.20}$$

This equation fits beautifully into our notational conventions, according to which the expression $|w\rangle \langle v \mid v'\rangle$ could potentially have one of two meanings: we will use it to denote the result when the operator $|w\rangle\langle v|$ acts on $|v'\rangle$, and it has an existing interpretation as the result of multiplying $|w\rangle$ by the complex number $\langle v \mid v'\rangle$. Our definitions are chosen so that these two potential meanings coincide. Indeed, we define the former in terms of the latter!

We can take linear combinations of outer product operators $|w\rangle\langle v|$ in the obvious way. By definition $\sum_i a_i |w_i\rangle \langle v_i|$ is the linear operator which, when acting on $|v'\rangle$, produces $\sum_i a_i |w_i\rangle \langle v_i \mid v'\rangle$ as output.

The usefulness of the outer product notation can be discerned from an important result known as the completeness relation for orthonormal vectors. Let $|i\rangle$ be any orthonormal basis for the vector space V, so an arbitrary vector $|v\rangle$ can be written $|v\rangle = \sum_i v_i |i\rangle$ for some set of complex numbers v_i. Note that $\langle i \mid v\rangle = v_i$ and therefore

$$\left(\sum_i |i\rangle\langle i| \right) |v\rangle = \sum_i |i\rangle\langle i \mid v\rangle = \sum_i v_i |i\rangle = |v\rangle. \tag{2.21}$$

Since the last equation is true for all $|v\rangle$ it follows that

$$\sum_i |i\rangle\langle i| = I. \tag{2.22}$$

This equation is known as the completeness relation. One application of the completeness relation is to give a means for representing any operator in the outer product notation. Suppose $A : V \rightarrow W$ is a linear operator, $|v_i\rangle$ is an orthonormal basis for V, and $|w_j\rangle$ an orthonormal basis for W. Using the completeness relation twice we obtain

$$A = I_W A I_V \tag{2.23}$$

$$= \sum_{ij} |w_j\rangle \langle w_j| A |v_i\rangle \langle v_i| \tag{2.24}$$

$$= \sum_{ij} \langle w_j| A |v_i\rangle |w_j\rangle \langle v_i| \tag{2.25}$$

which is the outer product representation for A. We also see from this equation that A has matrix element $\langle w_j| A |v_i\rangle$ in the i th column and j th row, with respect to the input basis $|v_i\rangle$ and output basis $|w_j\rangle$.

A second application illustrating the usefulness of the completeness relation is the Cauchy-Schwarz inequality. This important result is discussed in Box 2.1, on this page.

Exercise 2.9: (Pauli operators and the outer product) The Pauli matrices (Figure 2.2 on page 65) can be considered as operators with respect to an orthonormal basis $|0\rangle, |1\rangle$ for a two-dimensional Hilbert space. Express each of the Pauli operators in the outer product notation.

Exercise 2.10: Suppose $|v_i\rangle$ is an orthonormal basis for an inner product space V. What is the matrix representation for the operator $|v_j\rangle \langle v_k|$, with respect to the $|v_i\rangle$ basis?

Box 2.1: The Cauchy-Schwarz inequality

The Cauchy-Schwarz inequality is an important geometric fact about Hilbert spaces. It states that for any two vectors $|v\rangle$ and $|w\rangle, |\langle v \mid w\rangle|^2 \leq \langle v \mid v\rangle\langle w \mid w\rangle$. To see this, use the Gram-Schmidt procedure to construct an orthonormal basis $|i\rangle$ for the vector space such that the first member of the basis $|i\rangle$ is $|w\rangle / \sqrt{\langle w \mid w\rangle}$. Using the completeness relation $\sum_i |i\rangle\langle i| = I$, and dropping some non-negative terms gives

$$\langle v \mid v\rangle\langle w \mid w\rangle = \sum_i \langle v \mid i\rangle\langle i \mid v\rangle\langle w \mid w\rangle \tag{2.26}$$

$$\geq \frac{\langle v \mid w\rangle\langle w \mid v\rangle}{\langle w \mid w\rangle} \langle w \mid w\rangle \tag{2.27}$$

$$= \langle v \mid w\rangle\langle w \mid v\rangle = |\langle v \mid w\rangle|^2 \tag{2.28}$$

as required. A little thought shows that equality occurs if and only if $|v\rangle$ and $|w\rangle$ are linearly related, $|v\rangle = z|w\rangle$ or $|w\rangle = z|v\rangle$, for some scalar z.

7.2.6 2.1.5 Eigenvectors and eigenvalues

An eigenvector of a linear operator A on a vector space is a non-zero vector $|v\rangle$ such that $A|v\rangle = v|v\rangle$, where v is a complex number known as the eigenvalue of A corresponding to $|v\rangle$. It will often be convenient to use the notation v both as a label for the eigenvector, and to represent the eigenvalue. We assume that you are familiar with the elementary properties of eigenvalues and eigenvectors - in particular, how to find them, via the characteristic equation. The characteristic function is defined to be $c(\lambda) \equiv \det |A - \lambda I|$,
where det is the determinant function for matrices; it can be shown that the characteristic function depends only upon the operator A, and not on the specific matrix representation used for A. The solutions of the characteristic equation $c(\lambda) = 0$ are the eigenvalues of the operator A. By the fundamental theorem of algebra, every polynomial has at least one complex root, so every operator A has at least one eigenvalue, and a corresponding eigenvector. The eigenspace corresponding to an eigenvalue v is the set of vectors which have eigenvalue v. It is a vector subspace of the vector space on which A acts.

A diagonal representation for an operator A on a vector space V is a representation $A = \sum_i \lambda_i |i\rangle\langle i|$, where the vectors $|i\rangle$ form an orthonormal set of eigenvectors for A, with corresponding eigenvalues λ_i. An operator is said to be diagonalizable if it has a diagonal representation. In the next section we will find a simple set of necessary and sufficient conditions for an operator on a Hilbert space to be diagonalizable. As an example of a diagonal representation, note that the Pauli Z matrix may be written

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1|, \tag{2.29}$$

where the matrix representation is with respect to orthonormal vectors $|0\rangle$ and $|1\rangle$, respectively. Diagonal representations are sometimes also known as orthonormal decompositions.

When an eigenspace is more than one dimensional we say that it is degenerate. For example, the matrix A defined by

$$A \equiv \begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 0 \end{bmatrix} \tag{2.30}$$

has a two-dimensional eigenspace corresponding to the eigenvalue 2 . The eigenvectors ($1, 0, 0$) and ($0, 1, 0$) are said to be degenerate because they are linearly independent eigenvectors of A with the same eigenvalue.

Exercise 2.11: (Eigendecomposition of the Pauli matrices) Find the eigenvectors, eigenvalues, and diagonal representations of the Pauli matrices X, Y, and Z.

Exercise 2.12: Prove that the matrix

$$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \tag{2.31}$$

is not diagonalizable.

7.2.7 2.1.6 Adjoints and Hermitian operators

Suppose A is any linear operator on a Hilbert space, V. It turns out that there exists a unique linear operator $A^\dagger$ on V such that for all vectors $|v\rangle, |w\rangle \in V$,

$$(|v\rangle, A|w\rangle) = \left(A^\dagger|v\rangle, |w\rangle\right) \tag{2.32}$$

This linear operator is known as the adjoint or Hermitian conjugate of the operator A. From the definition it is easy to see that $(AB)^\dagger = B^\dagger A^\dagger$. By convention, if $|v\rangle$ is a vector, then we define $|v\rangle^\dagger \equiv \langle v|$. With this definition it is not difficult to see that $(A|v\rangle)^\dagger = \langle v|A^\dagger$.

Exercise 2.13: If $|w\rangle$ and $|v\rangle$ are any two vectors, show that $(|w\rangle\langle v|)^\dagger = |v\rangle\langle w|$.

Exercise 2.14: (Anti-linearity of the adjoint) Show that the adjoint operation is anti-linear,

$$\left(\sum_i a_i A_i\right)^\dagger = \sum_i a_i^* A_i^\dagger. \tag{2.33}$$

Exercise 2.15: Show that $\left(A^\dagger\right)^\dagger = A$.

In a matrix representation of an operator A, the action of the Hermitian conjugation operation is to take the matrix of A to the conjugate-transpose matrix, $A^\dagger \equiv (A^*)^T$, where the $*$ indicates complex conjugation, and T indicates the transpose operation. For example, we have

$$\begin{bmatrix} 1+3i & 2i \\ 1+i & 1-4i \end{bmatrix}^\dagger = \begin{bmatrix} 1-3i & 1-i \\ -2i & 1+4i \end{bmatrix} \tag{2.34}$$

An operator A whose adjoint is A is known as a Hermitian or self-adjoint operator. An important class of Hermitian operators is the projectors. Suppose W is a k-dimensional vector subspace of the d-dimensional vector space V. Using the GramSchmidt procedure it is possible to construct an orthonormal basis $|1\rangle, \ldots, |d\rangle$ for V such that $|1\rangle, \ldots, |k\rangle$ is an orthonormal basis for W. By definition,

$$P \equiv \sum_{i=1}^{k} |i\rangle\langle i| \tag{2.35}$$

is the projector onto the subspace W. It is easy to check that this definition is independent of the orthonormal basis $|1\rangle, \ldots, |k\rangle$ used for W. From the definition it can be shown that $|v\rangle\langle v|$ is Hermitian for any vector $|v\rangle$, so P is Hermitian, $P^\dagger = P$. We will often refer to the 'vector space' P, as shorthand for the vector space onto which P is a projector. The orthogonal complement of P is the operator $Q \equiv I - P$. It is easy to see that Q is a projector onto the vector space spanned by $|k+1\rangle, \ldots, |d\rangle$, which we also refer to as the orthogonal complement of P, and may denote by Q.

Exercise 2.16: Show that any projector P satisfies the equation $P^2 = P$.

An operator A is said to be normal if $AA^\dagger = A^\dagger A$. Clearly, an operator which is Hermitian is also normal. There is a remarkable representation theorem for normal operators known as the spectral decomposition, which states that an operator is a normal operator if and only if it is diagonalizable. This result is proved in Box 2.2 on page 72, which you should read closely.

Exercise 2.17: Show that a normal matrix is Hermitian if and only if it has real eigenvalues.

A matrix U is said to be unitary if $U^\dagger U = I$. Similarly an operator U is unitary if $U^\dagger U = I$. It is easily checked that an operator is unitary if and only if each of its matrix representations is unitary. A unitary operator also satisfies $UU^\dagger = I$, and therefore U is normal and has a spectral decomposition. Geometrically, unitary operators are important because they preserve inner products between vectors. To see this, let $|v\rangle$ and $|w\rangle$ be any
two vectors. Then the inner product of $U|v\rangle$ and $U|w\rangle$ is the same as the inner product of $|v\rangle$ and $|w\rangle$,

$$(U|v\rangle, U|w\rangle) = \langle v|U^\dagger U|w\rangle = \langle v|I|w\rangle = \langle v \mid w\rangle. \tag{2.36}$$

This result suggests the following elegant outer product representation of any unitary U. Let $|v_i\rangle$ be any orthonormal basis set. Define $|w_i\rangle \equiv U\,|v_i\rangle$, so $|w_i\rangle$ is also an orthonormal basis set, since unitary operators preserve inner products. Note that $U = \sum_i |w_i\rangle\,\langle v_i|$. Conversely,

if $|v_i\rangle$ and $|w_i\rangle$ are any two orthonormal bases, then it is easily checked that the operator U defined by $U \equiv \sum_i |w_i\rangle \langle v_i|$ is a unitary operator.

Exercise 2.18: Show that all eigenvalues of a unitary matrix have modulus 1 , that is, can be written in the form $e^{i\theta}$ for some real θ.

Exercise 2.19: (Pauli matrices: Hermitian and unitary) Show that the Pauli matrices are Hermitian and unitary.

Exercise 2.20: (Basis changes) Suppose A' and A'' are matrix representations of an operator A on a vector space V with respect to two different orthonormal bases, $|v_i\rangle$ and $|w_i\rangle$. Then the elements of A' and A'' are $A'_{ij} = \langle v_i| A |v_j\rangle$ and $A''_{ij} = \langle w_i| A |w_j\rangle$. Characterize the relationship between A' and A''.

A special subclass of Hermitian operators is extremely important. This is the positive operators. A positive operator A is defined to be an operator such that for any vector $|v\rangle$, $(|v\rangle, A|v\rangle)$ is a real, non-negative number. If $(|v\rangle, A|v\rangle)$ is strictly greater than zero for all $|v\rangle \neq 0$ then we say that A is positive definite. In Exercise 2.24 on this page you will show that any positive operator is automatically Hermitian, and therefore by the spectral decomposition has diagonal representation $\sum_i \lambda_i |i\rangle\langle i|$, with non-negative eigenvalues λ_i.

Exercise 2.21: Repeat the proof of the spectral decomposition in Box 2.2 for the case when M is Hermitian, simplifying the proof wherever possible.

Exercise 2.22: Prove that two eigenvectors of a Hermitian operator with different eigenvalues are necessarily orthogonal.

Exercise 2.23: Show that the eigenvalues of a projector P are all either 0 or 1 .

Exercise 2.24: (Hermiticity of positive operators) Show that a positive operator is necessarily Hermitian. (Hint: Show that an arbitrary operator A can be written $A = B + iC$ where B and C are Hermitian.)

Exercise 2.25: Show that for any operator $A, A^\dagger A$ is positive.

7.2.8 2.1.7 Tensor products

The tensor product is a way of putting vector spaces together to form larger vector spaces. This construction is crucial to understanding the quantum mechanics of multiparticle systems. The following discussion is a little abstract, and may be difficult to follow if you're not already familiar with the tensor product, so feel free to skip ahead now and revisit later when you come to the discussion of tensor products in quantum mechanics.

Suppose V and W are vector spaces of dimension m and n respectively. For convenience we also suppose that V and W are Hilbert spaces. Then $V \otimes W$ (read ' V tensor

Box 2.2: The spectral decomposition - important!

The spectral decomposition is an extremely useful representation theorem for normal operators.

Theorem 2.1: (Spectral decomposition) Any normal operator M on a vector space V is diagonal with respect to some orthonormal basis for V. Conversely, any diagonalizable operator is normal.

Proof

The converse is a simple exercise, so we prove merely the forward implication, by induction on the dimension d of V. The case $d = 1$ is trivial. Let λ be an eigenvalue of M, P the projector onto the λ eigenspace, and Q the projector onto the orthogonal complement. Then $M = (P+Q)M(P+Q) = PMP+QMP+PMQ+QMQ$. Obviously $PMP = \lambda P$. Furthermore, $QMP = 0$, as M takes the subspace P into itself. We claim that $PMQ = 0$ also. To see this,

let $|v\rangle$ be an element of the subspace P. Then $MM^\dagger|v\rangle = M^\dagger M|v\rangle = \lambda M^\dagger|v\rangle$. Thus, $M^\dagger|v\rangle$ has eigenvalue λ and therefore is an element of the subspace P. It follows that $QM^\dagger P = 0$. Taking the adjoint of this equation gives $PMQ = 0$. Thus $M = PMP + QMQ$. Next, we prove that QMQ is normal. To see this, note that $QM = QM(P+Q) = QMQ$, and $QM^\dagger = QM^\dagger(P+Q) = QM^\dagger Q$. Therefore, by the normality of M, and the observation that $Q^2 = Q$,

$$\begin{aligned} QMQQM^\dagger Q &= QMQM^\dagger Q && (2.37)\\ &= QMM^\dagger Q && (2.38)\\ &= QM^\dagger MQ && (2.39)\\ &= QM^\dagger QMQ && (2.40)\\ &= QM^\dagger QQMQ, && (2.41) \end{aligned}$$

so QMQ is normal. By induction, QMQ is diagonal with respect to some orthonormal basis for the subspace Q, and PMP is already diagonal with respect to some orthonormal basis for P. It follows that $M = PMP + QMQ$ is diagonal with respect to some orthonormal basis for the total vector space.

In terms of the outer product representation, this means that M can be written as $M = \sum_i \lambda_i |i\rangle\langle i|$, where λ_i are the eigenvalues of M, $|i\rangle$ is an orthonormal basis for V, and each $|i\rangle$ an eigenvector of M with eigenvalue λ_i. In terms of projectors, $M = \sum_i \lambda_i P_i$, where λ_i are again the eigenvalues of M, and P_i is the projector onto the λ_i eigenspace of M. These projectors satisfy the completeness relation $\sum_i P_i = I$, and the orthonormality relation $P_i P_j = \delta_{ij} P_i$.
W') is an mn dimensional vector space. The elements of $V \otimes W$ are linear combinations of 'tensor products' $|v\rangle \otimes |w\rangle$ of elements $|v\rangle$ of V and $|w\rangle$ of W. In particular, if $|i\rangle$ and $|j\rangle$ are orthonormal bases for the spaces V and W then $|i\rangle \otimes |j\rangle$ is a basis for $V \otimes W$. We often use the abbreviated notations $|v\rangle|w\rangle, |v, w\rangle$ or even $|vw\rangle$ for the tensor product
$|v\rangle \otimes |w\rangle$. For example, if V is a two-dimensional vector space with basis vectors $|0\rangle$ and $|1\rangle$ then $|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle$ is an element of $V \otimes V$.

By definition the tensor product satisfies the following basic properties:
(1) For an arbitrary scalar z and elements $|v\rangle$ of V and $|w\rangle$ of W,

$$z(|v\rangle \otimes |w\rangle) = (z|v\rangle) \otimes |w\rangle = |v\rangle \otimes (z|w\rangle) \tag{2.42}$$

(2) For arbitrary $|v_1\rangle$ and $|v_2\rangle$ in V and $|w\rangle$ in W,

$$(|v_1\rangle + |v_2\rangle) \otimes |w\rangle = |v_1\rangle \otimes |w\rangle + |v_2\rangle \otimes |w\rangle. \tag{2.43}$$

(3) For arbitrary $|v\rangle$ in V and $|w_1\rangle$ and $|w_2\rangle$ in W,

$$|v\rangle \otimes (|w_1\rangle + |w_2\rangle) = |v\rangle \otimes |w_1\rangle + |v\rangle \otimes |w_2\rangle\,. \tag{2.44}$$

What sorts of linear operators act on the space $V \otimes W$? Suppose $|v\rangle$ and $|w\rangle$ are vectors in V and W, and A and B are linear operators on V and W, respectively. Then we can define a linear operator $A \otimes B$ on $V \otimes W$ by the equation

$$(A \otimes B)(|v\rangle \otimes |w\rangle) \equiv A|v\rangle \otimes B|w\rangle. \tag{2.45}$$

The definition of $A \otimes B$ is then extended to all elements of $V \otimes W$ in the natural way to ensure linearity of $A \otimes B$, that is,

$$(A \otimes B) \left(\sum_i a_i \left| v_i \right\rangle \otimes \left| w_i \right\rangle \right) \equiv \sum_i a_i A \left| v_i \right\rangle \otimes B \left| w_i \right\rangle . \tag{2.46}$$

It can be shown that $A \otimes B$ defined in this way is a well-defined linear operator on $V \otimes W$. This notion of the tensor product of two operators extends in the obvious way to the case where $A : V \to V'$ and $B : W \to W'$ map between different vector spaces. Indeed, an arbitrary linear operator C mapping $V \otimes W$ to $V' \otimes W'$ can be represented as a linear combination of tensor products of operators mapping V to V' and W to W',

$$C = \sum_i c_i A_i \otimes B_i \tag{2.47}$$

where by definition

$$\left(\sum_i c_i A_i \otimes B_i \right) \left| v \right\rangle \otimes \left| w \right\rangle \equiv \sum_i c_i A_i \left| v \right\rangle \otimes B_i \left| w \right\rangle . \tag{2.48}$$

The inner products on the spaces V and W can be used to define a natural inner product on $V \otimes W$. Define

$$\left(\sum_i a_i \left| v_i \right\rangle \otimes \left| w_i \right\rangle , \sum_j b_j \left| v'_j \right\rangle \otimes \left| w'_j \right\rangle \right) \equiv \sum_{ij} a_i^* b_j \left\langle v_i \mid v'_j \right\rangle \left\langle w_i \mid w'_j \right\rangle . \tag{2.49}$$

It can be shown that the function so defined is a well-defined inner product. From this inner product, the inner product space $V \otimes W$ inherits the other structure we are familiar with, such as notions of an adjoint, unitarity, normality, and Hermiticity.

All this discussion is rather abstract. It can be made much more concrete by moving to a convenient matrix representation known as the Kronecker product. Suppose A is an m by n matrix, and B is a p by q matrix. Then we have the matrix representation:

$$A \otimes B \equiv \overbrace{\begin{bmatrix} A_{11}B & A_{12}B & \dots & A_{1n}B \\ A_{21}B & A_{22}B & \dots & A_{2n}B \\ \vdots & \vdots & \vdots & \vdots \\ A_{m1}B & A_{m2}B & \dots & A_{mn}B \end{bmatrix}}^{nq} mp. \tag{2.50}$$

In this representation terms like $A_{11}B$ denote p by q submatrices whose entries are proportional to B, with overall proportionality constant A_{11}. For example, the tensor product of the vectors $(1, 2)$ and $(2, 3)$ is the vector

$$\begin{bmatrix} 1 \\ 2 \end{bmatrix} \otimes \begin{bmatrix} 2 \\ 3 \end{bmatrix} = \begin{bmatrix} 1 \times 2 \\ 1 \times 3 \\ 2 \times 2 \\ 2 \times 3 \end{bmatrix} = \begin{bmatrix} 2 \\ 3 \\ 4 \\ 6 \end{bmatrix} . \tag{2.51}$$

The tensor product of the Pauli matrices X and Y is

$$X \otimes Y = \begin{bmatrix} 0 \cdot Y & 1 \cdot Y \\ 1 \cdot Y & 0 \cdot Y \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \\ 0 & -i & 0 & 0 \\ i & 0 & 0 & 0 \end{bmatrix} . \tag{2.52}$$

Finally, we mention the useful notation $|\psi\rangle^{\otimes k}$, which means $|\psi\rangle$ tensored with itself k times. For example $|\psi\rangle^{\otimes 2} = |\psi\rangle \otimes |\psi\rangle$. An analogous notation is also used for operators on tensor product spaces.

Exercise 2.26: Let $|\psi\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. Write out $|\psi\rangle^{\otimes 2}$ and $|\psi\rangle^{\otimes 3}$ explicitly, both in terms of tensor products like $|0\rangle|1\rangle$, and using the Kronecker product.

Exercise 2.27: Calculate the matrix representation of the tensor products of the Pauli operators (a) X and Z; (b) I and X; (c) X and I. Is the tensor product commutative?

Exercise 2.28: Show that the transpose, complex conjugation, and adjoint operations distribute over the tensor product,

$$(A \otimes B)^* = A^* \otimes B^*; (A \otimes B)^T = A^T \otimes B^T; (A \otimes B)^\dagger = A^\dagger \otimes B^\dagger. \tag{2.53}$$

Exercise 2.29: Show that the tensor product of two unitary operators is unitary.

Exercise 2.30: Show that the tensor product of two Hermitian operators is Hermitian.

Exercise 2.31: Show that the tensor product of two positive operators is positive.

Exercise 2.32: Show that the tensor product of two projectors is a projector.

Exercise 2.33: The Hadamard operator on one qubit may be written as

$$H = \frac{1}{\sqrt{2}}[(|0\rangle + |1\rangle)\langle 0| + (|0\rangle - |1\rangle)\langle 1|] \tag{2.54}$$

Show explicitly that the Hadamard transform on n qubits, $H^{\otimes n}$, may be written as

$$H^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x,y} (-1)^{x \cdot y} |x\rangle\langle y|. \tag{2.55}$$

Write out an explicit matrix representation for $H^{\otimes 2}$.

7.2.9 2.1.8 Operator functions

There are many important functions which can be defined for operators and matrices. Generally speaking, given a function f from the complex numbers to the complex numbers, it is possible to define a corresponding matrix function on normal matrices (or some subclass, such as the Hermitian matrices) by the following construction. Let $A = \sum_a a|a\rangle\langle a|$ be a spectral decomposition for a normal operator A. Define $f(A) \equiv \sum_a f(a)|a\rangle\langle a|$. A little thought shows that $f(A)$ is uniquely defined. This procedure can be used, for example, to define the square root of a positive operator, the logarithm of a positive-definite operator, or the exponential of a normal operator. As an example,

$$\exp(\theta Z) = \begin{bmatrix} e^\theta & 0 \\ 0 & e^{-\theta} \end{bmatrix} \tag{2.56}$$

since Z has eigenvectors $|0\rangle$ and $|1\rangle$.

Exercise 2.34: Find the square root and logarithm of the matrix

$$\begin{bmatrix} 4 & 3 \\ 3 & 4 \end{bmatrix}. \tag{2.57}$$

Exercise 2.35: (Exponential of the Pauli matrices) Let $\vec{v}$ be any real, three-dimensional unit vector and θ a real number. Prove that

$$\exp(i\theta \vec{v} \cdot \vec{\sigma}) = \cos(\theta) I + i \sin(\theta) \vec{v} \cdot \vec{\sigma} \tag{2.58}$$

where $\vec{v} \cdot \vec{\sigma} \equiv \sum_{i=1}^{3} v_i \sigma_i$. This exercise is generalized in Problem 2.1 on page 117.
Another important matrix function is the trace of a matrix. The trace of A is defined to be the sum of its diagonal elements,

$$\mathrm{tr}(A) \equiv \sum_i A_{ii}. \tag{2.59}$$

The trace is easily seen to be cyclic, $\mathrm{tr}(AB) = \mathrm{tr}(BA)$, and linear, $\mathrm{tr}(A+B) = \mathrm{tr}(A) + \mathrm{tr}(B), \mathrm{tr}(zA) = z\,\mathrm{tr}(A)$, where A and B are arbitrary matrices, and z is a complex number. Furthermore, from the cyclic property it follows that the trace of a matrix is invariant under the unitary similarity transformation $A \rightarrow UAU^\dagger$, as $\mathrm{tr}\left(UAU^\dagger\right) = \mathrm{tr}\left(U^\dagger UA\right) = \mathrm{tr}(A)$. In light of this result, it makes sense to define the trace of an operator A to be the trace of any matrix representation of A. The invariance of the trace under unitary similarity transformations ensures that the trace of an operator is well defined.

As an example of the trace, suppose $|\psi\rangle$ is a unit vector and A is an arbitrary operator. To evaluate $\mathrm{tr}(A|\psi\rangle\langle\psi|)$ use the Gram-Schmidt procedure to extend $|\psi\rangle$ to an orthonormal basis $|i\rangle$ which includes $|\psi\rangle$ as the first element. Then we have

$$\mathrm{tr}(A|\psi\rangle\langle\psi|) = \sum_i \langle i|A|\psi\rangle\langle\psi \mid i\rangle \tag{2.60}$$

$$= \langle\psi|A|\psi\rangle \tag{2.61}$$

This result, that $\mathrm{tr}(A|\psi\rangle\langle\psi|) = \langle\psi|A|\psi\rangle$ is extremely useful in evaluating the trace of an operator.

Exercise 2.36: Show that the Pauli matrices except for I have trace zero.
Exercise 2.37: (Cyclic property of the trace) If A and B are two linear operators show that

$$\mathrm{tr}(AB) = \mathrm{tr}(BA) \tag{2.62}$$

Exercise 2.38: (Linearity of the trace) If A and B are two linear operators, show that

$$\mathrm{tr}(A+B) = \mathrm{tr}(A) + \mathrm{tr}(B) \tag{2.63}$$

and if z is an arbitrary complex number show that

$$\mathrm{tr}(zA) = z\,\mathrm{tr}(A) \tag{2.64}$$

Exercise 2.39: (The Hilbert-Schmidt inner product on operators) The set L_V of linear operators on a Hilbert space V is obviously a vector space - the sum of two linear operators is a linear operator, zA is a linear operator if A is a linear operator and z is a complex number, and there is a zero element 0 . An important additional result is that the vector space L_V can be given a natural inner product structure, turning it into a Hilbert space.
(1) Show that the function $(\cdot,\cdot)$ on $L_V \times L_V$ defined by

$$(A,B) \equiv \mathrm{tr}\left(A^\dagger B\right) \tag{2.65}$$

is an inner product function. This inner product is known as the Hilbert-Schmidt or trace inner product.
(2) If V has d dimensions show that L_V has dimension d^2.
(3) Find an orthonormal basis of Hermitian matrices for the Hilbert space L_V.

7.2.10 2.1.9 The commutator and anti-commutator

The commutator between two operators A and B is defined to be

$$[A, B] \equiv AB - BA \tag{2.66}$$

If $[A, B] = 0$, that is, $AB = BA$, then we say A commutes with B. Similarly, the anti-commutator of two operators A and B is defined by

$$\{A, B\} \equiv AB + BA; \tag{2.67}$$

we say A anti-commutes with B if $\{A, B\} = 0$. It turns out that many important properties of pairs of operators can be deduced from their commutator and anti-commutator. Perhaps the most useful relation is the following connection between the commutator and the property of being able to simultaneously diagonalize Hermitian operators A and B,
that is, write $A = \sum_i a_i |i\rangle\langle i|, B = \sum_i b_i |i\rangle\langle i|$, where $|i\rangle$ is some common orthonormal set of eigenvectors for A and B.

Theorem 2.2: (Simultaneous diagonalization theorem) Suppose A and B are Hermitian operators. Then $[A, B] = 0$ if and only if there exists an orthonormal basis such that both A and B are diagonal with respect to that basis. We say that A and B are simultaneously diagonalizable in this case.

This result connects the commutator of two operators, which is often easy to compute, to the property of being simultaneously diagonalizable, which is a priori rather difficult to determine. As an example, consider that

$$[X, Y] = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} - \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{2.68}$$

$$= 2i \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{2.69}$$

$$= 2iZ \tag{2.70}$$

so X and Y do not commute. You have already shown, in Exercise 2.11, that X and Y do not have common eigenvectors, as we expect from the simultaneous diagonalization theorem.

Proof

You can (and should!) easily verify that if A and B are diagonal in the same orthonormal basis then $[A, B] = 0$. To show the converse, let $|a, j\rangle$ be an orthonormal basis for the eigenspace V_a of A with eigenvalue a; the index j is used to label possible degeneracies. Note that

$$AB|a, j\rangle = BA|a, j\rangle = aB|a, j\rangle \tag{2.71}$$

and therefore $B|a, j\rangle$ is an element of the eigenspace V_a. Let P_a denote the projector onto the space V_a and define $B_a \equiv P_a B P_a$. It is easy to see that the restriction of B_a to the space V_a is Hermitian on V_a, and therefore has a spectral decomposition in terms of an orthonormal set of eigenvectors which span the space V_a. Let's call these eigenvectors $|a, b, k\rangle$, where the indices a and b label the eigenvalues of A and B_a, and k is an extra index to allow for the possibility of a degenerate B_a. Note that $B|a, b, k\rangle$ is an element of V_a, so $B|a, b, k\rangle = P_a B|a, b, k\rangle$. Moreover we have $P_a|a, b, k\rangle = |a, b, k\rangle$, so

$$B|a, b, k\rangle = P_a B P_a|a, b, k\rangle = b|a, b, k\rangle \tag{2.72}$$

It follows that $|a,b,k\rangle$ is an eigenvector of B with eigenvalue b, and therefore $|a,b,k\rangle$ is an orthonormal set of eigenvectors of both A and B, spanning the entire vector space on which A and B are defined. That is, A and B are simultaneously diagonalizable.

Exercise 2.40: (Commutation relations for the Pauli matrices) Verify the commutation relations

$$[X,Y] = 2iZ; \quad [Y,Z] = 2iX; \quad [Z,X] = 2iY. \tag{2.73}$$

There is an elegant way of writing this using ϵ_{jkl}, the antisymmetric tensor on three indices, for which $\epsilon_{jkl} = 0$ except for $\epsilon_{123} = \epsilon_{231} = \epsilon_{312} = 1$, and $\epsilon_{321} = \epsilon_{213} = \epsilon_{132} = -1$:

$$[\sigma_j, \sigma_k] = 2i \sum_{l=1}^{3} \epsilon_{jkl} \sigma_l. \tag{2.74}$$

Exercise 2.41: (Anti-commutation relations for the Pauli matrices) Verify the anti-commutation relations

$$\{\sigma_i, \sigma_j\} = 0 \tag{2.75}$$

where $i \neq j$ are both chosen from the set $1,2,3$. Also verify that ($i = 0,1,2,3$)

$$\sigma_i^2 = I. \tag{2.76}$$

Exercise 2.42: Verify that

$$AB = \frac{[A,B] + \{A,B\}}{2}. \tag{2.77}$$

Exercise 2.43: Show that for $j,k = 1,2,3$,

$$\sigma_j \sigma_k = \delta_{jk} I + i \sum_{l=1}^{3} \epsilon_{jkl} \sigma_l \tag{2.78}$$

Exercise 2.44: Suppose $[A,B] = 0, \{A,B\} = 0$, and A is invertible. Show that B must be 0 .

Exercise 2.45: Show that $[A,B]^\dagger = \left[B^\dagger, A^\dagger\right]$.
Exercise 2.46: Show that $[A,B] = -[B,A]$.
Exercise 2.47: Suppose A and B are Hermitian. Show that $i[A,B]$ is Hermitian.

7.2.11 2.1.10 The polar and singular value decompositions

The polar and singular value decompositions are useful ways of breaking linear operators up into simpler parts. In particular, these decompositions allow us to break general linear operators up into products of unitary operators and positive operators. While we don't understand the structure of general linear operators terribly well, we do understand unitary operators and positive operators in quite some detail. The polar and singular value decompositions allow us to apply this understanding to better understand general linear operators.

Theorem 2.3: (Polar decomposition) Let A be a linear operator on a vector space V. Then there exists unitary U and positive operators J and K such that

$$A = UJ = KU, \tag{2.79}$$

where the unique positive operators J and K satisfying these equations are defined by $J \equiv \sqrt{A^\dagger A}$ and $K \equiv \sqrt{AA^\dagger}$. Moreover, if A is invertible then U is unique.

We call the expression $A = UJ$ the left polar decomposition of A, and $A = KU$ the right polar decomposition of A. Most often, we'll omit the 'right' or 'left' nomenclature, and use the term 'polar decomposition' for both expressions, with context indicating which is meant.

Proof

$J \equiv \sqrt{A^\dagger A}$ is a positive operator, so it can be given a spectral decomposition, $J = \sum_i \lambda_i |i\rangle\langle i| \, (\lambda_i \geq 0)$. Define $|\psi_i\rangle \equiv A|i\rangle$. From the definition, we see that $\langle \psi_i \mid \psi_i \rangle = \lambda_i^2$. Consider for now only those i for which $\lambda_i \neq 0$. For those i define $|e_i\rangle \equiv |\psi_i\rangle / \lambda_i$, so the $|e_i\rangle$ are normalized. Moreover, they are orthogonal, since if $i \neq j$ then $\langle e_i \mid e_j \rangle = \langle i|A^\dagger A|j\rangle / \lambda_i \lambda_j = \langle i|J^2|j\rangle / \lambda_i \lambda_j = 0$.

We have been considering i such that $\lambda_i \neq 0$. Now use the Gram-Schmidt procedure to extend the orthonormal set $|e_i\rangle$ so it forms an orthonormal basis, which we also label $|e_i\rangle$. Define a unitary operator $U \equiv \sum_i |e_i\rangle \langle i|$. When $\lambda_i \neq 0$ we have $UJ|i\rangle = \lambda_i |e_i\rangle = |\psi_i\rangle = A|i\rangle$. When $\lambda_i = 0$ we have $UJ|i\rangle = 0 = |\psi_i\rangle$. We have proved that the action of A and UJ agree on the basis $|i\rangle$, and thus that $A = UJ$.

J is unique, since multiplying $A = UJ$ on the left by the adjoint equation $A^\dagger = JU^\dagger$ gives $J^2 = A^\dagger A$, from which we see that $J = \sqrt{A^\dagger A}$, uniquely. A little thought shows that if A is invertible, then so is J, so U is uniquely determined by the equation $U = AJ^{-1}$. The proof of the right polar decomposition follows, since $A = UJ = UJU^\dagger U = KU$, where $K \equiv UJU^\dagger$ is a positive operator. Since $AA^\dagger = KUU^\dagger K = K^2$ we must have $K = \sqrt{AA^\dagger}$, as claimed.

The singular value decomposition combines the polar decomposition and the spectral theorem.

Corollary 2.4: (Singular value decomposition) Let A be a square matrix. Then there exist unitary matrices U and V, and a diagonal matrix D with non-negative entries such that

$$A = UDV \tag{2.80}$$

The diagonal elements of D are called the singular values of A.

Proof

By the polar decomposition, $A = SJ$, for unitary S, and positive J. By the spectral theorem, $J = TDT^\dagger$, for unitary T and diagonal D with non-negative entries. Setting $U \equiv ST$ and $V \equiv T^\dagger$ completes the proof.

Exercise 2.48: What is the polar decomposition of a positive matrix P ? Of a unitary matrix U ? Of a Hermitian matrix, H ?

Exercise 2.49: Express the polar decomposition of a normal matrix in the outer product representation.

Exercise 2.50: Find the left and right polar decompositions of the matrix

$$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}. \tag{2.81}$$

7.2.12 2.2 The postulates of quantum mechanics

> All understanding begins with our not accepting the world as it appears. - Alan Kay
>
> The most incomprehensible thing about the world is that it is comprehensible. - Albert Einstein

Quantum mechanics is a mathematical framework for the development of physical theories. On its own quantum mechanics doesn't tell you what laws a physical system must obey, but it does provide a mathematical and conceptual framework for the development of such laws. In the next few sections we give a complete description of the basic postulates of quantum mechanics. These postulates provide a connection between the physical world and the mathematical formalism of quantum mechanics.

The postulates of quantum mechanics were derived after a long process of trial and (mostly) error, which involved a considerable amount of guessing and fumbling by the originators of the theory. Don't be surprised if the motivation for the postulates is not always clear; even to experts the basic postulates of quantum mechanics appear surprising. What you should expect to gain in the next few sections is a good working grasp of the postulates - how to apply them, and when.

7.2.13 2.2.1 State space

The first postulate of quantum mechanics sets up the arena in which quantum mechanics takes place. The arena is our familiar friend from linear algebra, Hilbert space.

Postulate 1: Associated to any isolated physical system is a complex vector space with inner product (that is, a Hilbert space) known as the state space of the system. The system is completely described by its state vector, which is a unit vector in the system's state space.

Quantum mechanics does not tell us, for a given physical system, what the state space of that system is, nor does it tell us what the state vector of the system is. Figuring that out for a specific system is a difficult problem for which physicists have developed many intricate and beautiful rules. For example, there is the wonderful theory of quantum electrodynamics (often known as QED), which describes how atoms and light interact. One aspect of QED is that it tells us what state spaces to use to give quantum descriptions of atoms and light. We won't be much concerned with the intricacies of theories like QED (except in so far as they apply to physical realizations, in Chapter 7), as we are mostly interested in the general framework provided by quantum mechanics. For our purposes it will be sufficient to make some very simple (and reasonable) assumptions about the state spaces of the systems we are interested in, and stick with those assumptions.

The simplest quantum mechanical system, and the system which we will be most concerned with, is the qubit. A qubit has a two-dimensional state space. Suppose $|0\rangle$ and $|1\rangle$ form an orthonormal basis for that state space. Then an arbitrary state vector in the state space can be written

$$|\psi\rangle = a|0\rangle + b|1\rangle, \tag{2.82}$$

where a and b are complex numbers. The condition that $|\psi\rangle$ be a unit vector, $\langle\psi \mid \psi\rangle = 1$, is therefore equivalent to $|a|^2 + |b|^2 = 1$. The condition $\langle\psi \mid \psi\rangle = 1$ is often known as the normalization condition for state vectors.

We will take the qubit as our fundamental quantum mechanical system. Later, in Chapter 7, we will see that there are real physical systems which may be described in terms of qubits. For now, though, it is sufficient to think of qubits in abstract terms, without reference to a specific realization. Our discussions of qubits will always be referred to some orthonormal set of basis vectors, $|0\rangle$ and $|1\rangle$, which should be thought of as being fixed in advance. Intuitively, the states $|0\rangle$ and $|1\rangle$ are analogous to the two values 0 and 1 which a bit may take. The way a qubit differs from a bit is that superpositions of these two states, of the form $a|0\rangle + b|1\rangle$, can also exist, in which it is not possible to say that the qubit is definitely in the state $|0\rangle$, or definitely in the state $|1\rangle$.

We conclude with some useful terminology which is often used in connection with the description of quantum states. We say that any linear combination $\sum_i \alpha_i |\psi_i\rangle$ is a superposition of the states $|\psi_i\rangle$ with amplitude α_i for the state $|\psi_i\rangle$. So, for example, the state

$$\frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{2.83}$$

is a superposition of the states $|0\rangle$ and $|1\rangle$ with amplitude $1/\sqrt{2}$ for the state $|0\rangle$, and amplitude $-1/\sqrt{2}$ for the state $|1\rangle$.

7.2.14 2.2.2 Evolution

How does the state, $|\psi\rangle$, of a quantum mechanical system change with time? The following postulate gives a prescription for the description of such state changes.

Postulate 2: The evolution of a closed quantum system is described by a unitary transformation. That is, the state $|\psi\rangle$ of the system at time t_1 is related to the state $|\psi'\rangle$ of the system at time t_2 by a unitary operator U which depends only on the times t_1 and t_2,

$$|\psi'\rangle = U|\psi\rangle. \tag{2.84}$$

Just as quantum mechanics does not tell us the state space or quantum state of a particular quantum system, it does not tell us which unitary operators U describe realworld quantum dynamics. Quantum mechanics merely assures us that the evolution of any closed quantum system may be described in such a way. An obvious question to ask is: what unitary operators are natural to consider? In the case of single qubits, it turns out that any unitary operator at all can be realized in realistic systems.

Let's look at a few examples of unitary operators on a single qubit which are important in quantum computation and quantum information. We have already seen several examples of such unitary operators - the Pauli matrices, defined in Section 2.1.3, and the quantum gates described in Chapter 1. As remarked in Section 1.3.1, the X matrix is often known as the quantum not gate, by analogy to the classical not gate. The X and Z Pauli matrices are also sometimes referred to as the bit flip and phase flip matrices: the X matrix takes $|0\rangle$ to $|1\rangle$, and $|1\rangle$ to $|0\rangle$, thus earning the name bit flip; and the Z matrix leaves $|0\rangle$ invariant, and takes $|1\rangle$ to $-|1\rangle$, with the extra factor of -1 added known as a phase factor, thus justifying the term phase flip. We will not use the term phase flip for
Z very often, since it is easily confused with the phase gate to be defined in Chapter 4. (Section 2.2.7 contains more discussion of the many uses of the term 'phase'.)

Another interesting unitary operator is the Hadamard gate, which we denote H. This has the action $H|0\rangle \equiv (|0\rangle + |1\rangle)/\sqrt{2}, H|1\rangle \equiv (|0\rangle - |1\rangle)/\sqrt{2}$, and corresponding matrix representation

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{2.85}$$

Exercise 2.51: Verify that the Hadamard gate H is unitary.
Exercise 2.52: Verify that $H^2 = I$.
Exercise 2.53: What are the eigenvalues and eigenvectors of H ?
Postulate 2 requires that the system being described be closed. That is, it is not interacting in any way with other systems. In reality, of course, all systems (except the Universe as a whole) interact at least somewhat with other systems. Nevertheless, there are interesting systems which can be described to a good approximation as being closed, and which are described by unitary evolution to some good approximation. Furthermore, at least in principle every open system can be described as part of a larger closed system (the Universe) which is undergoing

unitary evolution. Later, we'll introduce more tools which allow us to describe systems which are not closed, but for now we'll continue with the description of the evolution of closed systems.

Postulate 2 describes how the quantum states of a closed quantum system at two different times are related. A more refined version of this postulate can be given which describes the evolution of a quantum system in continuous time. From this more refined postulate we will recover Postulate 2. Before we state the revised postulate, it is worth pointing out two things. First, a notational remark. The operator H appearing in the following discussion is not the same as the Hadamard operator, which we just introduced. Second, the following postulate makes use of the apparatus of differential equations. Readers with little background in the study of differential equations should be reassured that they will not be necessary for much of the book, with the exception of parts of Chapter 7, on real physical implementations of quantum information processing.

Postulate 2': The time evolution of the state of a closed quantum system is described by the Schrödinger equation,

$$i\hbar \frac{d|\psi\rangle}{dt} = H|\psi\rangle \tag{2.86}$$

In this equation, $\hbar$ is a physical constant known as Planck's constant whose value must be experimentally determined. The exact value is not important to us. In practice, it is common to absorb the factor $\hbar$ into H, effectively setting $\hbar = 1$.H is a fixed Hermitian operator known as the Hamiltonian of the closed system.

If we know the Hamiltonian of a system, then (together with a knowledge of $\hbar$) we understand its dynamics completely, at least in principle. In general figuring out the Hamiltonian needed to describe a particular physical system is a very difficult problem - much of twentieth century physics has been concerned with this problem - which requires substantial input from experiment in order to be answered. From our point of
view this is a problem of detail to be addressed by physical theories built within the framework of quantum mechanics - what Hamiltonian do we need to describe atoms in such-and-such a configuration - and is not a question that needs to be addressed by the theory of quantum mechanics itself. Most of the time in our discussion of quantum computation and quantum information we won't need to discuss Hamiltonians, and when we do, we will usually just posit that some matrix is the Hamiltonian as a starting point, and proceed from there, without attempting to justify the use of that Hamiltonian.

Because the Hamiltonian is a Hermitian operator it has a spectral decomposition

$$H = \sum_E E|E\rangle\langle E|, \tag{2.87}$$

with eigenvalues E and corresponding normalized eigenvectors $|E\rangle$. The states $|E\rangle$ are conventionally referred to as energy eigenstates, or sometimes as stationary states, and E is the energy of the state $|E\rangle$. The lowest energy is known as the ground state energy for the system, and the corresponding energy eigenstate (or eigenspace) is known as the ground state. The reason the states $|E\rangle$ are sometimes known as stationary states is because their only change in time is to acquire an overall numerical factor,

$$|E\rangle \rightarrow \exp(-iEt/\hbar)|E\rangle. \tag{2.88}$$

As an example, suppose a single qubit has Hamiltonian

$$H = \hbar\omega X. \tag{2.89}$$

In this equation ω is a parameter that, in practice, needs to be experimentally determined. We won't worry about the parameter overly much here - the point is to give you a feel for the

sort of Hamiltonians that are sometimes written down in the study of quantum computation and quantum information. The energy eigenstates of this Hamiltonian are obviously the same as the eigenstates of X, namely $(|0\rangle + |1\rangle)/\sqrt{2}$ and $(|0\rangle - |1\rangle)/\sqrt{2}$, with corresponding energies $\hbar\omega$ and $-\hbar\omega$. The ground state is therefore $(|0\rangle - |1\rangle)/\sqrt{2}$, and the ground state energy is $-\hbar\omega$.

What is the connection between the Hamiltonian picture of dynamics, Postulate 2', and the unitary operator picture, Postulate 2? The answer is provided by writing down the solution to Schrödinger's equation, which is easily verified to be:

$$|\psi(t_2)\rangle = \exp\left[\frac{-iH(t_2 - t_1)}{\hbar}\right]|\psi(t_1)\rangle = U(t_1, t_2)\,|\psi(t_1)\rangle\,, \tag{2.90}$$

where we define

$$U(t_1, t_2) \equiv \exp\left[\frac{-iH(t_2 - t_1)}{\hbar}\right]. \tag{2.91}$$

You will show in the exercises that this operator is unitary, and furthermore, that any unitary operator U can be realized in the form $U = \exp(iK)$ for some Hermitian operator K. There is therefore a one-to-one correspondence between the discrete-time description of dynamics using unitary operators, and the continuous time description using Hamiltonians. For most of the book we use the unitary formulation of quantum dynamics.

Exercise 2.54: Suppose A and B are commuting Hermitian operators. Prove that $\exp(A)\exp(B) = \exp(A + B)$. (Hint: Use the results of Section 2.1.9.)

Exercise 2.55: Prove that $U(t_1, t_2)$ defined in Equation (2.91) is unitary.

Exercise 2.56: Use the spectral decomposition to show that $K \equiv -i\log(U)$ is Hermitian for any unitary U, and thus $U = \exp(iK)$ for some Hermitian K.

In quantum computation and quantum information we often speak of applying a unitary operator to a particular quantum system. For example, in the context of quantum circuits we may speak of applying the unitary gate X to a single qubit. Doesn't this contradict what we said earlier, about unitary operators describing the evolution of a closed quantum system? After all, if we are 'applying' a unitary operator, then that implies that there is an external 'we' who is interacting with the quantum system, and the system is not closed.

An example of this occurs when a laser is focused on an atom. After a lot of thought and hard work it is possible to write down a Hamiltonian describing the total atomlaser system. The interesting thing is that when we write down the Hamiltonian for the atom-laser system and consider the effects on the atom alone, the behavior of the state vector of the atom turns out to be almost but not quite perfectly described by another Hamiltonian, the atomic Hamiltonian. The atomic Hamiltonian contains terms related to laser intensity, and other parameters of the laser, which we can vary at will. It is as if the evolution of the atom were being described by a Hamiltonian which we can vary at will, despite the atom not being a closed system.

More generally, for many systems like this it turns out to be possible to write down a time-varying Hamiltonian for a quantum system, in which the Hamiltonian for the system is not a constant, but varies according to some parameters which are under an experimentalist's control, and which may be changed during the course of an experiment. The system is not, therefore, closed, but it does evolve according to Schrödinger's equation with a time-varying Hamiltonian, to some good approximation.

The upshot is that to begin we will often describe the evolution of quantum systems even systems which aren't closed - using unitary operators. The main exception to this, quantum measurement, will be described in the next section. Later on we will investigate in more detail possible deviations from unitary evolution due to the interaction with other systems, and understand more precisely the dynamics of realistic quantum systems.

7.2.15 2.2.3 Quantum measurement

We postulated that closed quantum systems evolve according to unitary evolution. The evolution of systems which don't interact with the rest of the world is all very well, but there must also be times when the experimentalist and their experimental equipment an external physical system in other words - observes the system to find out what is going on inside the system, an interaction which makes the system no longer closed, and thus not necessarily subject to unitary evolution. To explain what happens when this is done, we introduce Postulate 3, which provides a means for describing the effects of measurements on quantum systems.

Postulate 3: Quantum measurements are described by a collection $\{M_m\}$ of measurement operators. These are operators acting on the state space of the system being measured. The index m refers to the measurement outcomes that may occur in the experiment. If the state of the quantum system is $|\psi\rangle$ immediately before the measurement then the probability that result m occurs is
given by

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle, \tag{2.92}$$

and the state of the system after the measurement is

$$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}. \tag{2.93}$$

The measurement operators satisfy the completeness equation,

$$\sum_m M_m^\dagger M_m = I. \tag{2.94}$$

The completeness equation expresses the fact that probabilities sum to one:

$$1 = \sum_m p(m) = \sum_m \langle\psi|M_m^\dagger M_m|\psi\rangle. \tag{2.95}$$

This equation being satisfied for all $|\psi\rangle$ is equivalent to the completeness equation. However, the completeness equation is much easier to check directly, so that's why it appears in the statement of the postulate.

A simple but important example of a measurement is the measurement of a qubit in the computational basis. This is a measurement on a single qubit with two outcomes defined by the two measurement operators $M_0 = |0\rangle\langle 0|, M_1 = |1\rangle\langle 1|$. Observe that each measurement operator is Hermitian, and that $M_0^2 = M_0, M_1^2 = M_1$. Thus the completeness relation is obeyed, $I = M_0^\dagger M_0 + M_1^\dagger M_1 = M_0 + M_1$. Suppose the state being measured is $|\psi\rangle = a|0\rangle + b|1\rangle$. Then the probability of obtaining measurement outcome 0 is

$$p(0) = \langle\psi|M_0^\dagger M_0|\psi\rangle = \langle\psi|M_0|\psi\rangle = |a|^2. \tag{2.96}$$

Similarly, the probability of obtaining the measurement outcome 1 is $p(1) = |b|^2$. The state after measurement in the two cases is therefore

$$\frac{M_0|\psi\rangle}{|a|} = \frac{a}{|a|}|0\rangle \tag{2.97}$$

$$\frac{M_1|\psi\rangle}{|b|} = \frac{b}{|b|}|1\rangle. \tag{2.98}$$

We will see in Section 2.2.7 that multipliers like $a/|a|$, which have modulus one, can effectively be ignored, so the two post-measurement states are effectively $|0\rangle$ and $|1\rangle$, just as described in Chapter 1.

The status of Postulate 3 as a fundamental postulate intrigues many people. Measuring devices are quantum mechanical systems, so the quantum system being measured and the measuring device together are part of a larger, isolated, quantum mechanical system. (It may be necessary to include quantum systems other than the system being measured and the measuring device to obtain a completely isolated system, but the point is that this can be done.) According to Postulate 2, the evolution of this larger isolated system can be described by a unitary evolution. Might it be possible to derive Postulate 3 as a consequence of this picture? Despite considerable investigation along these lines there is still disagreement between physicists about whether or not this is possible. We, however, are going to take the very pragmatic approach that in practice it is clear when to apply

Postulate 2 and when to apply Postulate 3, and not worry about deriving one postulate from the other.

Over the next few sections we apply Postulate 3 to several elementary but important measurement scenarios. Section 2.2.4 examines the problem of distinguishing a set of quantum states. Section 2.2.5 explains a special case of Postulate 3, the projective or von Neumann measurements. Section 2.2.6 explains another special case of Postulate 3, known as POVM measurements. Many introductions to quantum mechanics only discuss projective measurements, omitting a full discussion of Postulate 3 or of POVM elements. For this reason we have included Box 2.5 on page 91 which comments on the relationship between the different classes of measurement we describe.

Exercise 2.57: (Cascaded measurements are single measurements) Suppose $\{L_l\}$ and $\{M_m\}$ are two sets of measurement operators. Show that a measurement defined by the measurement operators $\{L_l\}$ followed by a measurement defined by the measurement operators $\{M_m\}$ is physically equivalent to a single measurement defined by measurement operators $\{N_{lm}\}$ with the representation $N_{lm} \equiv M_m L_l$.

7.2.16 2.2.4 Distinguishing quantum states

An important application of Postulate 3 is to the problem of distinguishing quantum states. In the classical world, distinct states of an object are usually distinguishable, at least in principle. For example, we can always identify whether a coin has landed heads or tails, at least in the ideal limit. Quantum mechanically, the situation is more complicated. In Section 1.6 we gave a plausible argument that non-orthogonal quantum states cannot be distinguished. With Postulate 3 as a firm foundation we can now give a much more convincing demonstration of this fact.

Distinguishability, like many ideas in quantum computation and quantum information, is most easily understood using the metaphor of a game involving two parties, Alice and Bob. Alice chooses a state $|\psi_i\rangle$ $(1 \leq i \leq n)$ from some fixed set of states known to both parties. She gives the state $|\psi_i\rangle$ to Bob, whose task it is to identify the index i of the state Alice has given him.

Suppose the states $|\psi_i\rangle$ are orthonormal. Then Bob can do a quantum measurement to distinguish these states, using the following procedure. Define measurement operators $M_i \equiv |\psi_i\rangle \langle\psi_i|$, one for each possible index i, and an additional measurement operator M_0 defined as the positive square root of the positive operator $I - \sum_{i \neq 0} |\psi_i\rangle \langle\psi_i|$. These operators satisfy the completeness relation, and if the state $|\psi_i\rangle$ is prepared then $p(i) = \langle\psi_i| M_i |\psi_i\rangle = 1$, so the result i occurs with certainty. Thus, it is possible to reliably distinguish the orthonormal states $|\psi_i\rangle$.

By contrast, if the states $|\psi_i\rangle$ are not orthonormal then we can prove that there is no quantum measurement capable of distinguishing the states. The idea is that Bob will do a measurement described by measurement operators M_j, with outcome j. Depending on the outcome of the measurement Bob tries to guess what the index i was using some rule, $i = f(j)$, where $f(\cdot)$ represents the rule he uses to make the guess. The key to why Bob can't distinguish non-orthogonal states $|\psi_1\rangle$ and $|\psi_2\rangle$ is the observation that $|\psi_2\rangle$ can be decomposed into a (non-zero) component parallel to $|\psi_1\rangle$, and a component orthogonal to $|\psi_1\rangle$. Suppose j is a measurement outcome such that $f(j) = 1$, that is, Bob guesses that the state was $|\psi_1\rangle$ when he observes j. But because of the component of $|\psi_2\rangle$ parallel
to $|\psi_1\rangle$, there is a non-zero probability of getting outcome j when $|\psi_2\rangle$ is prepared, so sometimes Bob will make an error identifying which state was prepared. A more rigorous argument that non-orthogonal states can't be distinguished is given in Box 2.3, but this captures the essential idea.

Box 2.3: Proof that non-orthogonal states can't be reliably distinguished

A proof by contradiction shows that no measurement distinguishing the nonorthogonal states $|\psi_1\rangle$ and $|\psi_2\rangle$ is possible. Suppose such a measurement is possible. If the state $|\psi_1\rangle$ ($|\psi_2\rangle$) is prepared then the probability of measuring j such that $f(j) = 1 (f(j) = 2)$ must be 1 . Defining $E_i \equiv \sum_{j:f(j)=i} M_j^\dagger M_j$, these observations may be written as:

$$\langle\psi_1| E_1 |\psi_1\rangle = 1; \quad \langle\psi_2| E_2 |\psi_2\rangle = 1. \tag{2.99}$$

Since $\sum_i E_i = I$ it follows that $\sum_i \langle\psi_1| E_i |\psi_1\rangle = 1$, and since $\langle\psi_1| E_1 |\psi_1\rangle = 1$ we must have $\langle\psi_1| E_2 |\psi_1\rangle = 0$, and thus $\sqrt{E_2}|\psi_1\rangle = 0$. Suppose we decompose $|\psi_2\rangle = \alpha|\psi_1\rangle + \beta|\varphi\rangle$, where $|\varphi\rangle$ is orthonormal to $|\psi_1\rangle$, $|\alpha|^2 + |\beta|^2 = 1$, and $|\beta| < 1$ since $|\psi_1\rangle$ and $|\psi_2\rangle$ are not orthogonal. Then $\sqrt{E_2}|\psi_2\rangle = \beta\sqrt{E_2}|\varphi\rangle$, which implies a contradiction with (2.99), as

$$\langle\psi_2| E_2 |\psi_2\rangle = |\beta|^2 \langle\varphi|E_2|\varphi\rangle \leq |\beta|^2 < 1, \tag{2.100}$$

where the second last inequality follows from the observation that

$$\langle\varphi|E_2|\varphi\rangle \leq \sum_i \langle\varphi|E_i|\varphi\rangle = \langle\varphi \mid \varphi\rangle = 1. \tag{2.101}$$

7.2.17 2.2.5 Projective measurements

In this section we explain an important special case of the general measurement postulate, Postulate 3. This special class of measurements is known as projective measurements. For many applications of quantum computation and quantum information we will be concerned primarily with projective measurements. Indeed, projective measurements actually turn out to be equivalent to the general measurement postulate, when they are augmented with the ability to perform unitary transformations, as described in Postulate 2. We will explain this equivalence in detail in Section 2.2.8, as the statement of the measurement postulate for projective measurements is superficially rather different from the general postulate, Postulate 3.

Projective measurements: A projective measurement is described by an observable, M, a Hermitian operator on the state space of the system being observed. The observable has a spectral decomposition,

$$M = \sum_m m P_m, \tag{2.102}$$

where P_m is the projector onto the eigenspace of M with eigenvalue m. The possible outcomes of the measurement correspond to the eigenvalues, m, of the observable. Upon measuring the state $|\psi\rangle$, the probability of getting result m is
given by

$$p(m) = \langle\psi|P_m|\psi\rangle. \tag{2.103}$$

Given that outcome m occurred, the state of the quantum system immediately after the measurement is

$$\frac{P_m|\psi\rangle}{\sqrt{p(m)}} \tag{2.104}$$

Projective measurements can be understood as a special case of Postulate 3. Suppose the measurement operators in Postulate 3, in addition to satisfying the completeness relation $\sum_m M_m^\dagger M_m = I$, also satisfy the conditions that M_m are orthogonal projectors, that is, the M_m are Hermitian, and $M_m M_{m'} = \delta_{m,m'} M_m$. With these additional restrictions, Postulate 3 reduces to a projective measurement as just defined.

Projective measurements have many nice properties. In particular, it is very easy to calculate average values for projective measurements. By definition, the average (see Appendix 1 for elementary definitions and results in probability theory) value of the measurement is

$$\begin{aligned}
\mathbf{E}(M) &= \sum_m m p(m) && (2.110)\\
&= \sum_m m\langle\psi|P_m|\psi\rangle && (2.111)\\
&= \langle\psi|\left(\sum_m m P_m\right)|\psi\rangle && (2.112)\\
&= \langle\psi|M|\psi\rangle. && (2.113)
\end{aligned}$$

This is a useful formula, which simplifies many calculations. The average value of the observable M is often written $\langle M\rangle \equiv \langle\psi|M|\psi\rangle$. From this formula for the average follows a formula for the standard deviation associated to observations of M,

$$\begin{aligned}
[\Delta(M)]^2 &= \left\langle (M - \langle M\rangle)^2 \right\rangle && (2.114)\\
&= \left\langle M^2 \right\rangle - \langle M\rangle^2. && (2.115)
\end{aligned}$$

The standard deviation is a measure of the typical spread of the observed values upon measurement of M. In particular, if we perform a large number of experiments in which the state $|\psi\rangle$ is prepared and the observable M is measured, then the standard deviation $\Delta(M)$ of the observed values is determined by the formula $\Delta(M) = \sqrt{\langle M^2\rangle - \langle M\rangle^2}$. This formulation of measurement and standard deviations in terms of observables gives rise in an elegant way to results such as the Heisenberg uncertainty principle (see Box 2.4).

Exercise 2.58: Suppose we prepare a quantum system in an eigenstate $|\psi\rangle$ of some observable M, with corresponding eigenvalue m. What is the average observed value of M, and the standard deviation?

Two widely used nomenclatures for measurements deserve emphasis. Rather than giving an observable to describe a projective measurement, often people simply list a complete set of orthogonal projectors P_m satisfying the relations $\sum_m P_m = I$ and $P_m P_{m'} =$

Box 2.4: The Heisenberg uncertainty principle

Perhaps the best known result of quantum mechanics is the Heisenberg uncertainty principle. Suppose A and B are two Hermitian operators, and $|\psi\rangle$ is a quantum state. Suppose $\langle\psi|AB|\psi\rangle = x + iy$, where x and y are real. Note that $\langle\psi|[A,B]|\psi\rangle = 2iy$ and $\langle\psi|\{A,B\}|\psi\rangle = 2x$. This implies that

$$|\langle\psi|[A,B]|\psi\rangle\ |^2 + |\langle\psi|\{A,B\}|\psi\rangle\ |^2 = 4|\langle\psi|AB|\psi\rangle\ |^2 . \tag{2.105}$$

By the Cauchy-Schwarz inequality

$$|\langle\psi|AB|\psi\rangle\ |^2 \leq \langle\psi|A^2|\psi\rangle\langle\psi|B^2|\psi\rangle, \tag{2.106}$$

which combined with Equation (2.105) and dropping a non-negative term gives

$$|\langle\psi|[A,B]|\psi\rangle\ |^2 \leq 4\langle\psi|A^2|\psi\rangle\langle\psi|B^2|\psi\rangle. \tag{2.107}$$

Suppose C and D are two observables. Substituting $A = C - \langle C\rangle$ and $B = D - \langle D\rangle$ into the last equation, we obtain Heisenberg's uncertainty principle as it is usually stated:

$$\Delta(C)\Delta(D) \geq \frac{|\langle\psi|[C,D]|\psi\rangle\ |}{2} \tag{2.108}$$

You should be wary of a common misconception about the uncertainty principle, that measuring an observable C to some 'accuracy' $\Delta(C)$ causes the value of D to be 'disturbed' by an amount $\Delta(D)$ in such a way that some sort of inequality similar to (2.108) is satisfied. While it is true that measurements in quantum mechanics cause disturbance to the system being measured, this is most emphatically not the content of the uncertainty principle.
The correct interpretation of the uncertainty principle is that if we prepare a large number of quantum systems in identical states, $|\psi\rangle$, and then perform measurements of C on some of those systems, and of D in others, then the standard deviation $\Delta(C)$ of the C results times the standard deviation $\Delta(D)$ of the results for D will satisfy the inequality (2.108).
As an example of the uncertainty principle, consider the observables X and Y when measured for the quantum state $|0\rangle$. In Equation (2.70) we showed that $[X,Y] = 2iZ$, so the uncertainty principle tells us that

$$\Delta(X)\Delta(Y) \geq \langle 0|Z|0\rangle = 1 \tag{2.109}$$

One elementary consequence of this is that $\Delta(X)$ and $\Delta(Y)$ must both be strictly greater than 0 , as can be verified by direct calculation.
$\delta_{mm'}P_m$. The corresponding observable implicit in this usage is $M = \sum_m mP_m$. Another widely used phrase, to 'measure in a basis $|m\rangle$ ', where $|m\rangle$ form an orthonormal basis, simply means to perform the projective measurement with projectors $P_m = |m\rangle\langle m|$.

Let's look at an example of projective measurements on single qubits. First is the measurement of the observable Z. This has eigenvalues +1 and -1 with corresponding eigenvectors $|0\rangle$ and $|1\rangle$. Thus, for example, measurement of Z on the state $|\psi\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ gives the result +1 with probability $\langle\psi\mid 0\rangle\langle 0\mid\psi\rangle = 1/2$, and similarly the
result -1 with probability 1/2. More generally, suppose $\vec{v}$ is any real three-dimensional unit vector. Then we can define an observable:

$$\vec{v}\cdot\vec{\sigma} \equiv v_1\sigma_1 + v_2\sigma_2 + v_3\sigma_3 \tag{2.116}$$

Measurement of this observable is sometimes referred to as a 'measurement of spin along the $\vec{v}$ axis', for historical reasons. The following two exercises encourage you to work out some elementary but important properties of such a measurement.

Exercise 2.59: Suppose we have qubit in the state $|0\rangle$, and we measure the observable X. What is the average value of X ? What is the standard deviation of X ?

Exercise 2.60: Show that $\vec{v} \cdot \vec{\sigma}$ has eigenvalues ± 1, and that the projectors onto the corresponding eigenspaces are given by $P_{\pm} = (I \pm \vec{v} \cdot \vec{\sigma})/2$.

Exercise 2.61: Calculate the probability of obtaining the result $+1$ for a measurement of $\vec{v} \cdot \vec{\sigma}$, given that the state prior to measurement is $|0\rangle$. What is the state of the system after the measurement if $+1$ is obtained?

7.2.18 2.2.6 POVM measurements

The quantum measurement postulate, Postulate 3, involves two elements. First, it gives a rule describing the measurement statistics, that is, the respective probabilities of the different possible measurement outcomes. Second, it gives a rule describing the postmeasurement state of the system. However, for some applications the post-measurement state of the system is of little interest, with the main item of interest being the probabilities of the respective measurement outcomes. This is the case, for example, in an experiment where the system is measured only once, upon conclusion of the experiment. In such instances there is a mathematical tool known as the POVM formalism which is especially well adapted to the analysis of the measurements. (The acronym POVM stands for 'Positive Operator-Valued Measure', a technical term whose historical origins we won't worry about.) This formalism is a simple consequence of the general description of measurements introduced in Postulate 3, but the theory of POVMs is so elegant and widely used that it merits a separate discussion here.

Suppose a measurement described by measurement operators M_m is performed upon a quantum system in the state $|\psi\rangle$. Then the probability of outcome m is given by $p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$. Suppose we define

$$E_m \equiv M_m^\dagger M_m \tag{2.117}$$

Then from Postulate 3 and elementary linear algebra, E_m is a positive operator such that $\sum_m E_m = I$ and $p(m) = \langle\psi|E_m|\psi\rangle$. Thus the set of operators E_m are sufficient to determine the probabilities of the different measurement outcomes. The operators E_m are known as the POVM elements associated with the measurement. The complete set $\{E_m\}$ is known as a POVM.

As an example of a POVM, consider a projective measurement described by measurement operators P_m, where the P_m are projectors such that $P_m P_{m'} = \delta_{mm'} P_m$ and $\sum_m P_m = I$. In this instance (and only this instance) all the POVM elements are the same as the measurement operators themselves, since $E_m \equiv P_m^\dagger P_m = P_m$.

Box 2.5: General measurements, projective measurements, and POVMs Most introductions to quantum mechanics describe only projective measurements, and consequently the general description of measurements given in Postulate 3 may be unfamiliar to many physicists, as may the POVM formalism described in Section 2.2.6. The reason most physicists don't learn the general measurement formalism is because most physical systems can only be measured in a very coarse manner. In quantum computation and quantum information we aim for an exquisite level of control over the measurements that may be done, and consequently it helps to use a more comprehensive formalism for the description of measurements.

Of course, when the other axioms of quantum mechanics are taken into account, projective measurements augmented by unitary operations turn out to be completely equivalent to general measurements, as shown in Section 2.2.8. So a physicist trained in the use of projective measurements might ask to what end we start with the general formalism, Postulate 3? There are several reasons for doing so. First, mathematically general measurements are in some sense simpler than projective measurements, since they involve fewer restrictions on the measurement

operators; there is, for example, no requirement for general measurements analogous to the condition $P_i P_j = \delta_{ij} P_i$ for projective measurements. This simpler structure also gives rise to many useful properties for general measurements that are not possessed by projective measurements. Second, it turns out that there are important problems in quantum computation and quantum information - such as the optimal way to distinguish a set of quantum states - the answer to which involves a general measurement, rather than a projective measurement.

A third reason for preferring Postulate 3 as a starting point is related to a property of projective measurements known as repeatability. Projective measurements are repeatable in the sense that if we perform a projective measurement once, and obtain the outcome m, repeating the measurement gives the outcome m again and does not change the state. To see this, suppose $|\psi\rangle$ was the initial state. After the first measurement the state is $|\psi_m\rangle = (P_m|\psi\rangle) / \sqrt{\langle\psi|P_m|\psi\rangle}$. Applying P_m to $|\psi_m\rangle$ does not change it, so we have $\langle\psi_m| P_m |\psi_m\rangle = 1$, and therefore repeated measurement gives the result m each time, without changing the state.

This repeatability of projective measurements tips us off to the fact that many important measurements in quantum mechanics are not projective measurements. For instance, if we use a silvered screen to measure the position of a photon we destroy the photon in the process. This certainly makes it impossible to repeat the measurement of the photon's position! Many other quantum measurements are also not repeatable in the same sense as a projective measurement. For such measurements, the general measurement postulate, Postulate 3, must be employed. Where do POVMs fit in this picture? POVMs are best viewed as a special case of the general measurement formalism, providing the simplest means by which one can study general measurement statistics, without the necessity for knowing the post-measurement state. They are a mathematical convenience that sometimes gives extra insight into quantum measurements.

Exercise 2.62: Show that any measurement where the measurement operators and the POVM elements coincide is a projective measurement.

Above we noticed that the POVM operators are positive and satisfy $\sum_m E_m = I$. Suppose now that $\{E_m\}$ is some arbitrary set of positive operators such that $\sum_m E_m = I$. We will show that there exists a set of measurement operators M_m defining a measurement described by the POVM $\{E_m\}$. Defining $M_m \equiv \sqrt{E_m}$ we see that $\sum_m M_m^\dagger M_m = \sum_m E_m = I$, and therefore the set $\{M_m\}$ describes a measurement with POVM $\{E_m\}$. For this reason it is convenient to define a POVM to be any set of operators $\{E_m\}$ such that: (a) each operator E_m is positive; and (b) the completeness relation $\sum_m E_m = I$ is obeyed, expressing the fact that probabilities sum to one. To complete the description of POVMs, we note again that given a POVM $\{E_m\}$, the probability of outcome m is given by $p(m) = \langle\psi|E_m|\psi\rangle$.

We've looked at projective measurements as an example of the use of POVMs, but it wasn't very exciting since we didn't learn much that was new. The following more sophisticated example illustrates the use of the POVM formalism as a guide for our intuition in quantum computation and quantum information. Suppose Alice gives Bob a qubit prepared in one of two states, $|\psi_1\rangle = |0\rangle$ or $|\psi_2\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. As explained in Section 2.2.4 it is impossible for Bob to determine whether he has been given $|\psi_1\rangle$ or $|\psi_2\rangle$ with perfect reliability. However, it is possible for him to perform a measurement which distinguishes the states some of the time, but never makes an error of mis-identification. Consider a POVM containing three elements,

$$E_1 \equiv \frac{\sqrt{2}}{1+\sqrt{2}} |1\rangle\langle 1| \tag{2.118}$$

$$E_2 \equiv \frac{\sqrt{2}}{1+\sqrt{2}} \frac{(|0\rangle - |1\rangle)(\langle 0| - \langle 1|)}{2} \tag{2.119}$$

$$E_3 \equiv I - E_1 - E_2 \tag{2.120}$$

It is straightforward to verify that these are positive operators which satisfy the completeness

relation $\sum_m E_m = I$, and therefore form a legitimate POVM.

Suppose Bob is given the state $|\psi_1\rangle = |0\rangle$. He performs the measurement described by the POVM $\{E_1, E_2, E_3\}$. There is zero probability that he will observe the result E_1, since E_1 has been cleverly chosen to ensure that $\langle\psi_1| E_1 |\psi_1\rangle = 0$. Therefore, if the result of his measurement is E_1 then Bob can safely conclude that the state he received must have been $|\psi_2\rangle$. A similar line of reasoning shows that if the measurement outcome E_2 occurs then it must have been the state $|\psi_1\rangle$ that Bob received. Some of the time, however, Bob will obtain the measurement outcome E_3, and he can infer nothing about the identity of the state he was given. The key point, however, is that Bob never makes a mistake identifying the state he has been given. This infallibility comes at the price that sometimes Bob obtains no information about the identity of the state.

This simple example demonstrates the utility of the POVM formalism as a simple and intuitive way of gaining insight into quantum measurements in instances where only the measurement statistics matter. In many instances later in the book we will only be concerned with measurement statistics, and will therefore use the POVM formalism rather than the more general formalism for measurements described in Postulate 3.

Exercise 2.63: Suppose a measurement is described by measurement operators M_m.

Show that there exist unitary operators U_m such that $M_m = U_m\sqrt{E_m}$, where E_m is the POVM associated to the measurement.

Exercise 2.64: Suppose Bob is given a quantum state chosen from a set $|\psi_1\rangle, \ldots, |\psi_m\rangle$ of linearly independent states. Construct a POVM $\{E_1, E_2, \ldots, E_{m+1}\}$ such that if outcome E_i occurs, $1 \leq i \leq m$, then Bob knows with certainty that he was given the state $|\psi_i\rangle$. (The POVM must be such that $\langle\psi_i| E_i |\psi_i\rangle > 0$ for each i.)

7.2.19 2.2.7 Phase

'Phase' is a commonly used term in quantum mechanics, with several different meanings dependent upon context. At this point it is convenient to review a couple of these meanings. Consider, for example, the state $e^{i\theta}|\psi\rangle$, where $|\psi\rangle$ is a state vector, and θ is a real number. We say that the state $e^{i\theta}|\psi\rangle$ is equal to $|\psi\rangle$, up to the global phase factor $e^{i\theta}$. It is interesting to note that the statistics of measurement predicted for these two states are the same. To see this, suppose M_m is a measurement operator associated to some quantum measurement, and note that the respective probabilities for outcome m occurring are $\langle\psi|M_m^\dagger M_m|\psi\rangle$ and $\langle\psi|e^{-i\theta}M_m^\dagger M_m e^{i\theta}|\psi\rangle = \langle\psi|M_m^\dagger M_m|\psi\rangle$. Therefore, from an observational point of view these two states are identical. For this reason we may ignore global phase factors as being irrelevant to the observed properties of the physical system.

There is another kind of phase known as the relative phase, which has quite a different meaning. Consider the states

$$\frac{|0\rangle + |1\rangle}{\sqrt{2}} \quad \text{and} \quad \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{2.121}$$

In the first state the amplitude of $|1\rangle$ is $1/\sqrt{2}$. For the second state the amplitude is $-1/\sqrt{2}$. In each case the magnitude of the amplitudes is the same, but they differ in sign. More generally, we say that two amplitudes, a and b, differ by a relative phase if there is a real θ such that $a = \exp(i\theta)b$. More generally still, two states are said to differ by a relative phase in some basis if each of the amplitudes in that basis is related by such a phase factor. For example, the two states displayed above are the same up to a relative phase shift because the $|0\rangle$ amplitudes are identical (a relative phase factor of 1), and the $|1\rangle$ amplitudes differ only by a relative phase factor of -1 . The difference between relative phase factors and global phase factors is that for relative phase the phase factors may vary from amplitude to amplitude. This

makes the relative phase a basis-dependent concept unlike global phase. As a result, states which differ only by relative phases in some basis give rise to physically observable differences in measurement statistics, and it is not possible to regard these states as physically equivalent, as we do with states differing by a global phase factor

Exercise 2.65: Express the states $(|0\rangle + |1\rangle)/\sqrt{2}$ and $(|0\rangle - |1\rangle)/\sqrt{2}$ in a basis in which they are not the same up to a relative phase shift.

7.2.20 2.2.8 Composite systems

Suppose we are interested in a composite quantum system made up of two (or more) distinct physical systems. How should we describe states of the composite system? The following postulate describes how the state space of a composite system is built up from the state spaces of the component systems.

Postulate 4: The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. Moreover, if we have systems numbered 1 through n, and system number i is prepared in the state $|\psi_i\rangle$, then the joint state of the total system is $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$.

Why is the tensor product the mathematical structure used to describe the state space of a composite physical system? At one level, we can simply accept it as a basic postulate, not reducible to something more elementary, and move on. After all, we certainly expect that there be some canonical way of describing composite systems in quantum mechanics. Is there some other way we can arrive at this postulate? Here is one heuristic that is sometimes used. Physicists sometimes like to speak of the superposition principle of quantum mechanics, which states that if $|x\rangle$ and $|y\rangle$ are two states of a quantum system, then any superposition $\alpha|x\rangle + \beta|y\rangle$ should also be an allowed state of a quantum system, where $|\alpha|^2 + |\beta|^2 = 1$. For composite systems, it seems natural that if $|A\rangle$ is a state of system A, and $|B\rangle$ is a state of system B, then there should be some corresponding state, which we might denote $|A\rangle|B\rangle$, of the joint system AB. Applying the superposition principle to product states of this form, we arrive at the tensor product postulate given above. This is not a derivation, since we are not taking the superposition principle as a fundamental part of our description of quantum mechanics, but it gives you the flavor of the various ways in which these ideas are sometimes reformulated.

A variety of different notations for composite systems appear in the literature. Part of the reason for this proliferation is that different notations are better adapted for different applications, and we will also find it convenient to introduce some specialized notations on occasion. At this point it suffices to mention a useful subscript notation to denote states and operators on different systems, when it is not clear from context. For example, in a system containing three qubits, X_2 is the Pauli σ_x operator acting on the second qubit.

Exercise 2.66: Show that the average value of the observable $X_1 Z_2$ for a two qubit system measured in the state $(|00\rangle + |11\rangle)/\sqrt{2}$ is zero.

In Section 2.2.5 we claimed that projective measurements together with unitary dynamics are sufficient to implement a general measurement. The proof of this statement makes use of composite quantum systems, and is a nice illustration of Postulate 4 in action. Suppose we have a quantum system with state space Q, and we want to perform a measurement described by measurement operators M_m on the system Q. To do this, we introduce an ancilla system, with state space M, having an orthonormal basis $|m\rangle$ in one-to-one correspondence with the possible outcomes of the measurement we wish to implement. This ancilla system can be regarded as merely a mathematical device appearing in the construction, or it can be interpreted physically as an extra quantum system introduced into the problem, which we assume has a state space with the required properties.

Letting $|0\rangle$ be any fixed state of M, define an operator U on products $|\psi\rangle|0\rangle$ of states $|\psi\rangle$

from Q with the state $|0\rangle$ by

$$U|\psi\rangle|0\rangle \equiv \sum_m M_m|\psi\rangle|m\rangle \tag{2.122}$$

Using the orthonormality of the states $|m\rangle$ and the completeness relation $\sum_m M_m^\dagger M_m = I$, we can see that U preserves inner products between states of the form $|\psi\rangle|0\rangle$,

$$\begin{aligned}\langle\varphi|\langle 0|U^\dagger U|\psi\rangle|0\rangle &= \sum_{m,m'}\langle\varphi|M_m^\dagger M_{m'}|\psi\rangle\,\langle m \mid m'\rangle &(2.123)\\ &= \sum_m \langle\varphi|M_m^\dagger M_m|\psi\rangle &(2.124)\\ &= \langle\varphi \mid \psi\rangle &(2.125)\end{aligned}$$

By the results of Exercise 2.67 it follows that U can be extended to a unitary operator on the space $Q \otimes M$, which we also denote by U.

Exercise 2.67: Suppose V is a Hilbert space with a subspace W. Suppose $U : W \to V$ is a linear operator which preserves inner products, that is, for any $|w_1\rangle$ and $|w_2\rangle$ in W,

$$\langle w_1|\, U^\dagger U\, |w_2\rangle = \langle w_1 \mid w_2\rangle\,. \tag{2.126}$$

Prove that there exists a unitary operator $U' : V \to V$ which extends U. That is, $U'|w\rangle = U|w\rangle$ for all $|w\rangle$ in W, but U' is defined on the entire space V. Usually we omit the prime symbol ' and just write U to denote the extension.

Next, suppose we perform a projective measurement on the two systems described by projectors $P_m \equiv I_Q \otimes |m\rangle\langle m|$. Outcome m occurs with probability

$$\begin{aligned}p(m) &= \langle\psi|\langle 0|U^\dagger P_m U|\psi\rangle|0\rangle &(2.127)\\ &= \sum_{m',m''}\langle\psi|M_{m'}^\dagger\,\langle m'|\,(I_Q\otimes|m\rangle\langle m|)\,M_{m''}|\psi\rangle\,|m''\rangle &(2.128)\\ &= \langle\psi|M_m^\dagger M_m|\psi\rangle, &(2.129)\end{aligned}$$

just as given in Postulate 3. The joint state of the system QM after measurement, conditional on result m occurring, is given by

$$\frac{P_m U|\psi\rangle|0\rangle}{\sqrt{\langle\psi|U^\dagger P_m U|\psi\rangle}} = \frac{M_m|\psi\rangle|m\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}. \tag{2.130}$$

It follows that the state of system M after the measurement is $|m\rangle$, and the state of system Q is

$$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}, \tag{2.131}$$

just as prescribed by Postulate 3. Thus unitary dynamics, projective measurements, and the ability to introduce ancillary systems, together allow any measurement of the form described in Postulate 3 to be realized.

Postulate 4 also enables us to define one of the most interesting and puzzling ideas associated with composite quantum systems - entanglement. Consider the two qubit state

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}. \tag{2.132}$$

This state has the remarkable property that there are no single qubit states $|a\rangle$ and $|b\rangle$ such that $|\psi\rangle = |a\rangle|b\rangle$, a fact which you should now convince yourself of:

Exercise 2.68: Prove that $|\psi\rangle \neq |a\rangle|b\rangle$ for all single qubit states $|a\rangle$ and $|b\rangle$.

We say that a state of a composite system having this property (that it can't be written as a product of states of its component systems) is an entangled state. For reasons which nobody fully understands, entangled states play a crucial role in quantum computation and quantum information, and arise repeatedly through the remainder of this book. We have already seen entanglement play a crucial role in quantum teleportation, as described in Section 1.3.7. In this chapter we give two examples of the strange effects enabled by entangled quantum states, superdense coding (Section 2.3), and the violation of Bell's inequality (Section 2.6).

7.2.21 2.2.9 Quantum mechanics: a global view

We have now explained all the fundamental postulates of quantum mechanics. Most of the rest of the book is taken up with deriving consequences of these postulates. Let's quickly review the postulates and try to place them in some kind of global perspective.

Postulate 1 sets the arena for quantum mechanics, by specifying how the state of an isolated quantum system is to be described. Postulate 2 tells us that the dynamics of closed quantum systems are described by the Schrödinger equation, and thus by unitary evolution. Postulate 3 tells us how to extract information from our quantum systems by giving a prescription for the description of measurement. Postulate 4 tells us how the state spaces of different quantum systems may be combined to give a description of the composite system.

What's odd about quantum mechanics, at least by our classical lights, is that we can't directly observe the state vector. It's a little bit like a game of chess where you can never find out exactly where each piece is, but only know the rank of the board they are on. Classical physics - and our intuition - tells us that the fundamental properties of an object, like energy, position, and velocity, are directly accessible to observation. In quantum mechanics these quantities no longer appear as fundamental, being replaced by the state vector, which can't be directly observed. It is as though there is a hidden world in quantum mechanics, which we can only indirectly and imperfectly access. Moreover, merely observing a classical system does not necessarily change the state of the system. Imagine how difficult it would be to play tennis if each time you looked at the ball its position changed! But according to Postulate 3, observation in quantum mechanics is an invasive procedure that typically changes the state of the system.

What conclusions should we draw from these strange features of quantum mechanics? Might it be possible to reformulate quantum mechanics in a mathematically equivalent way so that it had a structure more like classical physics? In Section 2.6 we'll prove Bell's inequality, a surprising result that shows any attempt at such a reformulation is doomed to failure. We're stuck with the counter-intuitive nature of quantum mechanics. Of course, the proper reaction to this is glee, not sorrow! It gives us an opportunity to develop tools of thought that make quantum mechanics intuitive. Moreover, we can exploit the hidden nature of the state vector to do information processing tasks beyond what is possible in the classical world. Without this counter-intuitive behavior, quantum computation and quantum information would be a lot less interesting.

We can also turn this discussion about, and ask ourselves: 'If quantum mechanics is so different from classical physics, then how come the everyday world looks so classical?" Why do we see no evidence of a hidden state vector in our everyday lives? It turns out that the classical world we see can be derived from quantum mechanics as an approximate

description of the world that will be valid on the sort of time, length and mass scales we commonly encounter in our everyday lives. Explaining the details of how quantum mechanics gives rise to classical physics is beyond the scope of this book, but the interested reader should check out the discussion of this topic in 'History and further reading'at the end of Chapter 8.

7.2.22 2.3 Application: superdense coding

Superdense coding is a simple yet surprising application of elementary quantum mechanics. It combines in a concrete, non-trivial way all the basic ideas of elementary quantum mechanics, as covered in the previous sections, and is therefore an ideal example of the information processing tasks that can be accomplished using quantum mechanics.

Superdense coding involves two parties, conventionally known as 'Alice' and 'Bob', who are a long way away from one another. Their goal is to transmit some classical information from Alice to Bob. Suppose Alice is in possession of two classical bits of information which she wishes to send Bob, but is only allowed to send a single qubit to Bob. Can she achieve her goal?

Superdense coding tells us that the answer to this question is yes. Suppose Alice and Bob initially share a pair of qubits in the entangled state

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}. \tag{2.133}$$

Alice is initially in possession of the first qubit, while Bob has possession of the second qubit, as illustrated in Figure 2.3. Note that $|\psi\rangle$ is a fixed state; there is no need for Alice to have sent Bob any qubits in order to prepare this state. Instead, some third party may prepare the entangled state ahead of time, sending one of the qubits to Alice, and the other to Bob.

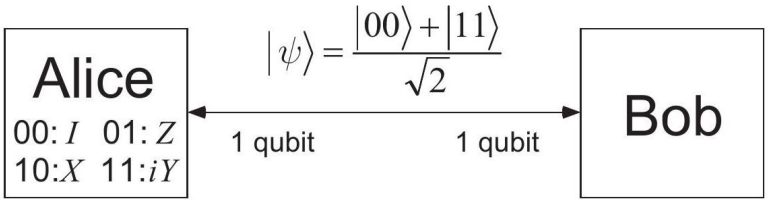


Figure 2.3. The initial setup for superdense coding, with Alice and Bob each in possession of one half of an entangled pair of qubits. Alice can use superdense coding to transmit two classical bits of information to Bob, using only a single qubit of communication and this preshared entanglement.

By sending the single qubit in her possession to Bob, it turns out that Alice can communicate two bits of classical information to Bob. Here is the procedure she uses. If she wishes to send the bit string ' 00 ' to Bob then she does nothing at all to her qubit. If she wishes to send ' 01 ' then she applies the phase flip Z to her qubit. If she wishes to send ' 10 ' then she applies the quantum not gate, X, to her qubit. If she wishes to send '11' then she applies the iY gate to her qubit. The four resulting states are easily seen
to be:

$$00 : |\psi\rangle \rightarrow \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{2.134}$$

$$01 : |\psi\rangle \rightarrow \frac{|00\rangle - |11\rangle}{\sqrt{2}} \tag{2.135}$$

$$10 : |\psi\rangle \rightarrow \frac{|10\rangle + |01\rangle}{\sqrt{2}} \tag{2.136}$$

$$11 : |\psi\rangle \rightarrow \frac{|01\rangle - |10\rangle}{\sqrt{2}} \tag{2.137}$$

As we noted in Section 1.3.6, these four states are known as the Bell basis, Bell states, or EPR pairs, in honor of several of the pioneers who first appreciated the novelty of entanglement. Notice that the Bell states form an orthonormal basis, and can therefore be distinguished by an appropriate quantum measurement. If Alice sends her qubit to Bob, giving Bob possession of both qubits, then by doing a measurement in the Bell basis Bob can determine which of the four possible bit strings Alice sent.

Summarizing, Alice, interacting with only a single qubit, is able to transmit two bits of information to Bob. Of course, two qubits are involved in the protocol, but Alice never need interact with the second qubit. Classically, the task Alice accomplishes would have been impossible had she only transmitted a single classical bit, as we will show in Chapter 12. Furthermore, this remarkable superdense coding protocol has received partial verification in the laboratory. (See 'History and further reading' for references to the experimental verification.) In later chapters we will see many other examples, some of them much more spectacular than superdense coding, of quantum mechanics being harnessed to perform information processing tasks. However, a key point can already be seen in this beautiful example: information is physical, and surprising physical theories such as quantum mechanics may predict surprising information processing abilities.

Exercise 2.69: Verify that the Bell basis forms an orthonormal basis for the two qubit state space.

Exercise 2.70: Suppose E is any positive operator acting on Alice's qubit. Show that $\langle\psi|E \otimes I|\psi\rangle$ takes the same value when $|\psi\rangle$ is any of the four Bell states. Suppose some malevolent third party ('Eve') intercepts Alice's qubit on the way to Bob in the superdense coding protocol. Can Eve infer anything about which of the four possible bit strings $00, 01, 10, 11$ Alice is trying to send? If so, how, or if not, why not?

7.2.23 2.4 The density operator

We have formulated quantum mechanics using the language of state vectors. An alternate formulation is possible using a tool known as the density operator or density matrix. This alternate formulation is mathematically equivalent to the state vector approach, but it provides a much more convenient language for thinking about some commonly encountered scenarios in quantum mechanics. The next three sections describe the density operator formulation of quantum mechanics. Section 2.4.1 introduces the density operator using the concept of an ensemble of quantum states. Section 2.4.2 develops some general
properties of the density operator. Finally, Section 2.4.3 describes an application where the density operator really shines - as a tool for the description of individual subsystems of a composite quantum system.

7.2.24 2.4.1 Ensembles of quantum states

The density operator language provides a convenient means for describing quantum systems whose state is not completely known. More precisely, suppose a quantum system is in one of a number of states $|\psi_i\rangle$, where i is an index, with respective probabilities p_i. We shall call $\{p_i, |\psi_i\rangle\}$ an ensemble of pure states. The density operator for the system is defined by the equation

$$\rho \equiv \sum_i p_i |\psi_i\rangle \langle\psi_i| \tag{2.138}$$

The density operator is often known as the density matrix; we will use the two terms interchangeably. It turns out that all the postulates of quantum mechanics can be reformulated in terms of the density operator language. The purpose of this section and the next is to explain how to perform this reformulation, and explain when it is useful. Whether one uses the density operator language or the state vector language is a matter of taste, since both give the same results; however it is sometimes much easier to approach problems from one point of view rather than the other.

Suppose, for example, that the evolution of a closed quantum system is described by the unitary operator U. If the system was initially in the state $|\psi_i\rangle$ with probability p_i then after the evolution has occurred the system will be in the state $U|\psi_i\rangle$ with probability p_i. Thus, the evolution of the density operator is described by the equation

$$\rho = \sum_i p_i |\psi_i\rangle \langle\psi_i| \stackrel{U}{\rightarrow} \sum_i p_i U |\psi_i\rangle \langle\psi_i| U^\dagger = U\rho U^\dagger. \tag{2.139}$$

Measurements are also easily described in the density operator language. Suppose we perform a measurement described by measurement operators M_m. If the initial state was $|\psi_i\rangle$, then the probability of getting result m is

$$p(m \mid i) = \langle\psi_i| M_m^\dagger M_m |\psi_i\rangle = \mathrm{tr}\left(M_m^\dagger M_m |\psi_i\rangle \langle\psi_i|\right), \tag{2.140}$$

where we have used Equation (2.61) to obtain the last equality. By the law of total probability (see Appendix 1 for an explanation of this and other elementary notions of probability theory) the probability of obtaining result m is

$$\begin{aligned} p(m) &= \sum_i p(m \mid i) p_i && (2.141)\\ &= \sum_i p_i \,\mathrm{tr}\left(M_m^\dagger M_m |\psi_i\rangle \langle\psi_i|\right) && (2.142)\\ &= \mathrm{tr}\left(M_m^\dagger M_m \rho\right). && (2.143) \end{aligned}$$

What is the density operator of the system after obtaining the measurement result m ? If the initial state was $|\psi_i\rangle$ then the state after obtaining the result m is

$$|\psi_i^m\rangle = \frac{M_m |\psi_i\rangle}{\sqrt{\langle\psi_i| M_m^\dagger M_m |\psi_i\rangle}} \tag{2.144}$$

Thus, after a measurement which yields the result m we have an ensemble of states $|\psi_i^m\rangle$ with respective probabilities $p(i \mid m)$. The corresponding density operator ρ_m is therefore

$$\rho_m = \sum_i p(i \mid m) |\psi_i^m\rangle \langle\psi_i^m| = \sum_i p(i \mid m) \frac{M_m |\psi_i\rangle \langle\psi_i| M_m^\dagger}{\langle\psi_i| M_m^\dagger M_m |\psi_i\rangle}. \tag{2.145}$$

But by elementary probability theory, $p(i \mid m) = p(m,i)/p(m) = p(m \mid i)p_i/p(m)$. Substituting from (2.143) and (2.140) we obtain

$$\rho_m = \sum_i p_i \frac{M_m |\psi_i\rangle \langle\psi_i| M_m^\dagger}{\mathrm{tr}\left(M_m^\dagger M_m \rho\right)} \tag{2.146}$$

$$= \frac{M_m \rho M_m^\dagger}{\mathrm{tr}\left(M_m^\dagger M_m \rho\right)}. \tag{2.147}$$

What we have shown is that the basic postulates of quantum mechanics related to unitary evolution and measurement can be rephrased in the language of density operators. In the next section we complete this rephrasing by giving an intrinsic characterization of the density operator that does not rely on the idea of a state vector.

Before doing so, however, it is useful to introduce some more language, and one more fact about the density operator. First, the language. A quantum system whose state $|\psi\rangle$ is known exactly is said to be in a pure state. In this case the density operator is simply $\rho = |\psi\rangle\langle\psi|$. Otherwise, ρ is in a mixed state; it is said to be a mixture of the different pure states in the ensemble for ρ. In the exercises you will be asked to demonstrate a simple criterion for determining whether a state is pure or mixed: a pure state satisfies $\mathrm{tr}\,(\rho^2) = 1$, while a mixed state satisfies $\mathrm{tr}\,(\rho^2) < 1$. A few words of warning about the nomenclature: sometimes people use the term 'mixed state' as a catch-all to include both pure and mixed quantum states. The origin for this usage seems to be that it implies that the writer is not necessarily assuming that a state is pure. Second, the term 'pure state' is often used in reference to a state vector $|\psi\rangle$, to distinguish it from a density operator ρ.

Finally, imagine a quantum system is prepared in the state ρ_i with probability p_i. It is not difficult to convince yourself that the system may be described by the density matrix $\sum_i p_i \rho_i$. A proof of this is to suppose that ρ_i arises from some ensemble $\{p_{ij}, |\psi_{ij}\rangle\}$ (note that i is fixed) of pure states, so the probability for being in the state $|\psi_{ij}\rangle$ is $p_i p_{ij}$. The density matrix for the system is thus

$$\rho = \sum_{ij} p_i p_{ij} |\psi_{ij}\rangle \langle\psi_{ij}| \tag{2.148}$$

$$= \sum_i p_i \rho_i \tag{2.149}$$

where we have used the definition $\rho_i = \sum_j p_{ij} |\psi_{ij}\rangle \langle\psi_{ij}|$. We say that ρ is a mixture of the states ρ_i with probabilities p_i. This concept of a mixture comes up repeatedly in the analysis of problems like quantum noise, where the effect of the noise is to introduce ignorance into our knowledge of the quantum state. A simple example is provided by the measurement scenario described above. Imagine that, for some reason, our record of the result m of the measurement was lost. We would have a quantum system in the state ρ_m with probability $p(m)$, but would no longer know the actual value of m. The state of
such a quantum system would therefore be described by the density operator

$$\rho = \sum_m p(m)\rho_m \tag{2.150}$$

$$= \sum_m \mathrm{tr}\left(M_m^\dagger M_m \rho\right) \frac{M_m \rho M_m^\dagger}{\mathrm{tr}\left(M_m^\dagger M_m \rho\right)} \tag{2.151}$$

$$= \sum_m M_m \rho M_m^\dagger, \tag{2.152}$$

a nice compact formula which may be used as the starting point for analysis of further operations on the system.

7.2.25 2.4.2 General properties of the density operator

The density operator was introduced as a means of describing ensembles of quantum states. In this section we move away from this description to develop an intrinsic characterization of density operators that does not rely on an ensemble interpretation. This allows us to complete the program of giving a description of quantum mechanics that does not take as its foundation the state vector. We also take the opportunity to develop numerous other elementary properties of the density operator.

The class of operators that are density operators are characterized by the following useful theorem:

Theorem 2.5: (Characterization of density operators) An operator ρ is the density operator associated to some ensemble $\{p_i, |\psi_i\rangle\}$ if and only if it satisfies the conditions:
(1) (Trace condition) ρ has trace equal to one.
(2) (Positivity condition) ρ is a positive operator.

Proof

Suppose $\rho = \sum_i p_i |\psi_i\rangle \langle\psi_i|$ is a density operator. Then

$$\mathrm{tr}(\rho) = \sum_i p_i \,\mathrm{tr}\left(|\psi_i\rangle \langle\psi_i|\right) = \sum_i p_i = 1, \tag{2.153}$$

so the trace condition $\mathrm{tr}(\rho) = 1$ is satisfied. Suppose $|\varphi\rangle$ is an arbitrary vector in state space. Then

$$\langle\varphi|\rho|\varphi\rangle = \sum_i p_i \langle\varphi \mid \psi_i\rangle \langle\psi_i \mid \varphi\rangle \tag{2.154}$$

$$= \sum_i p_i \left|\langle\varphi \mid \psi_i\rangle\right|^2 \tag{2.155}$$

$$\geq 0 \tag{2.156}$$

so the positivity condition is satisfied.
Conversely, suppose ρ is any operator satisfying the trace and positivity conditions. Since ρ is positive, it must have a spectral decomposition

$$\rho = \sum_j \lambda_j |j\rangle\langle j|, \tag{2.157}$$

where the vectors $|j\rangle$ are orthogonal, and λ_j are real, non-negative eigenvalues of ρ.

From the trace condition we see that $\sum_j \lambda_j = 1$. Therefore, a system in state $|j\rangle$ with probability λ_j will have density operator ρ. That is, the ensemble $\{\lambda_j, |j\rangle\}$ is an ensemble of states giving rise to the density operator ρ. $\Box$

This theorem provides a characterization of density operators that is intrinsic to the operator itself: we can define a density operator to be a positive operator ρ which has trace equal to one. Making this definition allows us to reformulate the postulates of quantum mechanics in the density operator picture. For ease of reference we state all the reformulated postulates here:

Postulate 1: Associated to any isolated physical system is a complex vector space with inner product (that is, a Hilbert space) known as the state space of the system. The system is completely described by its density operator, which is a positive operator ρ with trace one, acting on the state space of the system. If a quantum system is in the state ρ_i with probability p_i, then the density operator for the system is $\sum_i p_i \rho_i$.

Postulate 2: The evolution of a closed quantum system is described by a unitary transformation. That is, the state ρ of the system at time t_1 is related to the state ρ' of the system at time t_2 by a unitary operator U which depends only on the times t_1 and t_2,

$$\rho' = U \rho U^\dagger. \tag{2.158}$$

Postulate 3: Quantum measurements are described by a collection $\{M_m\}$ of measurement operators. These are operators acting on the state space of the system being measured. The index m refers to the measurement outcomes that may occur in the experiment. If the state of the quantum system is ρ immediately before the measurement then the probability that result m occurs is given by

$$p(m) = \mathrm{tr}\left(M_m^\dagger M_m \rho\right), \tag{2.159}$$

and the state of the system after the measurement is

$$\frac{M_m \rho M_m^\dagger}{\mathrm{tr}\left(M_m^\dagger M_m \rho\right)}. \tag{2.160}$$

The measurement operators satisfy the completeness equation,

$$\sum_m M_m^\dagger M_m = I. \tag{2.161}$$

Postulate 4: The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. Moreover, if we have systems numbered 1 through n, and system number i is prepared in the state ρ_i, then the joint state of the total system is $\rho_1 \otimes \rho_2 \otimes \ldots \rho_n$.

These reformulations of the fundamental postulates of quantum mechanics in terms of the density operator are, of course, mathematically equivalent to the description in terms of the state vector. Nevertheless, as a way of thinking about quantum mechanics, the density operator approach really shines for two applications: the description of quantum systems whose state is not known, and the description of subsystems of a composite
quantum system, as will be described in the next section. For the remainder of this section we flesh out the properties of the density matrix in more detail.

Exercise 2.71: (Criterion to decide if a state is mixed or pure) Let ρ be a density operator. Show that $\mathrm{tr}\left(\rho^2\right) \leq 1$, with equality if and only if ρ is a pure state.

It is a tempting (and surprisingly common) fallacy to suppose that the eigenvalues and eigenvectors of a density matrix have some special significance with regard to the ensemble of quantum states represented by that density matrix. For example, one might suppose that a quantum system with density matrix

$$\rho = \frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|. \tag{2.162}$$

must be in the state $|0\rangle$ with probability 3/4 and in the state $|1\rangle$ with probability 1/4. However, this is not necessarily the case. Suppose we define

$$|a\rangle \equiv \sqrt{\frac{3}{4}}|0\rangle + \sqrt{\frac{1}{4}}|1\rangle \tag{2.163}$$

$$|b\rangle \equiv \sqrt{\frac{3}{4}}|0\rangle - \sqrt{\frac{1}{4}}|1\rangle, \tag{2.164}$$

and the quantum system is prepared in the state $|a\rangle$ with probability 1/2 and in the state $|b\rangle$ with probability 1/2. Then it is easily checked that the corresponding density matrix is

$$\rho = \frac{1}{2}|a\rangle\langle a| + \frac{1}{2}|b\rangle\langle b| = \frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|. \tag{2.165}$$

That is, these two different ensembles of quantum states give rise to the same density matrix. In general, the eigenvectors and eigenvalues of a density matrix just indicate one of many possible ensembles that may give rise to a specific density matrix, and there is no reason to suppose it is an especially privileged ensemble.

A natural question to ask in the light of this discussion is what class of ensembles does give rise to a particular density matrix? The solution to this problem, which we now give, has surprisingly many applications in quantum computation and quantum information, notably in the understanding of quantum noise and quantum error-correction (Chapters 8 and 10). For the solution it is convenient to make use of vectors $\left|\tilde{\psi}_i\right\rangle$ which may not be normalized to unit length. We say the set $\left|\tilde{\psi}_i\right\rangle$ generates the operator $\rho \equiv \sum_i \left|\tilde{\psi}_i\right\rangle \left\langle\tilde{\psi}_i\right|$, and thus the connection to the usual ensemble picture of density operators is expressed by the equation $\left|\tilde{\psi}_i\right\rangle = \sqrt{p_i}\,|\psi_i\rangle$. When do two sets of vectors, $\left|\tilde{\psi}_i\right\rangle$ and $|\tilde{\varphi}_j\rangle$ generate the same operator ρ ? The solution to this problem will enable us to answer the question of what ensembles give rise to a given density matrix.

Theorem 2.6: (Unitary freedom in the ensemble for density matrices) The sets $\left|\tilde{\psi}_i\right\rangle$ and $|\tilde{\varphi}_j\rangle$ generate the same density matrix if and only if

$$\left|\tilde{\psi}_i\right\rangle = \sum_j u_{ij}\,|\tilde{\varphi}_j\rangle\,, \tag{2.166}$$

where u_{ij} is a unitary matrix of complex numbers, with indices i and j, and we 'pad' whichever set of vectors $\left|\tilde{\psi}_i\right\rangle$ or $|\tilde{\varphi}_j\rangle$ is smaller with additional vectors 0 so that the two sets have the same number of elements.

As a consequence of the theorem, note that $\rho = \sum_i p_i\,|\psi_i\rangle\,\langle\psi_i| = \sum_j q_j\,|\varphi_j\rangle\,\langle\varphi_j|$ for normalized states $|\psi_i\rangle\,, |\varphi_j\rangle$ and probability distributions p_i and q_j if and only if

$$\sqrt{p_i}\,|\psi_i\rangle = \sum_j u_{ij}\sqrt{q_j}\,|\varphi_j\rangle\,, \tag{2.167}$$

for some unitary matrix u_{ij}, and we may pad the smaller ensemble with entries having probability zero in order to make the two ensembles the same size. Thus, Theorem 2.6 characterizes the freedom in ensembles $\{p_i, |\psi_i\rangle\}$ giving rise to a given density matrix ρ. Indeed, it is easily checked that our earlier example of a density matrix with two different decompositions, (2.162), arises as a special case of this general result. Let's turn now to the proof of the theorem.

Proof

Suppose $\left|\tilde{\psi}_i\right\rangle = \sum_j u_{ij} \left|\tilde{\varphi}_j\right\rangle$ for some unitary u_{ij}. Then

$$\sum_i \left|\tilde{\psi}_i\right\rangle \left\langle\tilde{\psi}_i\right| = \sum_{ijk} u_{ij} u_{ik}^* \left|\tilde{\varphi}_j\right\rangle \left\langle\tilde{\varphi}_k\right| \tag{2.168}$$

$$= \sum_{jk} \left(\sum_i u_{ki}^\dagger u_{ij} \right) \left|\tilde{\varphi}_j\right\rangle \left\langle\tilde{\varphi}_k\right| \tag{2.169}$$

$$= \sum_{jk} \delta_{kj} \left|\tilde{\varphi}_j\right\rangle \left\langle\tilde{\varphi}_k\right| \tag{2.170}$$

$$= \sum_j \left|\tilde{\varphi}_j\right\rangle \left\langle\tilde{\varphi}_j\right|, \tag{2.171}$$

which shows that $\left|\tilde{\psi}_i\right\rangle$ and $\left|\tilde{\varphi}_j\right\rangle$ generate the same operator.
Conversely, suppose

$$A = \sum_i \left|\tilde{\psi}_i\right\rangle \left\langle\tilde{\psi}_i\right| = \sum_j \left|\tilde{\varphi}_j\right\rangle \left\langle\tilde{\varphi}_j\right|. \tag{2.172}$$

Let $A = \sum_k \lambda_k |k\rangle\langle k|$ be a decomposition for A such that the states $|k\rangle$ are orthonormal, and the λ_k are strictly positive. Our strategy is to relate the states $\left|\tilde{\psi}_i\right\rangle$ to the states $|\tilde{k}\rangle \equiv \sqrt{\lambda_k}|k\rangle$, and similarly relate the states $\left|\tilde{\varphi}_j\right\rangle$ to the states $|\tilde{k}\rangle$. Combining the two relations will give the result. Let $|\psi\rangle$ be any vector orthonormal to the space spanned by the $|\tilde{k}\rangle$, so $\langle\psi \mid \tilde{k}\rangle\langle\tilde{k} \mid \psi\rangle = 0$ for all k, and thus we see that

$$0 = \langle\psi|A|\psi\rangle = \sum_i \left\langle\psi \mid \tilde{\psi}_i\right\rangle \left\langle\tilde{\psi}_i \mid \psi\right\rangle = \sum_i \left|\left\langle\psi \mid \tilde{\psi}_i\right\rangle\right|^2. \tag{2.173}$$

Thus $\left\langle\psi \mid \tilde{\psi}_i\right\rangle = 0$ for all i and all $|\psi\rangle$ orthonormal to the space spanned by the $|\tilde{k}\rangle$. It follows that each $\left|\tilde{\psi}_i\right\rangle$ can be expressed as a linear combination of the $|\tilde{k}\rangle$, $\left|\tilde{\psi}_i\right\rangle = \sum_k c_{ik}|\tilde{k}\rangle$. Since $A = \sum_k |\tilde{k}\rangle\langle\tilde{k}| = \sum_i \left|\tilde{\psi}_i\right\rangle \left\langle\tilde{\psi}_i\right|$ we see that

$$\sum_k |\tilde{k}\rangle\langle\tilde{k}| = \sum_{kl} \left(\sum_i c_{ik} c_{il}^* \right) |\tilde{k}\rangle\langle\tilde{l}|. \tag{2.174}$$

The operators $|\tilde{k}\rangle\langle\tilde{l}|$ are easily seen to be linearly independent, and thus it must be that $\sum_i c_{ik} c_{il}^* = \delta_{kl}$. This ensures that we may append extra columns to c to obtain a unitary matrix v such that $\left|\tilde{\psi}_i\right\rangle = \sum_k v_{ik}|\tilde{k}\rangle$, where we have appended zero vectors to the list of $|\tilde{k}\rangle$. Similarly, we can find a unitary matrix w such that $|\tilde{\varphi}_j\rangle = \sum_k w_{jk}|\tilde{k}\rangle$. Thus $\left|\tilde{\psi}_i\right\rangle = \sum_j u_{ij} \left|\tilde{\varphi}_j\right\rangle$, where $u = vw^\dagger$ is unitary.

Exercise 2.72: (Bloch sphere for mixed states) The Bloch sphere picture for pure states of a single qubit was introduced in Section 1.2. This description has an important generalization to mixed states as follows.
(1) Show that an arbitrary density matrix for a mixed state qubit may be written as

$$\rho = \frac{I + \vec{r} \cdot \vec{\sigma}}{2}, \tag{2.175}$$

where $\vec{r}$ is a real three-dimensional vector such that $\|\vec{r}\| \leq 1$. This vector is known as the Bloch vector for the state ρ.
(2) What is the Bloch vector representation for the state $\rho = I/2$?
(3) Show that a state ρ is pure if and only if $\|\vec{r}\| = 1$.
(4) Show that for pure states the description of the Bloch vector we have given coincides with that in Section 1.2.

Exercise 2.73: Let ρ be a density operator. A minimal ensemble for ρ is an ensemble $\{p_i, |\psi_i\rangle\}$ containing a number of elements equal to the rank of ρ. Let $|\psi\rangle$ be any state in the support of ρ. (The support of a Hermitian operator A is the vector space spanned by the eigenvectors of A with non-zero eigenvalues.) Show that there is a minimal ensemble for ρ that contains $|\psi\rangle$, and moreover that in any such ensemble $|\psi\rangle$ must appear with probability

$$p_i = \frac{1}{\langle\psi_i| \rho^{-1} |\psi_i\rangle}, \tag{2.176}$$

where ρ^{-1} is defined to be the inverse of ρ, when ρ is considered as an operator acting only on the support of ρ. (This definition removes the problem that ρ may not have an inverse.)

7.2.26 2.4.3 The reduced density operator

Perhaps the deepest application of the density operator is as a descriptive tool for subsystems of a composite quantum system. Such a description is provided by the reduced density operator, which is the subject of this section. The reduced density operator is so useful as to be virtually indispensable in the analysis of composite quantum systems.

Suppose we have physical systems A and B, whose state is described by a density operator ρ^{AB}. The reduced density operator for system A is defined by

$$\rho^A \equiv \mathrm{tr}_B \left(\rho^{AB}\right), \tag{2.177}$$

where tr_B is a map of operators known as the partial trace over system B. The partial trace is defined by

$$\mathrm{tr}_B \left(|a_1\rangle \langle a_2| \otimes |b_1\rangle \langle b_2|\right) \equiv |a_1\rangle \langle a_2| \, \mathrm{tr} \left(|b_1\rangle \langle b_2|\right), \tag{2.178}$$

where $|a_1\rangle$ and $|a_2\rangle$ are any two vectors in the state space of A, and $|b_1\rangle$ and $|b_2\rangle$ are any two vectors in the state space of B. The trace operation appearing on the right hand side is the usual trace operation for system B, so $\mathrm{tr} \left(|b_1\rangle \langle b_2|\right) = \langle b_2 \mid b_1\rangle$. We have defined the partial trace operation only on a special subclass of operators on AB; the specification is completed by requiring in addition to Equation (2.178) that the partial trace be linear in its input.

It is not obvious that the reduced density operator for system A is in any sense a description for the state of system A. The physical justification for making this identification is that the reduced density operator provides the correct measurement statistics for measurements made on system A. This is explained in more detail in Box 2.6 on page 107. The following simple example calculations may also help understand the reduced density operator. First, suppose a quantum system is in the product state $\rho^{AB} = \rho \otimes \sigma$, where ρ is a density operator for system A, and σ is a density operator for system B. Then

$$\rho^A = \mathrm{tr}_B(\rho \otimes \sigma) = \rho \, \mathrm{tr}(\sigma) = \rho, \tag{2.184}$$

which is the result we intuitively expect. Similarly, $\rho^B = \sigma$ for this state. A less trivial example is the Bell state $(|00\rangle + |11\rangle)/\sqrt{2}$. This has density operator

$$\rho = \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right)\left(\frac{\langle 00| + \langle 11|}{\sqrt{2}}\right) \tag{2.185}$$

$$= \frac{|00\rangle\langle 00| + |11\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 11|}{2}. \tag{2.186}$$

Tracing out the second qubit, we find the reduced density operator of the first qubit,

$$\rho^1 = \mathrm{tr}_2(\rho) \tag{2.187}$$

$$= \frac{\mathrm{tr}_2(|00\rangle\langle 00|) + \mathrm{tr}_2(|11\rangle\langle 00|) + \mathrm{tr}_2(|00\rangle\langle 11|) + \mathrm{tr}_2(|11\rangle\langle 11|)}{2} \tag{2.188}$$

$$= \frac{|0\rangle\langle 0|\langle 0 \mid 0\rangle + |1\rangle\langle 0|\langle 0 \mid 1\rangle + |0\rangle\langle 1|\langle 1 \mid 0\rangle + |1\rangle\langle 1|\langle 1 \mid 1\rangle}{2} \tag{2.189}$$

$$= \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} \tag{2.190}$$

$$= \frac{I}{2} \tag{2.191}$$

Notice that this state is a mixed state, since $\mathrm{tr}\left((I/2)^2\right) = 1/2 < 1$. This is quite a remarkable result. The state of the joint system of two qubits is a pure state, that is, it is known exactly; however, the first qubit is in a mixed state, that is, a state about which we apparently do not have maximal knowledge. This strange property, that the joint state of a system can be completely known, yet a subsystem be in mixed states, is another hallmark of quantum entanglement.

Exercise 2.74: Suppose a composite of systems A and B is in the state $|a\rangle|b\rangle$, where $|a\rangle$ is a pure state of system A, and $|b\rangle$ is a pure state of system B. Show that the reduced density operator of system A alone is a pure state.

Exercise 2.75: For each of the four Bell states, find the reduced density operator for each qubit.

Quantum teleportation and the reduced density operator

A useful application of the reduced density operator is to the analysis of quantum teleportation. Recall from Section 1.3.7 that quantum teleportation is a procedure for sending

Box 2.6: Why the partial trace?

Why is the partial trace used to describe part of a larger quantum system? The reason for doing this is because the partial trace operation is the unique operation which gives rise to the correct description of observable quantities for subsystems of a composite system, in the following sense.

Suppose M is any observable on system A, and we have some measuring device which is capable of realizing measurements of M. Let $\tilde{M}$ denote the corresponding observable for the same measurement, performed on the composite system AB. Our immediate goal is to argue that $\tilde{M}$ is necessarily equal to $M \otimes I_B$. Note that if the system AB is prepared in the state $|m\rangle|\psi\rangle$, where $|m\rangle$ is an eigenstate of M with eigenvalue m, and $|\psi\rangle$ is any state of B, then the measuring device must yield the result m for the measurement, with probability one. Thus, if P_m is the projector onto the m eigenspace of the observable M, then the corresponding projector for $\tilde{M}$ is $P_m \otimes I_B$. We therefore have

$$\tilde{M} = \sum_m m P_m \otimes I_B = M \otimes I_B \tag{2.179}$$

The next step is to show that the partial trace procedure gives the correct measurement statistics for observations on part of a system. Suppose we perform a measurement on system A described by the observable M. Physical consistency requires that any prescription for associating a 'state', ρ^A, to system A, must have the property that measurement averages be the same whether computed via ρ^A or ρ^{AB},

$$\mathrm{tr}\left(M\rho^A\right) = \mathrm{tr}\left(\tilde{M}\rho^{AB}\right) = \mathrm{tr}\left(\left(M \otimes I_B\right)\rho^{AB}\right) \tag{2.180}$$

This equation is certainly satisfied if we choose $\rho^A \equiv \mathrm{tr}_B\left(\rho^{AB}\right)$. In fact, the partial trace turns out to be the unique function having this property. To see this uniqueness property, let $f(\cdot)$ be any map of density operators on AB to density operators on A such that

$$\mathrm{tr}\left(Mf\left(\rho^{AB}\right)\right) = \mathrm{tr}\left(\left(M \otimes I_B\right)\rho^{AB}\right), \tag{2.181}$$

for all observables M. Let M_i be an orthonormal basis of operators for the space of Hermitian operators with respect to the Hilbert-Schmidt inner product $(X, Y) \equiv \mathrm{tr}(XY)$ (compare Exercise 2.39 on page 76). Then expanding $f\left(\rho^{AB}\right)$ in this basis gives

$$f\left(\rho^{AB}\right) = \sum_i M_i \,\mathrm{tr}\left(M_i f\left(\rho^{AB}\right)\right) \tag{2.182}$$

$$= \sum_i M_i \,\mathrm{tr}\left(\left(M_i \otimes I_B\right)\rho^{AB}\right). \tag{2.183}$$

It follows that f is uniquely determined by Equation (2.180). Moreover, the partial trace satisfies (2.180), so it is the unique function having this property.
quantum information from Alice to Bob, given that Alice and Bob share an EPR pair, and have a classical communications channel.

At first sight it appears as though teleportation can be used to do faster than light communication, a big no-no according to the theory of relativity. We surmised in Section 1.3.7 that what prevents faster than light communication is the need for Alice to communicate her measurement result to Bob. The reduced density operator allows us to make this rigorous.

Recall that immediately before Alice makes her measurement the quantum state of the three qubits is (Equation (1.32)):

$$\begin{aligned}|\psi_2\rangle = \frac{1}{2}[&|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) \\ &+ |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)].\end{aligned} \tag{2.192}$$

Measuring in Alice's computational basis, the state of the system after the measurement is:

$$|00\rangle[\alpha|0\rangle + \beta|1\rangle] \text{ with probability } \frac{1}{4} \tag{2.193}$$

$$|01\rangle[\alpha|1\rangle + \beta|0\rangle] \text{ with probability } \frac{1}{4} \tag{2.194}$$

$$|10\rangle[\alpha|0\rangle - \beta|1\rangle] \text{ with probability } \frac{1}{4} \tag{2.195}$$

$$|11\rangle[\alpha|1\rangle - \beta|0\rangle] \text{ with probability } \frac{1}{4}. \tag{2.196}$$

The density operator of the system is thus

$$\begin{aligned}\rho =& \frac{1}{4}\left[|00\rangle\langle 00|(\alpha|0\rangle+\beta|1\rangle)\left(\alpha^*\langle 0|+\beta^*\langle 1|\right)+|01\rangle\langle 01|(\alpha|1\rangle+\beta|0\rangle)\left(\alpha^*\langle 1|+\beta^*\langle 0|\right)\right.\\ &\left.+|10\rangle\langle 10|(\alpha|0\rangle-\beta|1\rangle)\left(\alpha^*\langle 0|-\beta^*\langle 1|\right)+|11\rangle\langle 11|(\alpha|1\rangle-\beta|0\rangle)\left(\alpha^*\langle 1|-\beta^*\langle 0|\right)\right]. \quad (2.197)\end{aligned}$$

Tracing out Alice's system, we see that the reduced density operator of Bob's system is

$$\begin{aligned}\rho^B =& \frac{1}{4}\left[(\alpha|0\rangle+\beta|1\rangle)\left(\alpha^*\langle 0|+\beta^*\langle 1|\right)+(\alpha|1\rangle+\beta|0\rangle)\left(\alpha^*\langle 1|+\beta^*\langle 0|\right)\right.\\ &\left.+(\alpha|0\rangle-\beta|1\rangle)\left(\alpha^*\langle 0|-\beta^*\langle 1|\right)+(\alpha|1\rangle-\beta|0\rangle)\left(\alpha^*\langle 1|-\beta^*\langle 0|\right)\right] \quad (2.198)\\ =& \frac{2\left(|\alpha|^2+|\beta|^2\right)|0\rangle\langle 0|+2\left(|\alpha|^2+|\beta|^2\right)|1\rangle\langle 1|}{4} \quad (2.199)\\ =& \frac{|0\rangle\langle 0|+|1\rangle\langle 1|}{2} \quad (2.200)\\ =& \frac{I}{2} \quad (2.201)\end{aligned}$$

where we have used the completeness relation in the last line. Thus, the state of Bob's system after Alice has performed the measurement but before Bob has learned the measurement result is $I/2$. This state has no dependence upon the state $|\psi\rangle$ being teleported, and thus any measurements performed by Bob will contain no information about $|\psi\rangle$, thus preventing Alice from using teleportation to transmit information to Bob faster than light.

7.2.27 2.5 The Schmidt decomposition and purifications

Density operators and the partial trace are just the beginning of a wide array of tools useful for the study of composite quantum systems, which are at the heart of quantum computation and quantum information. Two additional tools of great value are the Schmidt decomposition and purifications. In this section we present both these tools, and try to give the flavor of their power.

Theorem 2.7: (Schmidt decomposition) Suppose $|\psi\rangle$ is a pure state of a composite system, AB. Then there exist orthonormal states $|i_A\rangle$ for system A, and orthonormal states $|i_B\rangle$ of system B such that

$$|\psi\rangle = \sum_i \lambda_i |i_A\rangle |i_B\rangle, \quad (2.202)$$

where λ_i are non-negative real numbers satisfying $\sum_i \lambda_i^2 = 1$ known as Schmidt co-efficients.

This result is very useful. As a taste of its power, consider the following consequence: let $|\psi\rangle$ be a pure state of a composite system, AB. Then by the Schmidt decomposition $\rho^A = \sum_i \lambda_i^2 |i_A\rangle\langle i_A|$ and $\rho^B = \sum_i \lambda_i^2 |i_B\rangle\langle i_B|$, so the eigenvalues of ρ^A and ρ^B are identical, namely λ_i^2 for both density operators. Many important properties of quantum systems are completely determined by the eigenvalues of the reduced density operator of the system, so for a pure state of a composite system such properties will be the same for both systems. As an example, consider the state of two qubits, $(|00\rangle+|01\rangle+|11\rangle)/\sqrt{3}$. This has no obvious symmetry property, yet if you calculate $\mathrm{tr}\left(\left(\rho^A\right)^2\right)$ and $\mathrm{tr}\left(\left(\rho^B\right)^2\right)$ you will discover that they have the same value, $7/9$ in each case. This is but one small consequence of the Schmidt decomposition.

Proof

We give the proof for the case where systems A and B have state spaces of the same dimension, and leave the general case to Exercise 2.76. Let $|j\rangle$ and $|k\rangle$ be any fixed orthonormal bases for systems A and B, respectively. Then $|\psi\rangle$ can be written

$$|\psi\rangle = \sum_{jk} a_{jk}|j\rangle|k\rangle, \tag{2.203}$$

for some matrix a of complex numbers a_{jk}. By the singular value decomposition, $a = udv$, where d is a diagonal matrix with non-negative elements, and u and v are unitary matrices. Thus

$$|\psi\rangle = \sum_{ijk} u_{ji} d_{ii} v_{ik}|j\rangle|k\rangle. \tag{2.204}$$

Defining $|i_A\rangle \equiv \sum_j u_{ji}|j\rangle$, $|i_B\rangle \equiv \sum_k v_{ik}|k\rangle$, and $\lambda_i \equiv d_{ii}$, we see that this gives

$$|\psi\rangle = \sum_i \lambda_i \, |i_A\rangle \, |i_B\rangle \, . \tag{2.205}$$

It is easy to check that $|i_A\rangle$ forms an orthonormal set, from the unitarity of u and the orthonormality of $|j\rangle$, and similarly that the $|i_B\rangle$ form an orthonormal set.

Exercise 2.76: Extend the proof of the Schmidt decomposition to the case where A and B may have state spaces of different dimensionality.

Exercise 2.77: Suppose ABC is a three component quantum system. Show by example that there are quantum states $|\psi\rangle$ of such systems which can not be written in the form

$$|\psi\rangle = \sum_i \lambda_i \, |i_A\rangle \, |i_B\rangle \, |i_C\rangle \, , \tag{2.206}$$

where λ_i are real numbers, and $|i_A\rangle \, , |i_B\rangle \, , |i_C\rangle$ are orthonormal bases of the respective systems.

The bases $|i_A\rangle$ and $|i_B\rangle$ are called the Schmidt bases for A and B, respectively, and the number of non-zero values λ_i is called the Schmidt number for the state $|\psi\rangle$. The Schmidt number is an important property of a composite quantum system, which in some sense quantifies the 'amount' of entanglement between systems A and B. To get some idea of why this is the case, consider the following obvious but important property: the Schmidt number is preserved under unitary transformations on system A or system B alone. To see this, notice that if $\sum_i \lambda_i \, |i_A\rangle \, |i_B\rangle$ is the Schmidt decomposition for $|\psi\rangle$ then $\sum_i \lambda_i \, (U \, |i_A\rangle) \, |i_B\rangle$ is the Schmidt decomposition for $U|\psi\rangle$, where U is a unitary operator acting on system A alone. Algebraic invariance properties of this type make the Schmidt number a very useful tool.

Exercise 2.78: Prove that a state $|\psi\rangle$ of a composite system AB is a product state if and only if it has Schmidt number 1. Prove that $|\psi\rangle$ is a product state if and only if ρ^A (and thus ρ^B) are pure states.

A second, related technique for quantum computation and quantum information is purification. Suppose we are given a state ρ^A of a quantum system A. It is possible to introduce another system, which we denote R, and define a pure state $|AR\rangle$ for the joint system AR such that $\rho^A = \mathrm{tr}_R(|AR\rangle\langle AR|)$. That is, the pure state $|AR\rangle$ reduces to ρ^A when we look at system A alone. This is a purely mathematical procedure, known as purification, which allows us to associate pure states with mixed states. For this reason we call system R a reference system: it is a fictitious system, without a direct physical significance.

To prove that purification can be done for any state, we explain how to construct a system R and purification $|AR\rangle$ for ρ^A. Suppose ρ^A has orthonormal decomposition $\rho^A = \sum_i p_i \left|i^A\right\rangle \left\langle i^A\right|$.

To purify ρ^A we introduce a system R which has the same state space as system A, with orthonormal basis states $\left|i^R\right\rangle$, and define a pure state for the combined system

$$|AR\rangle \equiv \sum_i \sqrt{p_i} \left|i^A\right\rangle \left|i^R\right\rangle. \tag{2.207}$$

We now calculate the reduced density operator for system A corresponding to the state $|AR\rangle$:

$$\mathrm{tr}_R(|AR\rangle\langle AR|) = \sum_{ij} \sqrt{p_i p_j} \left|i^A\right\rangle \left\langle j^A\right| \mathrm{tr}\left(\left|i^R\right\rangle \left\langle j^R\right|\right) \tag{2.208}$$

$$= \sum_{ij} \sqrt{p_i p_j} \left|i^A\right\rangle \left\langle j^A\right| \delta_{ij} \tag{2.209}$$

$$= \sum_i p_i \left|i^A\right\rangle \left\langle i^A\right| \tag{2.210}$$

$$= \rho^A. \tag{2.211}$$

Thus $|AR\rangle$ is a purification of ρ^A.

Notice the close relationship of the Schmidt decomposition to purification: the procedure used to purify a mixed state of system A is to define a pure state whose Schmidt basis for system A is just the basis in which the mixed state is diagonal, with the Schmidt coefficients being the square root of the eigenvalues of the density operator being purified.

In this section we've explained two tools for studying composite quantum systems, the Schmidt decomposition and purifications. These tools will be indispensable to the study of quantum computation and quantum information, especially quantum information, which is the subject of Part III of this book.

Exercise 2.79: Consider a composite system consisting of two qubits. Find the Schmidt decompositions of the states

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}; \quad \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2}; \text{ and } \frac{|00\rangle + |01\rangle + |10\rangle}{\sqrt{3}}. \tag{2.212}$$

Exercise 2.80: Suppose $|\psi\rangle$ and $|\varphi\rangle$ are two pure states of a composite quantum system with components A and B, with identical Schmidt coefficients. Show that there are unitary transformations U on system A and V on system B such that $|\psi\rangle = (U \otimes V)|\varphi\rangle$.

Exercise 2.81: (Freedom in purifications) Let $|AR_1\rangle$ and $|AR_2\rangle$ be two purifications of a state ρ^A to a composite system AR. Prove that there exists a unitary transformation U_R acting on system R such that $|AR_1\rangle = (I_A \otimes U_R)\,|AR_2\rangle$.

Exercise 2.82: Suppose $\{p_i, |\psi_i\rangle\}$ is an ensemble of states generating a density matrix $\rho = \sum_i p_i \,|\psi_i\rangle\,\langle\psi_i|$ for a quantum system A. Introduce a system R with orthonormal basis $|i\rangle$.

(1) Show that $\sum_i \sqrt{p_i}\,|\psi_i\rangle\,|i\rangle$ is a purification of ρ.

(2) Suppose we measure R in the basis $|i\rangle$, obtaining outcome i. With what probability do we obtain the result i, and what is the corresponding state of system A ?

(3) Let $|AR\rangle$ be any purification of ρ to the system AR. Show that there exists an orthonormal basis $|i\rangle$ in which R can be measured such that the corresponding post-measurement state for system A is $|\psi_i\rangle$ with probability p_i.

7.2.28 2.6 EPR and the Bell inequality

Anybody who is not shocked by quantum theory has not understood it.

- Niels Bohr

\begin{abstract}
I recall that during one walk Einstein suddenly stopped, turned to me and asked whether I really believed that the moon exists only when I look at it. The rest of this walk was devoted to a discussion of what a physicist should mean by the term 'to exist'.
- Abraham Pais
\end{abstract}

> ...quantum phenomena do not occur in a Hilbert space, they occur in a laboratory.
>
> - Asher Peres
>
> ...what is proved by impossibility proofs is lack of imagination.
>
> - John Bell

This chapter has focused on introducing the tools and mathematics of quantum mechanics. As these techniques are applied in the following chapters of this book, an important recurring theme is the unusual, non-classical properties of quantum mechanics. But what exactly is the difference between quantum mechanics and the classical world? Understanding this difference is vital in learning how to perform information processing tasks that are difficult or impossible with classical physics. This section concludes the chapter with a discussion of the Bell inequality, a compelling example of an essential difference between quantum and classical physics.

When we speak of an object such as a person or a book, we assume that the physical properties of that object have an existence independent of observation. That is, measurements merely act to reveal such physical properties. For example, a tennis ball has as one of its physical properties its position, which we typically measure using light scattered from the surface of the ball. As quantum mechanics was being developed in the 1920s and 1930s a strange point of view arose that differs markedly from the classical view. As described earlier in the chapter, according to quantum mechanics, an unobserved particle does not possess physical properties that exist independent of observation. Rather, such physical properties arise as a consequence of measurements performed upon the system. For example, according to quantum mechanics a qubit does not possess definite properties of 'spin in the z direction, σ_z ', and 'spin in the x direction, σ_x ', each of which can be revealed by performing the appropriate measurement. Rather, quantum mechanics gives a set of rules which specify, given the state vector, the probabilities for the possible measurement outcomes when the observable σ_z is measured, or when the observable σ_x is measured.

Many physicists rejected this new view of Nature. The most prominent objector was Albert Einstein. In the famous 'EPR paper', co-authored with Nathan Rosen and Boris Podolsky, Einstein proposed a thought experiment which, he believed, demonstrated that quantum mechanics is not a complete theory of Nature.

The essence of the EPR argument is as follows. EPR were interested in what they termed 'elements of reality'. Their belief was that any such element of reality must be represented in any complete physical theory. The goal of the argument was to show that quantum mechanics is not a complete physical theory, by identifying elements of reality that were not included in quantum mechanics. The way they attempted to do this was by introducing what they claimed was a sufficient condition for a physical property to
be an element of reality, namely, that it be possible to predict with certainty the value that property will have, immediately before measurement.

Box 2.7: Anti-correlations in the EPR experiment

Suppose we prepare the two qubit state

$$|\psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}, \tag{2.213}$$

a state sometimes known as the spin singlet for historical reasons. It is not difficult to show that this state is an entangled state of the two qubit system. Suppose we perform a measurement of spin along the $\vec{v}$ axis on both qubits, that is, we measure the observable $\vec{v} \cdot \vec{\sigma}$ (defined in Equation (2.116) on page 90) on each qubit, getting a result of $+1$ or -1 for each qubit. It turns out that no matter what choice of $\vec{v}$ we make, the results of the two measurements are always opposite to one another. That is, if the measurement on the first qubit yields $+1$, then the measurement on the second qubit will yield -1 , and vice versa. It is as though the second qubit knows the result of the measurement on the first, no matter how the first qubit is measured. To see why this is true, suppose $|a\rangle$ and $|b\rangle$ are the eigenstates of $\vec{v} \cdot \vec{\sigma}$. Then there exist complex numbers $\alpha, \beta, \gamma, \delta$ such that

$$|0\rangle = \alpha|a\rangle + \beta|b\rangle \tag{2.214}$$
$$|1\rangle = \gamma|a\rangle + \delta|b\rangle. \tag{2.215}$$

Substituting we obtain

$$\frac{|01\rangle - |10\rangle}{\sqrt{2}} = (\alpha\delta - \beta\gamma)\frac{|ab\rangle - |ba\rangle}{\sqrt{2}}. \tag{2.216}$$

But $\alpha\delta - \beta\gamma$ is the determinant of the unitary matrix $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$, and thus is equal to a phase factor $e^{i\theta}$ for some real θ. Thus

$$\frac{|01\rangle - |10\rangle}{\sqrt{2}} = \frac{|ab\rangle - |ba\rangle}{\sqrt{2}}, \tag{2.217}$$

up to an unobservable global phase factor. As a result, if a measurement of $\vec{v}\cdot\vec{\sigma}$ is performed on both qubits, then we can see that a result of $+1(-1)$ on the first qubit implies a result of $-1(+1)$ on the second qubit.

Consider, for example, an entangled pair of qubits belonging to Alice and Bob, respectively:

$$\frac{|01\rangle - |10\rangle}{\sqrt{2}}. \tag{2.218}$$

Suppose Alice and Bob are a long way away from one another. Alice performs a measurement of spin along the $\vec{v}$ axis, that is, she measures the observable $\vec{v}\cdot\vec{\sigma}$ (defined in Equation (2.116) on page 90). Suppose Alice receives the result $+1$. Then a simple quantum mechanical calculation, given in Box 2.7, shows that she can predict with certainty
that Bob will measure -1 on his qubit if he also measures spin along the $\vec{v}$ axis. Similarly, if Alice measured -1 , then she can predict with certainty that Bob will measure $+1$ on his qubit. Because it is always possible for Alice to predict the value of the measurement result recorded when Bob's qubit is measured in the $\vec{v}$ direction, that physical property must correspond to an element of reality, by the EPR criterion, and should be represented in any complete physical theory. However, standard quantum mechanics, as we have presented it, merely tells one how to calculate the probabilities of the respective measurement outcomes if $\vec{v} \cdot \vec{\sigma}$ is measured. Standard quantum mechanics certainly does not include any fundamental element intended to represent the value of $\vec{v} \cdot \vec{\sigma}$, for all unit vectors $\vec{v}$.

The goal of EPR was to show that quantum mechanics is incomplete, by demonstrating that quantum mechanics lacked some essential 'element of reality', by their criterion. They hoped to force a return to a more classical view of the world, one in which systems could be ascribed properties which existed independently of measurements performed on those systems. Unfortunately for EPR, most physicists did not accept the above reasoning as convincing. The attempt to impose on Nature by fiat properties which she must obey seems a most peculiar way of studying her laws.

Indeed, Nature has had the last laugh on EPR. Nearly thirty years after the EPR paper was published, an experimental test was proposed that could be used to check whether or not the picture of the world which EPR were hoping to force a return to is valid or not. It turns out that Nature experimentally invalidates that point of view, while agreeing with quantum mechanics.

The key to this experimental invalidation is a result known as Bell's inequality. Bell's inequality is not a result about quantum mechanics, so the first thing we need to do is momentarily forget all our knowledge of quantum mechanics. To obtain Bell's inequality, we're going to do a thought experiment, which we will analyze using our common sense notions of how the world works - the sort of notions Einstein and his collaborators thought Nature ought to obey. After we have done the common sense analysis, we will perform a quantum mechanical analysis which we can show is not consistent with the common sense analysis. Nature can then be asked, by means of a real experiment, to decide between our common sense notions of how the world works, and quantum mechanics.

Imagine we perform the following experiment, illustrated in Figure 2.4. Charlie prepares two particles. It doesn't matter how he prepares the particles, just that he is capable of repeating the experimental procedure which he uses. Once he has performed the preparation, he sends one particle to Alice, and the second particle to Bob.

Once Alice receives her particle, she performs a measurement on it. Imagine that she has available two different measurement apparatuses, so she could choose to do one of two different measurements. These measurements are of physical properties which we shall label P_Q and P_R, respectively. Alice doesn't know in advance which measurement she will choose to perform. Rather, when she receives the particle she flips a coin or uses some other random method to decide which measurement to perform. We suppose for simplicity that the measurements can each have one of two outcomes, +1 or -1 . Suppose Alice's particle has a value Q for the property P_Q.Q is assumed to be an objective property of Alice's particle, which is merely revealed by the measurement, much as we imagine the position of a tennis ball to be revealed by the particles of light being scattered off it. Similarly, let R denote the value revealed by a measurement of the property P_R.

Similarly, suppose that Bob is capable of measuring one of two properties, P_S or P_T, once again revealing an objectively existing value S or T for the property, each taking value +1 or -1 . Bob does not decide beforehand which property he will measure, but waits until he has received the particle and then chooses randomly. The timing of the experiment is arranged so that Alice and Bob do their measurements at the same time (or, to use the more precise language of relativity, in a causally disconnected manner). Therefore, the measurement which Alice performs cannot disturb the result of Bob's measurement (or vice versa), since physical influences cannot propagate faster than light.

Figure 2.4. Schematic experimental setup for the Bell inequalities. Alice can choose to measure either Q or R, and Bob chooses to measure either S or T. They perform their measurements simultaneously. Alice and Bob are assumed to be far enough apart that performing a measurement on one system can not have any effect on the result of measurements on the other.

We are going to do some simple algebra with the quantity $QS + RS + RT - QT$. Notice that

$$QS + RS + RT - QT = (Q + R)S + (R - Q)T. \tag{2.219}$$

Because $R, Q = \pm 1$ it follows that either $(Q + R)S = 0$ or $(R - Q)T = 0$. In either case, it is easy to see from (2.219) that $QS + RS + RT - QT = \pm 2$. Suppose next that $p(q, r, s, t)$ is the probability that, before the measurements are performed, the system is in a state where $Q = q, R = r, S = s$, and $T = t$. These probabilities may depend on how Charlie performs his preparation, and on experimental noise. Letting $\mathbf{E}(\cdot)$ denote the mean value of a quantity, we have

$$\begin{aligned} \mathbf{E}(QS + RS + RT - QT) &= \sum_{qrst} p(q, r, s, t)(qs + rs + rt - qt) && (2.220)\\ &\leq \sum_{qrst} p(q, r, s, t) \times 2 && (2.221)\\ &= 2 && (2.222) \end{aligned}$$

Also,

$$\begin{aligned} \mathbf{E}(QS + RS + RT - QT) =& \sum_{qrst} p(q, r, s, t)qs + \sum_{qrst} p(q, r, s, t)rs \\ &+ \sum_{qrst} p(q, r, s, t)rt - \sum_{qrst} p(q, r, s, t)qt && (2.223)\\ =& \mathbf{E}(QS) + \mathbf{E}(RS) + \mathbf{E}(RT) - \mathbf{E}(QT). && (2.224) \end{aligned}$$

Comparing (2.222) and (2.224) we obtain the Bell inequality,

$$\mathbf{E}(QS) + \mathbf{E}(RS) + \mathbf{E}(RT) - \mathbf{E}(QT) \leq 2. \tag{2.225}$$

This result is also often known as the CHSH inequality after the initials of its four discoverers. It is part of a larger set of inequalities known generically as Bell inequalities, since the first was found by John Bell.

By repeating the experiment many times, Alice and Bob can determine each quantity on the left hand side of the Bell inequality. For example, after finishing a set of experiments, Alice and Bob get together to analyze their data. They look at all the experiments where Alice measured P_Q and Bob measured P_S. By multiplying the results of their experiments together, they get a sample of values for QS. By averaging over this sample, they can estimate $\mathbf{E}(QS)$

to an accuracy only limited by the number of experiments which they perform. Similarly, they can estimate all the other quantities on the left hand side of the Bell inequality, and thus check to see whether it is obeyed in a real experiment.

It's time to put some quantum mechanics back in the picture. Imagine we perform the following quantum mechanical experiment. Charlie prepares a quantum system of two qubits in the state

$$|\psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}. \tag{2.226}$$

He passes the first qubit to Alice, and the second qubit to Bob. They perform measurements of the following observables:

$$\begin{array}{ll} Q = Z_1 & S = \frac{-Z_2 - X_2}{\sqrt{2}} \\ R = X_1 & T = \frac{Z_2 - X_2}{\sqrt{2}}. \end{array} \tag{2.228}$$

Simple calculations show that the average values for these observables, written in the quantum mechanical $\langle \cdot \rangle$ notation, are:

$$\langle QS \rangle = \frac{1}{\sqrt{2}}; \langle RS \rangle = \frac{1}{\sqrt{2}}; \langle RT \rangle = \frac{1}{\sqrt{2}}; \langle QT \rangle = -\frac{1}{\sqrt{2}}. \tag{2.229}$$

Thus,

$$\langle QS \rangle + \langle RS \rangle + \langle RT \rangle - \langle QT \rangle = 2\sqrt{2}. \tag{2.230}$$

Hold on! We learned back in (2.225) that the average value of QS plus the average value of RS plus the average value of RT minus the average value of QT can never exceed two. Yet here, quantum mechanics predicts that this sum of averages yields $2\sqrt{2}$!

Fortunately, we can ask Nature to resolve the apparent paradox for us. Clever experiments using photons - particles of light - have been done to check the prediction (2.230) of quantum mechanics versus the Bell inequality (2.225) which we were led to by our common sense reasoning. The details of the experiments are outside the scope of the book, but the results were resoundingly in favor of the quantum mechanical prediction. The Bell inequality (2.225) is not obeyed by Nature.

What does this mean? It means that one or more of the assumptions that went into the derivation of the Bell inequality must be incorrect. Vast tomes have been written analyzing the various forms in which this type of argument can be made, and analyzing the subtly different assumptions which must be made to reach Bell-like inequalities. Here we merely summarize the main points.

There are two assumptions made in the proof of (2.225) which are questionable:
(1) The assumption that the physical properties P_Q, P_R, P_S, P_T have definite values Q, R, S, T which exist independent of observation. This is sometimes known as the assumption of realism.
(2) The assumption that Alice performing her measurement does not influence the result of Bob's measurement. This is sometimes known as the assumption of locality.

These two assumptions together are known as the assumptions of local realism. They are certainly intuitively plausible assumptions about how the world works, and they fit our everyday experience. Yet the Bell inequalities show that at least one of these assumptions is not correct.

What can we learn from Bell's inequality? For physicists, the most important lesson is that their deeply held commonsense intuitions about how the world works are wrong. The world is not locally realistic. Most physicists take the point of view that it is the assumption of realism which needs to be dropped from our worldview in quantum mechanics, although others have argued that the assumption of locality should be dropped instead. Regardless, Bell's inequality

together with substantial experimental evidence now points to the conclusion that either or both of locality and realism must be dropped from our view of the world if we are to develop a good intuitive understanding of quantum mechanics.

What lessons can the fields of quantum computation and quantum information learn from Bell's inequality? Historically the most useful lesson has perhaps also been the most vague: there is something profoundly 'up' with entangled states like the EPR state. A lot of mileage in quantum computation and, especially, quantum information, has come from asking the simple question: 'what would some entanglement buy me in this problem?' As we saw in teleportation and superdense coding, and as we will see repeatedly later in the book, by throwing some entanglement into a problem we open up a new world of possibilities unimaginable with classical information. The bigger picture is that Bell's inequality teaches us that entanglement is a fundamentally new resource in the world that goes essentially beyond classical resources; iron to the classical world's bronze age. A major task of quantum computation and quantum information is to exploit this new resource to do information processing tasks impossible or much more difficult with classical resources.

Problem 2.1: (Functions of the Pauli matrices) Let $f(\cdot)$ be any function from complex numbers to complex numbers. Let $\vec{n}$ be a normalized vector in three dimensions, and let θ be real. Show that

$$f(\theta \vec{n} \cdot \vec{\sigma}) = \frac{f(\theta) + f(-\theta)}{2} I + \frac{f(\theta) - f(-\theta)}{2} \vec{n} \cdot \vec{\sigma}. \tag{2.231}$$

Problem 2.2: (Properties of the Schmidt number) Suppose $|\psi\rangle$ is a pure state of a composite system with components A and B.
(1) Prove that the Schmidt number of $|\psi\rangle$ is equal to the rank of the reduced density matrix $\rho_A \equiv \mathrm{tr}_B(|\psi\rangle\langle\psi|)$. (Note that the rank of a Hermitian operator is equal to the dimension of its support.)
(2) Suppose $|\psi\rangle = \sum_j |\alpha_j\rangle |\beta_j\rangle$ is a representation for $|\psi\rangle$, where $|\alpha_j\rangle$ and $|\beta_j\rangle$ are (unnormalized) states for systems A and B, respectively. Prove that the
number of terms in such a decomposition is greater than or equal to the Schmidt number of $|\psi\rangle, \mathrm{Sch}(\psi)$.
(3) Suppose $|\psi\rangle = \alpha|\varphi\rangle + \beta|\gamma\rangle$. Prove that

$$\mathrm{Sch}(\psi) \geq |\,\mathrm{Sch}(\varphi) - \mathrm{Sch}(\gamma)|. \tag{2.232}$$

Problem 2.3: (Tsirelson's inequality) Suppose
$Q = \vec{q} \cdot \vec{\sigma}, R = \vec{r} \cdot \vec{\sigma}, S = \vec{s} \cdot \vec{\sigma}, T = \vec{t} \cdot \vec{\sigma}$, where $\vec{q}, \vec{r}, \vec{s}$ and $\vec{t}$ are real unit vectors in three dimensions. Show that

$$(Q \otimes S + R \otimes S + R \otimes T - Q \otimes T)^2 = 4I + [Q, R] \otimes [S, T]. \tag{2.233}$$

Use this result to prove that

$$\langle Q \otimes S \rangle + \langle R \otimes S \rangle + \langle R \otimes T \rangle - \langle Q \otimes T \rangle \leq 2\sqrt{2}, \tag{2.234}$$

so the violation of the Bell inequality found in Equation (2.230) is the maximum possible in quantum mechanics.

History and further reading

There are an enormous number of books on linear algebra at levels ranging from High School through to Graduate School. Perhaps our favorites are the two volume set by Horn and Johnson [HJ85, HJ91], which cover an extensive range of topics in an accessible manner. Other useful

references include Marcus and Minc [MM92] , and Bhatia [Bha97]. Good introductions to linear algebra include Halmos [Hal58], Perlis [Per52], and Strang [Str76].

There are many excellent books on quantum mechanics. Unfortunately, most of these books focus on topics of tangential interest to quantum information and computation. Perhaps the most relevant in the existing literature is Peres' superb book [Per93] . Beside an extremely clear exposition of elementary quantum mechanics, Peres gives an extensive discussion of the Bell inequalities and related results. Good introductory level texts include Sakurai's book [Sak95], Volume III of the superb series by Feynman, Leighton, and Sands [FLS65a], and the two volume work by Cohen-Tannoudji, Diu and Laloë[CTDL77a, CTDL77b]. All three of these works are somewhat closer in spirit to quantum computation and quantum information than are most other quantum mechanics texts, although the great bulk of each is still taken up by applications far removed from quantum computation and quantum information. As a result, none of these texts need be read in detail by someone interested in learning about quantum computation and quantum information. However, any one of these texts may prove handy as a reference, especially when reading articles by physicists. References for the history of quantum mechanics may be found at the end of Chapter 1.

Many texts on quantum mechanics deal only with projective measurements. For applications to quantum computing and quantum information it is more convenient - and, we believe, easier for novices - to start with the general description of measurements, of which projective measurements can be regarded as a special case. Of course, ultimately, as we have shown, the two approaches are equivalent. The theory of generalized measurements which we have employed was developed between the 1940s and 1970s. Much of the history can be distilled from the book of Kraus[Kra83]. Interesting discussion of quantum measurements may be found in Section 2.2 of Gardiner [Gar 91], and in the book by Braginsky and Khahili[BK92]. The POVM measurement for distinguishing
non-orthogonal states described in Section 2.2.6 is due to Peres [Per88] . The extension described in Exercise 2.64 appeared in Duan and Guo [DG98].

Superdense coding was invented by Bennett and Wiesner [BW92]. An experiment implementing a variant of superdense coding using entangled photon pairs was performed by Mattle, Weinfurter, Kwiat, and Zeilinger [MWKZ96] .

The density operator formalism was introduced independently by Landau [Lan27] and by von Neumann [von 27]. The unitary freedom in the ensemble for density matrices, Theorem 2.6, was first pointed out by Schrodinger [*Sch*36], and was later rediscovered and extended by Jaynes [Jay 57] and by Hughston, Jozsa and Wootters [HJW93] . The result of Exercise 2.73 is from the paper by Jaynes, and the results of Exercises 2.81 and 2.82 appear in the paper by Hughston, Jozsa and Wootters. The class of probability distributions which may appear in a density matrix decomposition for a given density matrix has been studied by Uhlmann [U*h*70] and by Nielsen [Nie996]. Schmidt's eponymous decomposition appeared in [Sch06]. The result of Exercise 2.77 was noted by Peres [Per95] .

The EPR thought experiment is due to Einstein, Podolsky and Rosen [EPR35] , and was recast in essentially the form we have given here by Bohm [Boh51]. It is sometimes misleadingly referred to as the EPR 'paradox'. The Bell inequality is named in honour of Bell [Bel64], who first derived inequalities of this type. The form we have presented is due to Clauser, Horne, Shimony, and Holt [CHSH69], and is often known as the CHSH inequality. This inequality was derived independently by Bell, who did not publish the result.

Part 3 of Problem 2.2 is due to Thapliyal (private communication). Tsirelson's inequality is due to Tsirelson [Tsi80].

7.3 3 Introduction to computer science

> In natural science, Nature has given us a world and we're just to discover its laws. In computers, we can stuff laws into it and create a world. - Alan Kay
>
> Our field is still in its embryonic stage. It's great that we haven't been around for 2000 years. We are still at a stage where very, very important results occur in front of our eyes.
>
> - Michael Rabin, on computer science

Algorithms are the key concept of computer science. An algorithm is a precise recipe for performing some task, such as the elementary algorithm for adding two numbers which we all learn as children. This chapter outlines the modern theory of algorithms developed by computer science. Our fundamental model for algorithms will be the Turing machine. This is an idealized computer, rather like a modern personal computer, but with a simpler set of basic instructions, and an idealized unbounded memory. The apparent simplicity of Turing machines is misleading; they are very powerful devices. We will see that they can be used to execute any algorithm whatsoever, even one running on an apparently much more powerful computer.

The fundamental question we are trying to address in the study of algorithms is: what resources are required to perform a given computational task? This question splits up naturally into two parts. First, we'd like to understand what computational tasks are possible, preferably by giving explicit algorithms for solving specific problems. For example, we have many excellent examples of algorithms that can quickly sort a list of numbers into ascending order. The second aspect of this question is to demonstrate limitations on what computational tasks may be accomplished. For example, lower bounds can be given for the number of operations that must be performed by any algorithm which sorts a list of numbers into ascending order. Ideally, these two tasks - the finding of algorithms for solving computational problems, and proving limitations on our ability to solve computational problems - would dovetail perfectly. In practice, a significant gap often exists between the best techniques known for solving a computational problem, and the most stringent limitations known on the solution. The purpose of this chapter is to give a broad overview of the tools which have been developed to aid in the analysis of computational problems, and in the construction and analysis of algorithms to solve such problems.

Why should a person interested in quantum computation and quantum information spend time investigating classical computer science? There are three good reasons for this effort. First, classical computer science provides a vast body of concepts and techniques which may be reused to great effect in quantum computation and quantum information. Many of the triumphs of quantum computation and quantum information have come by combining existing ideas from computer science with novel ideas from quantum
mechanics. For example, some of the fast algorithms for quantum computers are based upon the Fourier transform, a powerful tool utilized by many classical algorithms. Once it was realized that quantum computers could perform a type of Fourier transform much more quickly than classical computers this enabled the development of many important quantum algorithms.

Second, computer scientists have expended great effort understanding what resources are required to perform a given computational task on a classical computer. These results can be used as the basis for a comparison with quantum computation and quantum information. For example, much attention has been focused on the problem of finding the prime factors of a given number. On a classical computer this problem is believed to have no 'efficient' solution, where 'efficient' has a meaning we'll explain later in the chapter. What is interesting is that an efficient solution to this problem is known for quantum computers. The lesson is that, for this

task of finding prime factors, there appears to be a gap between what is possible on a classical computer and what is possible on a quantum computer. This is both intrinsically interesting, and also interesting in the broader sense that it suggests such a gap may exist for a wider class of computational problems than merely the finding of prime factors. By studying this specific problem further, it may be possible to discern features of the problem which make it more tractable on a quantum computer than on a classical computer, and then act on these insights to find interesting quantum algorithms for the solution of other problems.

Third, and most important, there is learning to think like a computer scientist. Computer scientists think in a rather different style than does a physicist or other natural scientist. Anybody wanting a deep understanding of quantum computation and quantum information must learn to think like a computer scientist at least some of the time; they must instinctively know what problems, what techniques, and most importantly what problems are of greatest interest to a computer scientist.

The structure of this chapter is as follows. In Section 3.1 we introduce two models for computation: the Turing machine model, and the circuit model. The Turing machine model will be used as our fundamental model for computation. In practice, however, we mostly make use of the circuit model of computation, and it is this model which is most useful in the study of quantum computation. With our models for computation in hand, the remainder of the chapter discusses resource requirements for computation. Section 3.2 begins by overviewing the computational tasks we are interested in as well as discusing some associated resource questions. It continues with a broad look at the key concepts of computational complexity, a field which examines the time and space requirements necessary to solve particular computational problems, and provides a broad classification of problems based upon their difficulty of solution. Finally, the section concludes with an examination of the energy resources required to perform computations. Surprisingly, it turns out that the energy required to perform a computation can be made vanishingly small, provided one can make the computation reversible. We explain how to construct reversible computers, and explain some of the reasons they are important both for computer science and for quantum computation and quantum information. Section 3.3 concludes the chapter with a broad look at the entire field of computer science, focusing on issues of particular relevance to quantum computation and quantum information.

7.3.1 3.1 Models for computation

...algorithms are concepts that have existence apart from any programming language.

- Donald Knuth

What does it mean to have an algorithm for performing some task? As children we all learn a procedure which enables us to add together any two numbers, no matter how large those numbers are. This is an example of an algorithm. Finding a mathematically precise formulation of the concept of an algorithm is the goal of this section.

Historically, the notion of an algorithm goes back centuries; undergraduates learn Euclid's two thousand year old algorithm for finding the greatest common divisor of two positive integers. However, it wasn't until the 1930s that the fundamental notions of the modern theory of algorithms, and thus of computation, were introduced, by Alonzo Church, Alan Turing, and other pioneers of the computer era. This work arose in response to a profound challenge laid down by the great mathematician David Hilbert in the early part of the twentieth century. Hilbert asked whether or not there existed some algorithm which could be used, in principle, to solve all the problems of mathematics. Hilbert expected that the answer to this question, sometimes known as the entscheidungsproblem, would be yes.

Amazingly, the answer to Hilbert's challenge turned out to be no: there is no algorithm to solve all mathematical problems. To prove this, Church and Turing had to solve the deep problem of capturing in a mathematical definition what we mean when we use the intuitive concept of an algorithm. In so doing, they laid the foundations for the modern theory of algorithms, and consequently for the modern theory of computer science.

In this chapter, we use two ostensibly different approaches to the theory of computation. The first approach is that proposed by Turing. Turing defined a class of machines, now known as Turing machines, in order to capture the notion of an algorithm to perform a computational task. In Section 3.1.1, we describe Turing machines, and then discuss some of the simpler variants of the Turing machine model. The second approach is via the circuit model of computation, an approach that is especially useful as preparation for our later study of quantum computers. The circuit model is described in Section 3.1.2. Although these models of computation appear different on the surface, it turns out that they are equivalent. Why introduce more than one model of computation, you may ask? We do so because different models of computation may yield different insights into the solution of specific problems. Two (or more) ways of thinking about a concept are better than one.

7.3.2 3.1.1 Turing machines

The basic elements of a Turing machine are illustrated in Figure 3.1. A Turing machine contains four main elements: (a) a program, rather like an ordinary computer; (b) a finite state control, which acts like a stripped-down microprocessor, co-ordinating the other operations of the machine; (c) a tape, which acts like a computer memory; and (d) a readwrite tape-head, which points to the position on the tape which is currently readable or writable. We now describe each of these four elements in more detail.

The finite state control for a Turing machine consists of a finite set of internal states,

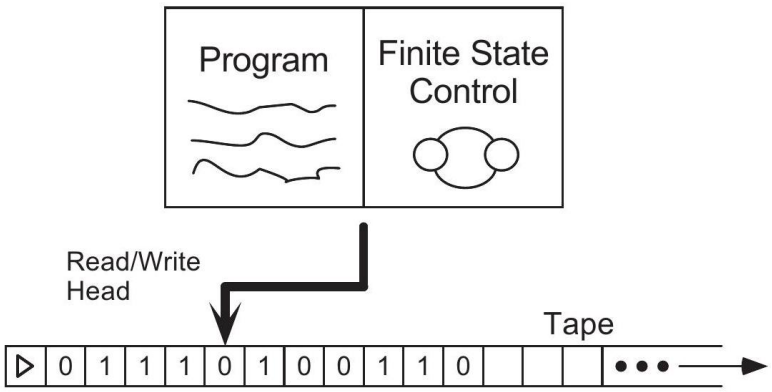


Figure 3.1. Main elements of a Turing machine. In the text, blanks on the tape are denoted by a 'b'. Note the ▷ marking the left hand end of the tape.

$q_1, \ldots, q_m$. The number m is allowed to be varied; it turns out that for m sufficiently large this does not affect the power of the machine in any essential way, so without loss of generality we may suppose that m is some fixed constant. The best way to think of the finite state control is as a sort of microprocessor, co-ordinating the Turing machine's operation. It provides temporary storage off-tape, and a central place where all processing for the machine may be done. In addition to the states $q_1, \ldots, q_m$, there are also two special internal states, labelled $q_{\rm s}$ and $q_{\rm h}$. We call these the starting state and the halting state, respectively. The idea is that at the beginning of the computation, the Turing machine is in the starting state $q_{\rm s}$. The execution of the computation causes the Turing machine's internal state to change. If

the computation ever finishes, the Turing machine ends up in the state $q_{\rm h}$ to indicate that the machine has completed its operation.

The Turing machine tape is a one-dimensional object, which stretches off to infinity in one direction. The tape consists of an infinite sequence of tape squares. We number the tape squares $0, 1, 2, 3, \ldots$. The tape squares each contain one symbol drawn from some alphabet, Γ, which contains a finite number of distinct symbols. For now, it will be convenient to assume that the alphabet contains four symbols, which we denote by $0, 1, b$ (the 'blank' symbol), and $\triangleright$, to mark the left hand edge of the tape. Initially, the tape contains a $\triangleright$ at the left hand end, a finite number of 0 s and 1 s , and the rest of the tape contains blanks. The read-write tape-head identifies a single square on the Turing machine tape as the square that is currently being accessed by the machine.

Summarizing, the machine starts its operation with the finite state control in the state $q_{\rm s}$, and with the read-write head at the leftmost tape square, the square numbered 0 . The computation then proceeds in a step by step manner according to the program, to be defined below. If the current state is $q_{\rm h}$, then the computation has halted, and the output of the computation is the current (non-blank) contents of the tape.

A program for a Turing machine is a finite ordered list of program lines of the form $\langle q, x, q', x', s\rangle$. The first item in the program line, q, is a state from the set of internal states of the machine. The second item, x, is taken from the alphabet of symbols which may appear on the tape, Γ. The way the program works is that on each machine cycle, the Turing machine looks through the list of program lines in order, searching for a line $\langle q, x, \cdot, \cdot, \cdot\rangle$, such that the current internal state of the machine is q, and the symbol
being read on the tape is x. If it doesn't find such a program line, the internal state of the machine is changed to $q_{\rm h}$, and the machine halts operation. If such a line is found, then that program line is executed. Execution of a program line involves the following steps: the internal state of the machine is changed to q'; the symbol x on the tape is overwritten by the symbol x', and the tape-head moves left, right, or stands still, depending on whether s is $-1, +1$, or 0 , respectively. The only exception to this rule is if the tape-head is at the leftmost tape square, and $s = -1$, in which case the tape-head stays put.

Now that we know what a Turing machine is, let's see how it may be used to compute a simple function. Consider the following example of a Turing machine. The machine starts with a binary number, x, on the tape, followed by blanks. The machine has three internal states, q_1, q_2, and q_3, in addition to the starting state $q_{\rm s}$ and halting state $q_{\rm h}$. The program contains the following program lines (the numbers on the left hand side are for convenience in referring to the program lines in later discussion, and do not form part of the program):

$$
\begin{aligned}
&1 : \langle q_{\rm s}, \triangleright, q_1, \triangleright, +1\rangle \\
&2 : \langle q_1, 0, q_1, b, +1\rangle \\
&3 : \langle q_1, 1, q_1, b, +1\rangle \\
&4 : \langle q_1, b, q_2, b, -1\rangle \\
&5 : \langle q_2, b, q_2, b, -1\rangle \\
&6 : \langle q_2, \triangleright, q_3, \triangleright, +1\rangle \\
&7 : \langle q_3, b, q_{\rm h}, 1, 0\rangle\,.
\end{aligned}
$$

What function does this program compute? Initially the machine is in the state $q_{\rm s}$ and at the left-most tape position so line $1, \langle q_{\rm s}, \triangleright, q_1, \triangleright, +1\rangle$, is executed, which causes the tape-head to move right without changing what is written on the tape, but changing the internal state of the machine to q_1. The next three lines of the program ensure that while the machine is in the state q_1 the tape-head will continue moving right while it reads either 0 s (line 2) or 1 s (line 3) on the tape, over-writing the tape contents with blanks as it goes and remaining in the state

q_1, until it reaches a tape square that is already blank, at which point the tape-head is moved one position to the left, and the internal state is changed to q_2 (line 4). Line 5 then ensures that the tape-head keeps moving left while blanks are being read by the tape-head, without changing the contents of the tape. This keeps up until the tape-head returns to its starting point, at which point it reads a $\triangleright$ on the tape, changes the internal state to q_3, and moves one step to the right (line 6). Line 7 completes the program, simply printing the number 1 onto the tape, and then halting.

The preceding analysis shows that this program computes the constant function $f(x) = 1$. That is, regardless of what number is input on the tape the number 1 is output. More generally, a Turing machine can be thought of as computing functions from the nonnegative integers to the non-negative integers; the initial state of the tape is used to represent the input to the function, and the final state of the tape is used to represent the output of the function.

It seems as though we have gone to a very great deal of trouble to compute this simple function using our Turing machines. Is it possible to build up more complicated functions using Turing machines? For example, could we construct a machine such that when two numbers, x and y, are input on the tape with a blank to demarcate them, it will
output the sum $x + y$ on the tape? More generally, what class of functions is it possible to compute using a Turing machine?

It turns out that the Turing machine model of computation can be used to compute an enormous variety of functions. For example, it can be used to do all the basic arithmetical operations, to search through text represented as strings of bits on the tape, and many other interesting operations. Surprisingly, it turns out that a Turing machine can be used to simulate all the operations performed on a modern computer! Indeed, according to a thesis put forward independently by Church and by Turing, the Turing machine model of computation completely captures the notion of computing a function using an algorithm. This is known as the Church-Turing thesis:

The class of functions computable by a Turing machine corresponds exactly to the class of functions which we would naturally regard as being computable by an algorithm.

The Church-Turing thesis asserts an equivalence between a rigorous mathematical concept - function computable by a Turing machine - and the intuitive concept of what it means for a function to be computable by an algorithm. The thesis derives its importance from the fact that it makes the study of real-world algorithms, prior to 1936 a rather vague concept, amenable to rigorous mathematical study. To understand the significance of this point it may be helpful to consider the definition of a continuous function from real analysis. Every child can tell you what it means for a line to be continuous on a piece of paper, but it is far from obvious how to capture that intuition in a rigorous definition. Mathematicians in the nineteenth century spent a great deal of time arguing about the merits of various definitions of continuity before the modern definition of continuity came to be accepted. When making fundamental definitions like that of continuity or of computability it is important that good definitions be chosen, ensuring that one's intuitive notions closely match the precise mathematical definition. From this point of view the Church-Turing thesis is simply the assertion that the Turing machine model of computation provides a good foundation for computer science, capturing the intuitive notion of an algorithm in a rigorous definition.

A priori it is not obvious that every function which we would intuitively regard as computable by an algorithm can be computed using a Turing machine. Church, Turing and many other people have spent a great deal of time gathering evidence for the Church-Turing thesis, and in sixty years no evidence to the contrary has been found. Nevertheless, it is possible that in the future we will discover in Nature a process which computes a function not computable on a Turing machine. It would be wonderful if that ever happened, because we could then harness that process to help us perform new computations which could not be performed before. Of

course, we would also need to overhaul the definition of computability, and with it, computer science.

Exercise 3.1: (Non-computable processes in Nature) How might we recognize that a process in Nature computes a function not computable by a Turing machine?

Exercise 3.2: (Turing numbers) Show that single-tape Turing machines can each be given a number from the list $1, 2, 3, \ldots$ in such a way that the number uniquely specifies the corresponding machine. We call this number the Turing number of the corresponding Turing machine. (Hint: Every positive integer has
a unique prime factorization $p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$, where p_i are distinct prime numbers, and $a_1, \ldots, a_k$ are non-negative integers.)

In later chapters, we will see that quantum computers also obey the Church-Turing thesis. That is, quantum computers can compute the same class of functions as is computable by a Turing machine. The difference between quantum computers and Turing machines turns out to lie in the efficiency with which the computation of the function may be performed - there are functions which can be computed much more efficiently on a quantum computer than is believed to be possible with a classical computing device such as a Turing machine.

Demonstrating in complete detail that the Turing machine model of computation can be used to build up all the usual concepts used in computer programming languages is beyond the scope of this book (see 'History and further reading' at the end of the chapter for more information). When specifying algorithms, instead of explicitly specifying the Turing machine used to compute the algorithm, we shall usually use a much higher level pseudocode, trusting in the Church-Turing thesis that this pseudocode can be translated into the Turing machine model of computation. We won't give any sort of rigorous definition for pseudocode. Think of it as a slightly more formal version of English or, if you like, a sloppy version of a high-level programming language such as C++ or BASIC. Pseudocode provides a convenient way of expressing algorithms, without going into the extreme level of detail required by a Turing machine. An example use of pseudocode may be found in Box 3.2 on page 130; it is also used later in the book to describe quantum algorithms.

There are many variants on the basic Turing machine model. We might imagine Turing machines with different kinds of tapes. For example, one could consider two-way infinite tapes, or perhaps computation with tapes of more than one dimension. So far as is presently known, it is not possible to change any aspect of the Turing model in a way that is physically reasonable, and which manages to extend the class of functions computable by the model.

As an example consider a Turing machine equipped with multiple tapes. For simplicity we consider the two-tape case, as the generalization to more than two tapes is clear from this example. Like the basic Turing machine, a two-tape Turing machine has a finite number of internal states $q_1, \ldots, q_m$, a start state $q_{\rm s}$, and a halt state $q_{\rm h}$. It has two tapes, each of which contain symbols from some finite alphabet of symbols, Γ. As before we find it convenient to assume that the alphabet contains four symbols, $0, 1, b$ and $\triangleright$, where $\triangleright$ marks the left hand edge of each tape. The machine has two tape-heads, one for each tape. The main difference between the two-tape Turing machine and the basic Turing machine is in the program. Program lines are of the form $\langle q, x_1, x_2, q', x_1', x_2', s_1, s_2 \rangle$, meaning that if the internal state of the machine is q, tape one is reading x_1 at its current position, and tape two is reading x_2 at its current position, then the internal state of the machine should be changed to q', x_1 overwritten with x_1', x_2 overwritten with x_2', and the tape-heads for tape one and tape two moved according to whether s_1 or s_2 are equal to $+1, -1$ or 0 , respectively.

In what sense are the basic Turing machine and the two-tape Turing machine equivalent models of computation? They are equivalent in the sense that each computational model is able to simulate the other. Suppose we have a two-tape Turing machine which takes as input a bit string x on the first tape and blanks on the remainder of both tapes,

except the endpoint marker $\triangleright$. This machine computes a function $f(x)$, where $f(x)$ is defined to be the contents of the first tape after the Turing machine has halted. Rather remarkably, it turns out that given a two-tape Turing machine to compute f, there exists an equivalent single-tape Turing machine that is also able to compute f. We won't explain how to do this explicitly, but the basic idea is that the single-tape Turing machine simulates the two-tape Turing machine, using its single tape to store the contents of both tapes of the two-tape Turing machine. There is some computational overhead required to do this simulation, but the important point is that in principle it can always be done. In fact, there exists a Universal Turing machine (see Box 3.1) which can simulate any other Turing machine!

Another interesting variant of the Turing machine model is to introduce randomness into the model. For example, imagine that the Turing machine can execute a program line whose effect is the following: if the internal state is q and the tape-head reads x, then flip an unbiased coin. If the coin lands heads, change the internal state to $q_{i_{\rm H}}$, and if it lands tails, change the internal state to $q_{i_{\rm T}}$, where $q_{i_{\rm H}}$ and $q_{i_{\rm T}}$ are two internal states of the Turing machine. Such a program line can be represented as $\langle q, x, q_{i_{\rm H}}, q_{i_{\rm T}} \rangle$. However, even this variant doesn't change the essential power of the Turing machine model of computation. It is not difficult to see that we can simulate the effect of the above algorithm on a deterministic Turing machine by explicitly 'searching out' all the possible computational paths corresponding to different values of the coin tosses. Of course, this deterministic simulation may be far less efficient than the random model, but the key point for the present discussion is that the class of functions computable is not changed by introducing randomness into the underlying model.

Exercise 3.3: (Turing machine to reverse a bit string) Describe a Turing machine which takes a binary number x as input, and outputs the bits of x in reverse order. (Hint: In this exercise and the next it may help to use a multi-tape Turing machine and/or symbols other than $\triangleright, 0, 1$ and the blank.)

Exercise 3.4: (Turing machine to add modulo 2) Describe a Turing machine to add two binary numbers x and y modulo 2 . The numbers are input on the Turing machine tape in binary, in the form x, followed by a single blank, followed by a y. If one number is not as long as the other then you may assume that it has been padded with leading 0 s to make the two numbers the same length.

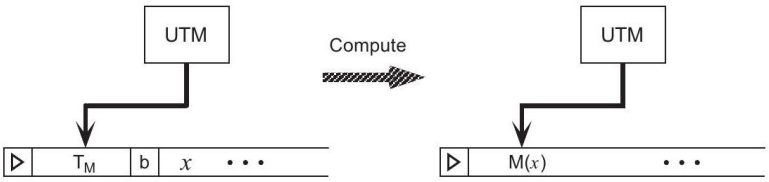
Let us return to Hilbert's entscheidungsproblem, the original inspiration for the founders of computer science. Is there an algorithm to decide all the problems of mathematics? The answer to this question was shown by Church and Turing to be no. In Box 3.2, we explain Turing's proof of this remarkable fact. This phenomenon of undecidability is now known to extend far beyond the examples which Church and Turing constructed. For example, it is known that the problem of deciding whether two topological spaces are topologically equivalent ('homeomorphic') is undecidable. There are simple problems related to the behavior of dynamical systems which are undecidable, as you will show in Problem 3.4. References for these and other examples are given in the end of chapter 'History and further reading'.

Besides its intrinsic interest, undecidability foreshadows a topic of great concern in computer science, and also to quantum computation and quantum information: the dis-

Box 3.1: The Universal Turing Machine

We've described Turing machines as containing three elements which may vary from machine to machine - the initial configuration of the tape, the internal states of the finite state control, and the program for the machine. A clever idea known as the Universal Turing Machine (UTM) allows us to fix the program and finite state control once and for all, leaving the initial contents of the tape as the only part of the machine which needs to be varied.
The Universal Turing Machine (see the figure below) has the following property. Let M be any Turing machine, and let T_M be the Turing number associated to machine M. Then on input

of the binary representation for T_M followed by a blank, followed by any string of symbols x on the remainder of the tape, the Universal Turing Machine gives as output whatever machine M would have on input of x. Thus, the Universal Turing Machine is capable of simulating any other Turing machine!



The Universal Turing Machine is similar in spirit to a modern programmable computer, in which the action to be taken by the computer - the 'program' - is stored in memory, analogous to the bit string T_M stored at the beginning of the tape by the Universal Turing Machine. The data to be processed by the program is stored in a separate part of memory, analogous to the role of x in the Universal Turing Machine. Then some fixed hardware is used to run the program, producing the output. This fixed hardware is analogous to the internal states and the (fixed) program being executed by the Universal Turing Machine.
Describing the detailed construction of a Universal Turing Machine is beyond the scope of this book. (Though industrious readers may like to attempt the construction.) The key point is the existence of such a machine, showing that a single fixed machine can be used to run any algorithm whatsoever. The existence of a Universal Turing Machine also explains our earlier statement that the number of internal states in a Turing machine does not matter much, for provided that number m exceeds the number needed for a Universal Turing Machine, such a machine can be used to simulate a Turing machine with any number of internal states.
tinction between problems which are easy to solve, and problems which are hard to solve. Undecidability provides the ultimate example of problems which are hard to solve - so hard that they are in fact impossible to solve.

Exercise 3.5: (Halting problem with no inputs) Show that given a Turing machine M there is no algorithm to determine whether M halts when the input to the machine is a blank tape.

Exercise 3.6: (Probabilistic halting problem) Suppose we number the probabilistic Turing machines using a scheme similar to that found in Exercise 3.2 and define the probabilistic halting function $h_p(x)$ to be 1 if machine x halts on input of x with probability at least $1/2$ and 0 if machine x halts on input of x with probability less than $1/2$. Show that there is no probabilistic Turing machine which can output $h_p(x)$ with probability of correctness strictly greater than $1/2$ for all x.

Exercise 3.7: (Halting oracle) Suppose a black box is made available to us which takes a non-negative integer x as input, and then outputs the value of $h(x)$, where $h(\cdot)$ is the halting function defined in Box 3.2 on page 130. This type of black box is sometimes known as an oracle for the halting problem. Suppose we have a regular Turing machine which is augmented by the power to call the oracle. One way of accomplishing this is to use a two-tape Turing machine, and add an extra program instruction to the Turing machine which results in the oracle being called, and the value of $h(x)$ being printed on the second tape, where x is the current contents of the second tape. It is clear that this model for computation is more powerful than the conventional Turing machine model, since it can be used to compute the halting function. Is the halting problem for this model of computation undecidable? That is, can a Turing machine aided by an oracle for the halting problem decide whether a program for the Turing machine with oracle will halt on a particular input?

7.3.3 3.1.2 Circuits

Turing machines are rather idealized models of computing devices. Real computers are finite in size, whereas for Turing machines we assumed a computer of unbounded size. In this section we investigate an alternative model of computation, the circuit model, that is equivalent to the Turing machine in terms of computational power, but is more convenient and realistic for many applications. In particular the circuit model of computation is especially important as preparation for our investigation of quantum computers.

A circuit is made up of wires and gates, which carry information around, and perform simple computational tasks, respectively. For example, Figure 3.2 shows a simple circuit which takes as input a single bit, a. This bit is passed through a not gate, which flips the bit, taking 1 to 0 and 0 to 1 . The wires before and after the not gate serve merely to carry the bit to and from the NOT gate; they can represent movement of the bit through space, or perhaps just through time.

More generally, a circuit may involve many input and output bits, many wires, and many logical gates. A logic gate is a function $f : \{0,1\}^k \rightarrow \{0,1\}^l$ from some fixed number k of input bits to some fixed number l of output bits. For example, the not gate is a gate with one input bit and one output bit which computes the function $f(a) = 1 \oplus a$, where a is a single bit, and $\oplus$ is modulo 2 addition. It is also usual to make the convention that no loops are allowed in the circuit, to avoid possible instabilities, as illustrated in Figure 3.3. We say such a circuit is acyclic, and we adhere to the convention that circuits in the circuit model of computation be acyclic.

Box 3.2: The halting problem

In Exercise 3.2 you showed that each Turing machine can be uniquely associated with a number from the list $1, 2, 3, \ldots$. To solve Hilbert's problem, Turing used this numbering to pose the halting problem: does the machine with Turing number x halt upon input of the number y ? This is a well posed and interesting mathematical problem. After all, it is a matter of some considerable interest to us whether our algorithms halt or not. Yet it turns out that there is no algorithm which is capable of solving the halting problem. To see this, Turing asked whether there is an algorithm to solve an even more specialized problem: does the machine with Turing number x halt upon input of the same number x ? Turing defined the halting function,

$$h(x) \equiv \begin{cases} 0 & \text{if machine number } x \text{ does not halt upon input of } x \\ 1 & \text{if machine number } x \text{ halts upon input of } x. \end{cases}$$

If there is an algorithm to solve the halting problem, then there surely is an algorithm to evaluate $h(x)$. We will try to reach a contradiction by supposing such an algorithm exists, denoted by HALT (x). Consider an algorithm computing the function TURING(x), with pseudocode

```
TURING(x)
y = HALT(x)
if y = 0 then
    halt
else
    loop forever
end if
```

Since HALT is a valid program, TURING must also be a valid program, with some Turing number, t. By definition of the halting function, $h(t) = 1$ if and only if TURING halts on input

of t. But by inspection of the program for TURING, we see that TURING halts on input of t if and only if $h(t) = 0$. Thus $h(t) = 1$ if and only if $h(t) = 0$, a contradiction. Therefore, our initial assumption that there is an algorithm to evaluate $h(x)$ must have been wrong. We conclude that there is no algorithm allowing us to solve the halting problem.

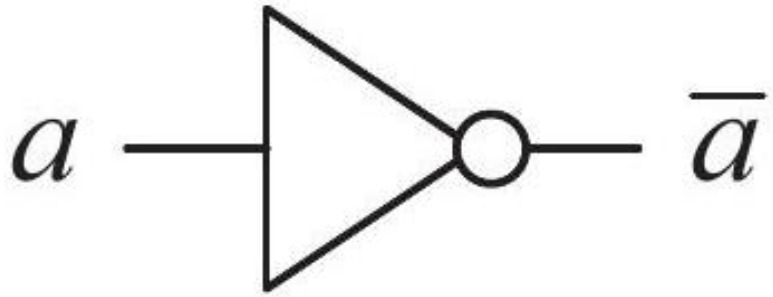


Figure 3.2. Elementary circuit performing a single NOT gate on a single input bit.

There are many other elementary logic gates which are useful for computation. A partial list includes the AND gate, the OR gate, the XOR gate, the NAND gate, and the NOR gate. Each of these gates takes two bits as input, and produces a single bit as output. The and gate outputs 1 if and only if both of its inputs are 1 . The or gate outputs 1 if

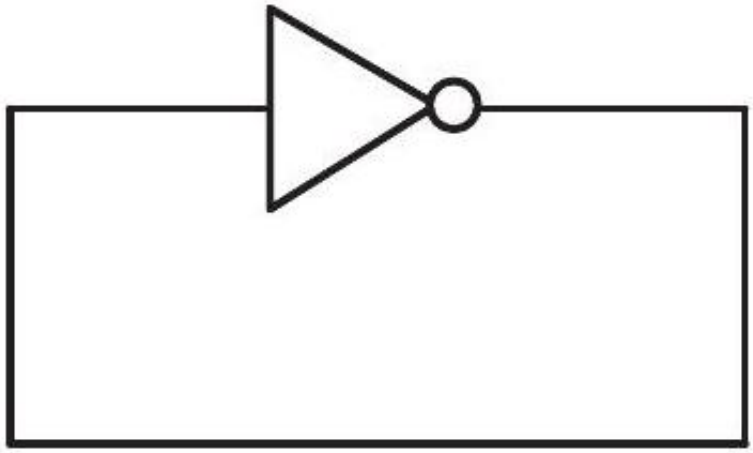


Figure 3.3. Circuits containing cycles can be unstable, and are not usually permitted in the circuit model of computation.

and only if at least one of its inputs is 1 . The XOR gate outputs the sum, modulo 2 , of its inputs. The NAND and NOR gates take the AND and OR, respectively, of their inputs, and then apply a not to whatever is output. The action of these gates is illustrated in Figure 3.4.

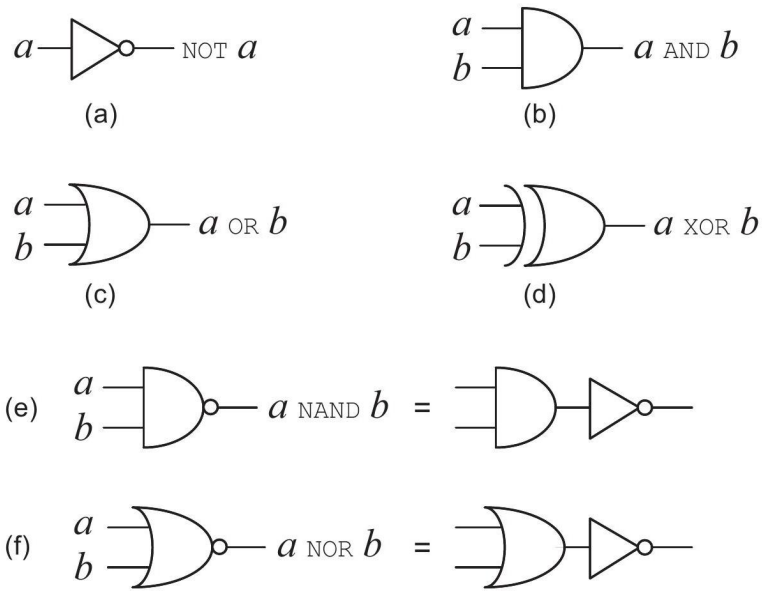


Figure 3.4. Elementary circuits performing the and, or, xor, nand, and nor gates.

There are two important 'gates' missing from Figure 3.4, namely the fanout gate and the CROSSOVER gate. In circuits we often allow bits to 'divide', replacing a bit with two copies of itself, an operation referred to as fanout. We also allow bits to crossover, that is, the value of two bits are interchanged. A third operation missing from Figure 3.4, not really a logic gate at all, is to allow the preparation of extra ancilla or work bits, to allow extra working space during the computation.

These simple circuit elements can be put together to perform an enormous variety of computations. Below we'll show that these elements can be used to compute any function whatsoever. In the meantime, let's look at a simple example of a circuit which adds two n bit integers, using essentially the same algorithm taught to school-children around the
world. The basic element in this circuit is a smaller circuit known as a half-adder, shown in Figure 3.5. A half-adder takes two bits, x and y, as input, and outputs the sum of the bits $x \oplus y$ modulo 2 , together with a carry bit set to 1 if x and y are both 1 , or 0 otherwise.

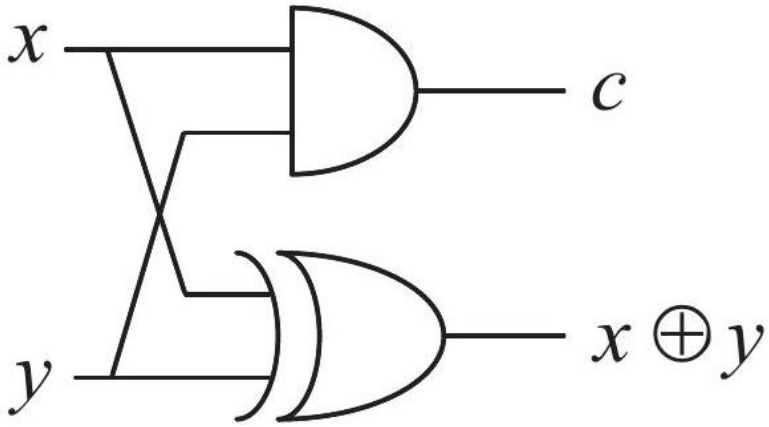


Figure 3.5. Half-adder circuit. The carry bit c is set to 1 when x and y are both 1 , otherwise it is 0 .

Two cascaded half-adders may be used to build a full-adder, as shown in Figure 3.6. A full-adder takes as input three bits, x, y, and c. The bits x and y should be thought of as data

to be added, while c is a carry bit from an earlier computation. The circuit outputs two bits. One output bit is the modulo 2 sum, $x \oplus y \oplus c$ of all three input bits. The second output bit, c', is a carry bit, which is set to 1 if two or more of the inputs is 1 , and is 0 otherwise.

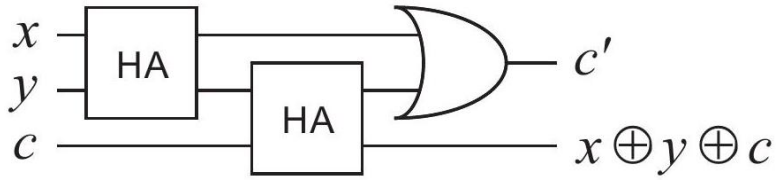


Figure 3.6. Full-adder circuit.

By cascading many of these full-adders together we obtain a circuit to add two n-bit integers, as illustrated in Figure 3.7 for the case $n = 3$.

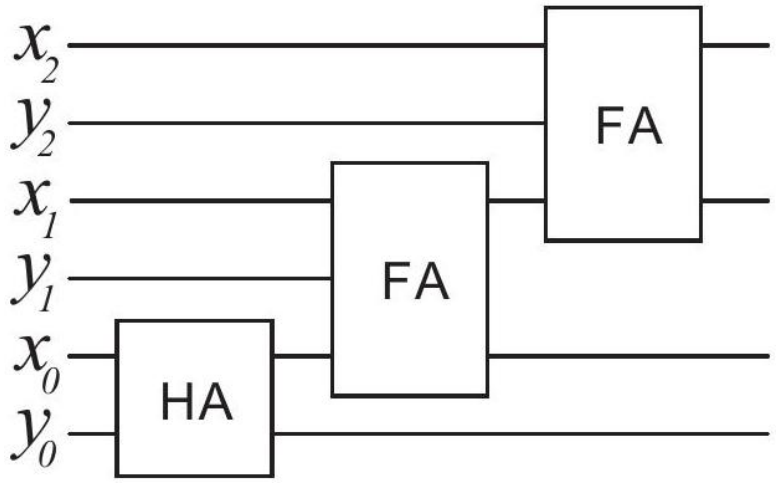


Figure 3.7. Addition circuit for two three-bit integers, $x=x_{2 x_{1} x_{0}$ and $y = y_2y_1y_0$, using the elementary algorithm taught to school-children.}

We claimed earlier that just a few fixed gates can be used to compute any function $f : \{0,1\}^n \rightarrow \{0,1\}^m$ whatsoever. We will now prove this for the simplified case of a function $f : \{0,1\}^n \rightarrow \{0,1\}$ with n input bits and a single output bit. Such a function is known as a Boolean function, and the corresponding circuit is a Boolean circuit. The general universality proof follows immediately from the special case of Boolean functions. The proof is by induction on n. For $n = 1$ there are four possible functions: the identity, which has a circuit consisting of a single wire; the bit flip, which is implemented using a single not gate; the function which replaces the input bit with a 0 , which can be obtained by anding the input with a work bit initially in the 0 state; and the function which replaces the input with a 1 , which can be obtained by oring the input with a work bit initially in the 1 state.

To complete the induction, suppose that any function on n bits may be computed by a circuit, and let f be a function on $n+1$ bits. Define n-bit functions f_0 and f_1 by $f_0(x_1, \ldots, x_n) \equiv f(0, x_1, \ldots, x_n)$ and $f_1(x_1, \ldots, x_n) \equiv f(1, x_1, \ldots, x_n)$. These are both n-bit functions, so by the inductive hypothesis there are circuits to compute these functions.

It is now an easy matter to design a circuit which computes f. The circuit computes both f_0 and f_1 on the last n bits of the input. Then, depending on whether the first bit of the input was a 0 or a 1 it outputs the appropriate answer. A circuit to do this is shown in Figure 3.8. This completes the induction.

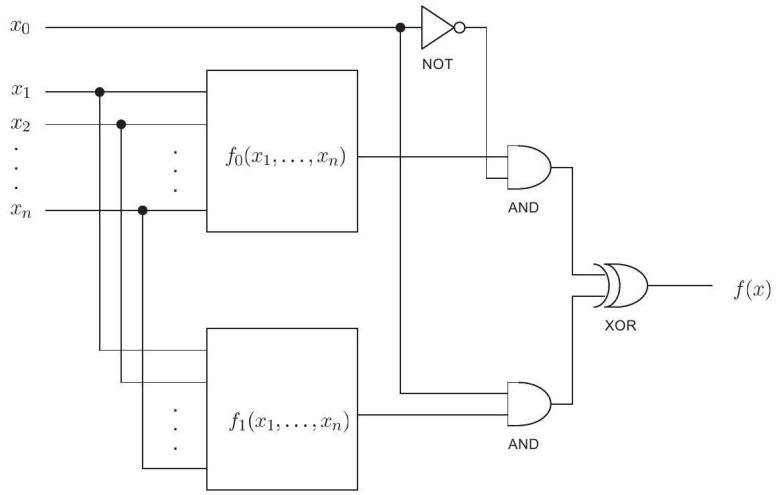


Figure 3.8. Circuit to compute an arbitrary function f on $n+1$ bits, assuming by induction that there are circuits to compute the n-bit functions f_0 and f_1.

Five elements may be identified in the universal circuit construction: (1) wires, which preserve the states of the bits; (2) ancilla bits prepared in standard states, used in the $n = 1$ case of the proof; (3) the FANOUT operation, which takes a single bit as input and outputs two copies of that bit; (4) the CROSSOVER operation, which interchanges the value of two bits; and (5) the AND, XOR, and not gates. In Chapter 4 we'll define the quantum circuit model of computation in a manner analogous to classical circuits. It is interesting to note that many of these five elements pose some interesting challenges when extending to the quantum case: it is not necessarily obvious that good quantum wires for the preservation of qubits can be constructed, even in principle, the fanout
operation cannot be performed in a straightforward manner in quantum mechanics, due to the no-cloning theorem (as explained in Section 1.3.5), and the AND and XOR gates are not invertible, and thus can't be implemented in a straightforward manner as unitary quantum gates. There is certainly plenty to think about in defining a quantum circuit model of computation!

Exercise 3.8: (Universality of NAND) Show that the NAND gate can be used to simulate the AND, XOR and NOT gates, provided wires, ancilla bits and FANOUT are available.

Let's return from our brief quantum digression, to the properties of classical circuits. We claimed earlier that the Turing machine model is equivalent to the circuit model of computation. In what sense do we mean the two models are equivalent? On the face of it, the two models appear quite different. The unbounded nature of a Turing machine makes them more useful for abstractly specifying what it is we mean by an algorithm, while circuits more closely capture what an actual physical computer does.

The two models are connected by introducing the notion of a uniform circuit family. A circuit family consists of a collection of circuits, $\{C_n\}$, indexed by a positive integer n. The circuit C_n has n input bits, and may have any finite number of extra work bits, and output bits. The output of the circuit C_n, upon input of a number x of at most n bits in length, is denoted by $C_n(x)$. We require that the circuits be consistent, that is, if $m < n$ and x is at most m bits in length, then $C_m(x) = C_n(x)$. The function computed by the circuit family $\{C_n\}$ is the function $C(\cdot)$ such that if x is n bits in length then $C(x) = C_n(x)$. For example, consider a circuit C_n that squares an n-bit number. This defines a family of circuits $\{C_n\}$ that computes the function, $C(x) = x^2$, where x is any positive integer.

It's not enough to consider unrestricted families of circuits, however. In practice, we need an algorithm to build the circuit. Indeed, if we don't place any restrictions on the circuit family

then it becomes possible to compute all sorts of functions which we do not expect to be able to compute in a reasonable model of computation. For example, let $h_n(x)$ denote the halting function, restricted to values of x which are n bits in length. Thus h_n is a function from n bits to 1 bit, and we have proved there exists a circuit C_n to compute $h_n(\cdot)$. Therefore the circuit family $\{C_n\}$ computes the halting function! However, what prevents us from using this circuit family to solve the halting problem is that we haven't specified an algorithm which will allow us to build the circuit C_n for all values of n. Adding this requirement results in the notion of a uniform circuit family.

That is, a family of circuits $\{C_n\}$ is said to be a uniform circuit family if there is some algorithm running on a Turing machine which, upon input of n, generates a description of C_n. That is, the algorithm outputs a description of what gates are in the circuit C_n, how those gates are connected together to form a circuit, any ancilla bits needed by the circuit, FANOUT and CROSSOVER operations, and where the output from the circuit should be read out. For example, the family of circuits we described earlier for squaring n-bit numbers is certainly a uniform circuit family, since there is an algorithm which, given n, outputs a description of the circuit needed to square an n-bit number. You can think of this algorithm as the means by which an engineer is able to generate a description of (and thus build) the circuit for any n whatsoever. By contrast, a circuit family that is not uniform is said to be a non-uniform circuit family. There is no algorithm to construct
the circuit for arbitrary n, which prevents our engineer from building circuits to compute functions like the halting function.

Intuitively, a uniform circuit family is a family of circuits that can be generated by some reasonable algorithm. It can be shown that the class of functions computable by uniform circuit families is exactly the same as the class of functions which can be computed on a Turing machine. With this uniformity restriction, results in the Turing machine model of computation can usually be given a straightforward translation into the circuit model of computation, and vice versa. Later we give similar attention to issues of uniformity in the quantum circuit model of computation.

7.3.4 3.2 The analysis of computational problems

The analysis of computational problems depends upon the answer to three fundamental questions:
(1) What is a computational problem? Multiplying two numbers together is a computational problem; so is programming a computer to exceed human abilities in the writing of poetry. In order to make progress developing a general theory for the analysis of computational problems we are going to isolate a special class of problems known as decision problems, and concentrate our analysis on those. Restricting ourselves in this way enables the development of a theory which is both elegant and rich in structure. Most important, it is a theory whose principles have application far beyond decision problems.
(2) How may we design algorithms to solve a given computational problem? Once a problem has been specified, what algorithms can be used to solve the problem? Are there general techniques which can be used to solve wide classes of problems? How can we be sure an algorithm behaves as claimed?
(3) What are the minimal resources required to solve a given computational problem? Running an algorithm requires the consumption of resources, such as time, space, and energy. In different situations it may be desirable to minimize consumption of one or more resource. Can we classify problems according to the resource requirements needed to solve them?

In the next few sections we investigate these three questions, especially questions 1 and 3. Although question 1, 'what is a computational problem?', is perhaps the most fundamental of

the questions, we shall defer answering it until Section 3.2.3, pausing first to establish some background notions related to resource quantification in Section 3.2.1, and then reviewing the key ideas of computational complexity in Section 3.2.2.

Question 2, how to design good algorithms, is the subject of an enormous amount of ingenious work by many researchers. So much so that in this brief introduction we cannot even begin to describe the main ideas employed in the design of good algorithms. If you are interested in this beautiful subject, we refer you to the end of chapter 'History and further reading'. Our closest direct contact with this subject will occur later in the book, when we study quantum algorithms. The techniques involved in the creation of quantum algorithms have typically involved a blend of deep existing ideas in algorithm design for classical computers, and the creation of new, wholly quantum mechanical techniques for algorithm design. For this reason, and because the spirit of quantum algorithm design
is so similar in many ways to classical algorithm design, we encourage you to become familiar with at least the basic ideas of algorithm design.

Question 3, what are the minimal resources required to solve a given computational problem, is the main focus of the next few sections. For example, suppose we are given two numbers, each n bits in length, which we wish to multiply. If the multiplication is performed on a single-tape Turing machine, how many computational steps must be executed by the Turing machine in order to complete the task? How much space is used on the Turing machine while completing the task?

These are examples of the type of resource questions we may ask. Generally speaking, computers make use of many different kinds of resources, however we will focus most of our attention on time, space, and energy. Traditionally in computer science, time and space have been the two major resource concerns in the study of algorithms, and we study these issues in Sections 3.2.2 through 3.2.4. Energy has been a less important consideration; however, the study of energy requirements motivates the subject of reversible classical computation, which in turn is a prerequisite for quantum computation, so we examine energy requirements for computation in some considerable detail in Section 3.2.5.

7.3.5 3.2.1 How to quantify computational resources

Different models of computation lead to different resource requirements for computation. Even something as simple as changing from a single-tape to a two-tape Turing machine may change the resources required to solve a given computational problem. For a computational task which is extremely well understood, like addition of integers, for example, such differences between computational models may be of interest. However, for a first pass at understanding a problem, we would like a way of quantifying resource requirements that is independent of relatively trivial changes in the computational model. One of the tools which has been developed to do this is the asymptotic notation, which can be used to summarize the essential behavior of a function. This asymptotic notation can be used, for example, to summarize the essence of how many time steps it takes a given algorithm to run, without worrying too much about the exact time count. In this section we describe this notation in detail, and apply it to a simple problem illustrating the quantification of computational resources - the analysis of algorithms for sorting a list of names into alphabetical order.

Suppose, for example, that we are interested in the number of gates necessary to add together two n-bit numbers. Exact counts of the number of gates required obscure the big picture: perhaps a specific algorithm requires $24n + 2\lceil \log n \rceil + 16$ gates to perform this task. However, in the limit of large problem size the only term which matters is the $24n$ term. Furthermore, we disregard constant factors as being of secondary importance to the analysis of the algorithm. The essential behavior of the algorithm is summed up by saying that the

number of operations required scales like n, where n is the number of bits in the numbers being added. The asymptotic notation consists of three tools which make this notion precise.

The O ('big O ') notation is used to set upper bounds on the behavior of a function. Suppose $f(n)$ and $g(n)$ are two functions on the non-negative integers. We say ' $f(n)$ is in the class of functions $O(g(n))$ ', or just ' $f(n)$ is $O(g(n))$ ', if there are constants c and n_0 such that for all values of n greater than $n_0, f(n) \leq cg(n)$. That is, for sufficiently large n, the function $g(n)$ is an upper bound on $f(n)$, up to an unimportant constant
factor. The big O notation is particularly useful for studying the worst-case behavior of specific algorithms, where we are often satisfied with an upper bound on the resources consumed by an algorithm.

When studying the behaviors of a class of algorithms - say the entire class of algorithms which can be used to multiply two numbers - it is interesting to set lower bounds on the resources required. For this the Ω ('big Omega') notation is used. A function $f(n)$ is said to be $\Omega(g(n))$ if there exist constants c and n_0 such that for all n greater than n_0, $cg(n) \leq f(n)$. That is, for sufficiently large $n, g(n)$ is a lower bound on $f(n)$, up to an unimportant constant factor.

Finally, the Θ ('big Theta') notation is used to indicate that $f(n)$ behaves the same as $g(n)$ asymptotically, up to unimportant constant factors. That is, we say $f(n)$ is $\Theta(g(n))$ if it is both $O(g(n))$ and $\Omega(g(n))$.

Asymptotic notation: examples

Let's consider a few simple examples of the asymptotic notation. The function $2n$ is in the class $O\left(n^2\right)$, since $2n \leq 2n^2$ for all positive n. The function 2^n is $\Omega\left(n^3\right)$, since $n^3 \leq 2^n$ for sufficiently large n. Finally, the function $7n^2 + \sqrt{n}\log(n)$ is $\Theta\left(n^2\right)$, since $7n^2 \leq 7n^2 + \sqrt{n}\log(n) \leq 8n^2$ for all sufficiently large values of n. In the following few exercises you will work through some of the elementary properties of the asymptotic notation that make it a useful tool in the analysis of algorithms.

Exercise 3.9: Prove that $f(n)$ is $O(g(n))$ if and only if $g(n)$ is $\Omega(f(n))$. Deduce that $f(n)$ is $\Theta(g(n))$ if and only if $g(n)$ is $\Theta(f(n))$.

Exercise 3.10: Suppose $g(n)$ is a polynomial of degree k. Show that $g(n)$ is $O\left(n^l\right)$ for any $l \geq k$.

Exercise 3.11: Show that $\log n$ is $O\left(n^k\right)$ for any $k > 0$.

Exercise 3.12: ($n^{\log n}$ is super-polynomial) Show that n^k is $O\left(n^{\log n}\right)$ for any k, but that $n^{\log n}$ is never $O\left(n^k\right)$.

Exercise 3.13: ($n^{\log n}$ is sub-exponential) Show that c^n is $\Omega\left(n^{\log n}\right)$ for any $c > 1$, but that $n^{\log n}$ is never $\Omega\left(c^n\right)$.

Exercise 3.14: Suppose $e(n)$ is $O(f(n))$ and $g(n)$ is $O(h(n))$. Show that $e(n)g(n)$ is $O(f(n)h(n))$.

An example of the use of the asymptotic notation in quantifying resources is the following simple application to the problem of sorting an n element list of names into alphabetical order. Many sorting algorithms are based upon the 'compare-and-swap' operation: two elements of an n element list are compared, and swapped if they are in the wrong order. If this compare-and-swap operation is the only means by which we can access the list, how many such operations are required in order to ensure that the list has been correctly sorted?

A simple compare-and-swap algorithm for solving the sorting problem is as follows: (note that compare-and-swap (j, k) compares the list entries numbered j and k, and swaps them if they are out of order)

```
for j = 1 to n-1
    for k = j+1 to n
```

```
        compare-and-swap(j,k)
    end k
end j
```

It is clear that this algorithm correctly sorts a list of n names into alphabetical order. Note that the number of compare-and-swap operations executed by the algorithm is $(n-1)+(n-2)+\cdots+1 = n(n-1)/2$. Thus the number of compare-and-swap operations used by the algorithm is $\Theta(n^2)$. Can we do better than this? It turns out that we can. Algorithms such as 'heapsort' are known which run using $O(n \log n)$ compare-andswap operations. Furthermore, in Exercise 3.15 you'll work through a simple counting argument that shows any algorithm based upon the compare-and-swap operation requires $\Omega(n \log n)$ such operations. Thus, the sorting problem requires $\Theta(n \log n)$ compare-andswap operations, in general.

Exercise 3.15: (Lower bound for compare-and-swap based sorts) Suppose an n element list is sorted by applying some sequence of compare-and-swap operations to the list. There are $n!$ possible initial orderings of the list. Show that after k of the compare-and-swap operations have been applied, at most 2^k of the possible initial orderings will have been sorted into the correct order. Conclude that $\Omega(n \log n)$ compare-and-swap operations are required to sort all possible initial orderings into the correct order.

7.3.6 3.2.2 Computational complexity

The idea that there won't be an algorithm to solve it - this is something fundamental that won't ever change - that idea appeals to me.

- Stephen Cook

Sometimes it is good that some things are impossible. I am happy there are many things that nobody can do to me.

- Leonid Levin

It should not come as a surprise that our choice of polynomial algorithms as the mathematical concept that is supposed to capture the informal notion of 'practically efficient computation' is open to criticism from all sides. [...] Ultimately, our argument for our choice must be this: Adopting polynomial worst-case performance as our criterion of efficiency results in an elegant and useful theory that says something meaningful about practical computation, and would be impossible without this simplification.

- Christos Papadimitriou

What time and space resources are required to perform a computation? In many cases these are the most important questions we can ask about a computational problem. Problems like addition and multiplication of numbers are regarded as efficiently solvable because we have fast algorithms to perform addition and multiplication, which consume
little space when running. Many other problems have no known fast algorithm, and are effectively impossible to solve, not because we can't find an algorithm to solve the problem, but because all known algorithms consume such vast quantities of space or time as to render them practically useless.

Computational complexity is the study of the time and space resources required to solve computational problems. The task of computational complexity is to prove lower bounds on the resources required by the best possible algorithm for solving a problem, even if that algorithm is not explicitly known. In this and the next two sections, we give an overview of computational

complexity, its major concepts, and some of the more important results of the field. Note that computational complexity is in a sense complementary to the field of algorithm design; ideally, the most efficient algorithms we could design would match perfectly with the lower bounds proved by computational complexity. Unfortunately, this is often not the case. As already noted, in this book we won't examine classical algorithm design in any depth.

One difficulty in formulating a theory of computational complexity is that different computational models may require different resources to solve the same problem. For instance, multiple-tape Turing machines can solve many problems substantially faster than single-tape Turing machines. This difficulty is resolved in a rather coarse way. Suppose a problem is specified by giving n bits as input. For instance, we might be interested in whether a particular n-bit number is prime or not. The chief distinction made in computational complexity is between problems which can be solved using resources which are bounded by a polynomial in n, or which require resources which grow faster than any polynomial in n. In the latter case we usually say that the resources required are exponential in the problem size, abusing the term exponential, since there are functions like $n^{\log n}$ which grow faster than any polynomial (and thus are 'exponential' according to this convention), yet which grow slower than any true exponential. A problem is regarded as easy, tractable or feasible if an algorithm for solving the problem using polynomial resources exists, and as hard, intractable or infeasible if the best possible algorithm requires exponential resources.

As a simple example, suppose we have two numbers with binary expansions $x_1 \ldots x_{m_1}$ and $y_1 \ldots y_{m_2}$, and we wish to determine the sum of the two numbers. The total size of the input is $n \equiv m_1 + m_2$. It's easy to see that the two numbers can be added using a number of elementary operations that scales as $\Theta(n)$; this algorithm uses a polynomial (indeed, linear) number of operations to perform its tasks. By contrast, it is believed (though it has never been proved!) that the problem of factoring an integer into its prime factors is intractable. That is, the belief is that there is no algorithm which can factor an arbitrary n-bit integer using $O(p(n))$ operations, where p is some fixed polynomial function of n. We will later give many other examples of problems which are believed to be intractable in this sense.

The polynomial versus exponential classification is rather coarse. In practice, an algorithm that solves a problem using $2^{n/1000}$ operations is probably more useful than one which runs in n^{1000} operations. Only for very large input sizes ($n \approx 10^8$) will the 'efficient' polynomial algorithm be preferable to the 'inefficient' exponential algorithm, and for many purposes it may be more practical to prefer the 'inefficient' algorithm.

Nevertheless, there are many reasons to base computational complexity primarily on the polynomial versus exponential classification. First, historically, with few exceptions, polynomial resource algorithms have been much faster than exponential algorithms. We
might speculate that the reason for this is lack of imagination: coming up with algorithms requiring n, n^2 or some other low degree polynomial number of operations is often much easier than finding a natural algorithm which requires n^{1000} operations, although examples like the latter do exist. Thus, the predisposition for the human mind to come up with relatively simple algorithms has meant that in practice polynomial algorithms usually do perform much more efficiently than their exponential cousins.

A second and more fundamental reason for emphasizing the polynomial versus exponential classification is derived from the strong Church-Turing thesis. As discussed in Section 1.1, it was observed in the 1960s and 1970s that probabilistic Turing machines appear to be the strongest 'reasonable' model of computation. More precisely, researchers consistently found that if it was possible to compute a function using k elementary operations in some model that was not the probabilistic Turing machine model of computation, then it was always possible to compute the same function in the probabilistic Turing machine model, using at most $p(k)$ elementary operations, where $p(\cdot)$ is some polynomial function. This statement is known as the

strong Church-Turing thesis:

> Strong Church-Turing thesis: Any model of computation can be simulated on a probabilistic Turing machine with at most a polynomial increase in the number of elementary operations required.

The strong Church-Turing thesis is great news for the theory of computational complexity, for it implies that attention may be restricted to the probabilistic Turing machine model of computation. After all, if a problem has no polynomial resource solution on a probabilistic Turing machine, then the strong Church-Turing thesis implies that it has no efficient solution on any computing device. Thus, the strong Church-Turing thesis implies that the entire theory of computational complexity will take on an elegant, model-independent form if the notion of efficiency is identified with polynomial resource algorithms, and this elegance has provided a strong impetus towards acceptance of the identification of 'solvable with polynomial resources' and 'efficiently solvable'. Of course, one of the prime reasons for interest in quantum computers is that they cast into doubt the strong Church-Turing thesis, by enabling the efficient solution of a problem which is believed to be intractable on all classical computers, including probabilistic Turing machines! Nevertheless, it is useful to understand and appreciate the role the strong Church-Turing thesis has played in the search for a model-independent theory of computational complexity.

Finally, we note that, in practice, computer scientists are not only interested in the polynomial versus exponential classification of problems. This is merely the first and coarsest way of understanding how difficult a computational problem is. However, it is an exceptionally important distinction, and illustrates many broader points about the nature of resource questions in computer science. For most of this book, it will be our central concern in evaluating the efficiency of a given algorithm.

Having examined the merits of the polynomial versus exponential classification, we now have to confess that the theory of computational complexity has one remarkable outstanding failure: it seems very hard to prove that there are interesting classes of problems which require exponential resources to solve. It is quite easy to give non-constructive proofs that most problems require exponential resources (see Exercise 3.16, below), and furthermore many interesting problems are conjectured to require exponential resources for their solution, but rigorous proofs seem very hard to come by, at least with the present
state of knowledge. This failure of computational complexity has important implications for quantum computation, because it turns out that the computational power of quantum computers can be related to some major open problems in classical computational complexity theory. Until these problems are resolved, it cannot be stated with certainty how computationally powerful a quantum computer is, or even whether it is more powerful than a classical computer!

Exercise 3.16: (Hard-to-compute functions exist) Show that there exist Boolean functions on n inputs which require at least $2^n/\log n$ logic gates to compute.

7.3.7 3.2.3 Decision problems and the complexity classes P and NP

Many computational problems are most cleanly formulated as decision problems - problems with a yes or no answer. For example, is a given number m a prime number or not? This is the primality decision problem. The main ideas of computational complexity are most easily and most often formulated in terms of decision problems, for two reasons: the theory takes its simplest and most elegant form in this form, while still generalizing in a natural way to more complex scenarios; and historically computational complexity arose primarily from the study of decision problems.

Although most decision problems can easily be stated in simple, familiar language, discussion of the general properties of decision problems is greatly helped by the terminology of formal languages. In this terminology, a language L over the alphabet Σ is a subset of the set Σ^* of all (finite) strings of symbols from Σ. For example, if $\Sigma = \{0, 1\}$, then the set of binary representations of even numbers, $L = \{0, 10, 100, 110, \ldots\}$ is a language over Σ.

Decision problems may be encoded in an obvious way as problems about languages. For instance, the primality decision problem can be encoded using the binary alphabet $\Sigma = \{0, 1\}$. Strings from Σ^* can be interpreted in a natural way as non-negative integers. For example, 0010 can be interpreted as the number 2. The language L is defined to consist of all binary strings such that the corresponding number is prime.

To solve the primality decision problem, what we would like is a Turing machine which, when started with a given number n on its input tape, eventually outputs some equivalent of 'yes' if n is prime, and outputs 'no' if n is not prime. To make this idea precise, it is convenient to modify our old Turing machine definition (of Section 3.1.1) slightly, replacing the halting state q_{h} with two states q_{Y} and q_{N} to represent the answers 'yes' and 'no' respectively. In all other ways the machine behaves in the same way, and it still halts when it enters the state q_{Y} or q_{N}. More generally, a language L is decided by a Turing machine if the machine is able to decide whether an input x on its tape is a member of the language of L or not, eventually halting in the state q_{Y} if $x \in L$, and eventually halting in the state q_{N} if $x \notin L$. We say that the machine has accepted or rejected x depending on which of these two cases comes about.

How quickly can we determine whether or not a number is prime? That is, what is the fastest Turing machine which decides the language representing the primality decision problem? We say that a problem is in TIME $(f(n))$ if there exists a Turing machine which decides whether a candidate x is in the language in time $O(f(n))$, where n is the length of x. A problem is said to be solvable in polynomial time if it is in TIME $\left(n^k\right)$ for some finite k. The collection of all languages which are in TIME $\left(n^k\right)$, for some k, is denoted $\mathbf{P}$.$\mathbf{P}$ is our first example of a complexity class. More generally, a complexity
class is defined to be a collection of languages. Much of computational complexity theory is concerned with the definition of various complexity classes, and understanding the relationship between different complexity classes.

Not surprisingly, there are problems which cannot be solved in polynomial time. Unfortunately, proving that any given problem can't be solved in polynomial time seems to be very difficult, although conjectures abound! A simple example of an interesting decision problem which is believed not to be in $\mathbf{P}$ is the factoring decision problem:

> FACTORING: Given a composite integer m and $l < m$, does m have a non-trivial factor less than l ?

An interesting property of factoring is that if somebody claims that the answer is 'yes, m does have a non-trivial factor less than l " then they can establish this by exhibiting such a factor, which can then be efficiently checked by other parties, simply by doing long-division. We call such a factor a witness to the fact that m has a factor less than l. This idea of an easily checkable witness is the key idea in the definition of the complexity class NP, below. We have phrased factoring as a decision problem, but you can easily verify that the decision problem is equivalent to finding the factors of a number:

Exercise 3.17: Prove that a polynomial-time algorithm for finding the factors of a number m exists if and only if the factoring decision problem is in $\mathbf{P}$.

Factoring is an example of a problem in an important complexity class known as NP. What distinguishes problems in NP is that 'yes' instances of a problem can easily be verified with the aid of an appropriate witness. More rigorously, a language L is in NP if there is a Turing machine M with the following properties:

(1) If $x \in L$ then there exists a witness string w such that M halts in the state $q_{\rm Y}$ after a time polynomial in $|x|$ when the machine is started in the state x-blank- w.
(2) If $x \notin L$ then for all strings w which attempt to play the role of a witness, the machine halts in state $q_{\rm N}$ after a time polynomial in $|x|$ when M is started in the state x-blank- w.

There is an interesting asymmetry in the definition of NP. While we have to be able to quickly decide whether a possible witness to $x \in L$ is truly a witness, there is no such need to produce a witness to $x \notin L$. For instance, in the factoring problem, we have an easy way of proving that a given number has a factor less than m, but exhibiting a witness to prove that a number has no factors less than m is more daunting. This suggests defining coNP, the class of languages which have witnesses to 'no' instances; obviously the languages in coNP are just the complements of languages in NP.

How are **P** and NP related? It is clear that **P** is a subset of NP. The most famous open problem in computer science is whether or not there are problems in NP which are not in **P**, often abbreviated as the $\mathbf{P} \neq \mathbf{NP}$ problem. Most computer scientists believe that $\mathbf{P} \neq \mathbf{NP}$, but despite decades of work nobody has been able to prove this, and the possibility remains that $\mathbf{P} = \mathbf{NP}$.

Exercise 3.18: Prove that if coNP $\neq$ NP then $\mathbf{P} \neq \mathbf{NP}$.

Upon first acquaintance it's tempting to conclude that the conjecture $\mathbf{P} \neq \mathbf{NP}$ ought to be pretty easy to resolve. To see why it's actually rather subtle it helps to see couple of examples of problems that are in **P** and NP. We'll draw the examples from graph theory, a rich source of decision problems with surprisingly many practical applications. A graph is a finite collection of vertices $\{v_1, \ldots, v_n\}$ connected by edges, which are pairs (v_i, v_j) of vertices. For now, we are only concerned with undirected graphs, in which the order of the vertices (in each edge pair) does not matter; similar ideas can be investigated for directed graphs in which the order of vertices does matter. A typical graph is illustrated in Figure 3.9.

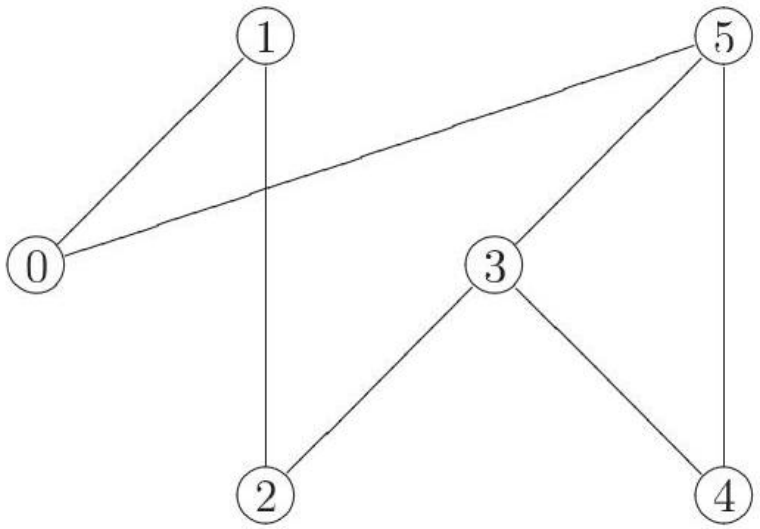


Figure 3.9. A graph.

A cycle in a graph is a sequence $v_1, \ldots, v_m$ of vertices such that each pair (v_j, v_{j+1}) is an edge, as is (v_1, v_m). A simple cycle is a cycle in which none of the vertices is repeated, except for the first and last vertices. A Hamiltonian cycle is a simple cycle which visits every vertex in the graph. Examples of graphs with and without Hamiltonian cycles are shown in Figure 3.10.

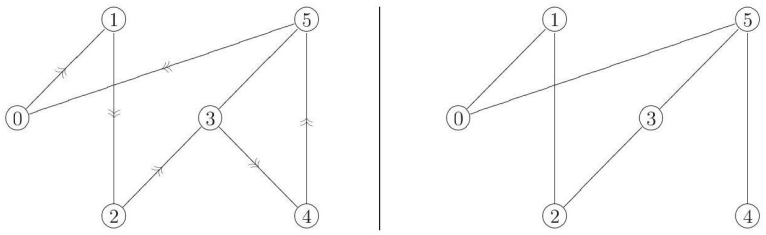


Figure 3.10. The graph on the left contains a Hamiltonian cycle, $0, 1, 2, 3, 4, 5, 0$. The graph on the right contains no Hamiltonian cycle, as can be verified by inspection.

The Hamiltonian cycle problem (HC) is to determine whether a given graph contains a Hamiltonian cycle or not. HC is a decision problem in NP, since if a given graph has a Hamiltonian cycle, then that cycle can be used as an easily checkable witness. Moreover, HC has no known polynomial time algorithm. Indeed, HC is a problem in the class of so-called NP-complete problems, which can be thought of as the 'hardest' problems in **NP**, in the sense that solving HC in time t allows any other problem in NP to be solved in time $O(\mathrm{pol}\, y(t))$. This also means that if any NP-complete problem has a polynomial time solution then it will follow that $\mathbf{P} = \mathbf{NP}$.

There is a problem, the Euler cycle decision problem, which is superficially similar to HC, but which has astonishingly different properties. An Euler cycle is an ordering of the edges of a graph G so that every edge in the graph is visited exactly once. The Euler
cycle decision problem (EC) is to determine, given a graph G on n vertices, whether that graph contains an Euler cycle or not. EC is, in fact, exactly the same problem as HC, only the path visits edges, rather than vertices. Consider the following remarkable theorem, to be proven in Exercise 3.20:

Theorem 3.1: (Euler's theorem) A connected graph contains an Euler cycle if and only if every vertex has an even number of edges incident upon it.

Euler's theorem gives us a method for efficiently solving EC. First, check to see whether the graph is connected; this is easily done with $O\left(n^2\right)$ operations, as shown in Exercise 3.19. If the graph is not connected, then obviously no Euler cycle exists. If the graph is connected then for each vertex check whether there is an even number of edges incident upon the vertex. If a vertex is found for which this is not the case, then there is no Euler cycle, otherwise an Euler cycle exists. Since there are n vertices, and at most $n(n-1)/2$ edges, this algorithm requires $O\left(n^3\right)$ elementary operations. Thus EC is in P! Somehow, there is a structure present in the problem of visiting each edge that can be exploited to provide an efficient algorithm for EC, yet which does not seem to be reflected in the problem of visiting each vertex; it is not at all obvious why such a structure should be present in one case, but not in the other, if indeed it is absent for the HC problem.

Exercise 3.19: The reachability problem is to determine whether there is a path between two specified vertices in a graph. Show that reachability can be solved using $O(n)$ operations if the graph has n vertices. Use the solution to reachability to show that it is possible to decide whether a graph is connected in $O\left(n^2\right)$ operations.

Exercise 3.20: (Euler's theorem) Prove Euler's theorem. In particular, if each vertex has an even number of incident edges, give a constructive procedure for finding an Euler cycle.

The equivalence between the factoring decision problem and the factoring problem proper is a special instance of one of the most important ideas in computer science, an idea known as reduction. Intuitively, we know that some problems can be viewed as special instances of other problems. A less trivial example of reduction is the reduction of HC to the traveling salesman decision problem (TSP). The traveling salesman decision problem is as follows: we are given

n cities $1, 2, \ldots, n$ and a non-negative integer distance d_{ij} between each pair of cities. Given a distance d the problem is to determine if there is a tour of all the cities of distance less than d.

The reduction of HC to TSP goes as follows. Suppose we have a graph containing n vertices. We turn this into an instance of TSP by thinking of each vertex of the graph as a 'city' and defining the distance d_{ij} between cities i and j to be one if vertices i and j are connected, and the distance to be two if the vertices are unconnected. Then a tour of the cities of distance less than $n + 1$ must be of distance n, and be a Hamiltonian cycle for the graph. Conversely, if a Hamiltonian cycle exists then a tour of the cities of distance less than $n + 1$ must exist. In this way, given an algorithm for solving TSP, we can convert it into an algorithm for solving HC without much overhead. Two consequences can be inferred from this. First, if TSP is a tractable problem, then HC is also tractable. Second, if HC is hard then TSP must also be hard. This is an example of a general technique known
as reduction: we've reduced the problem HC to the problem TSP. This is a technique we will use repeatedly throughout this book.

A more general notion of reduction is illustrated in Figure 3.11. A language B is said to be reducible to another language A if there exists a Turing machine operating in polynomial time such that given as input x it outputs $R(x)$, and $x \in B$ if and only if $R(x) \in A$. Thus, if we have an algorithm for deciding A, then with a little extra overhead we can decide the language B. In this sense, the language B is essentially no more difficult to decide than the language A.

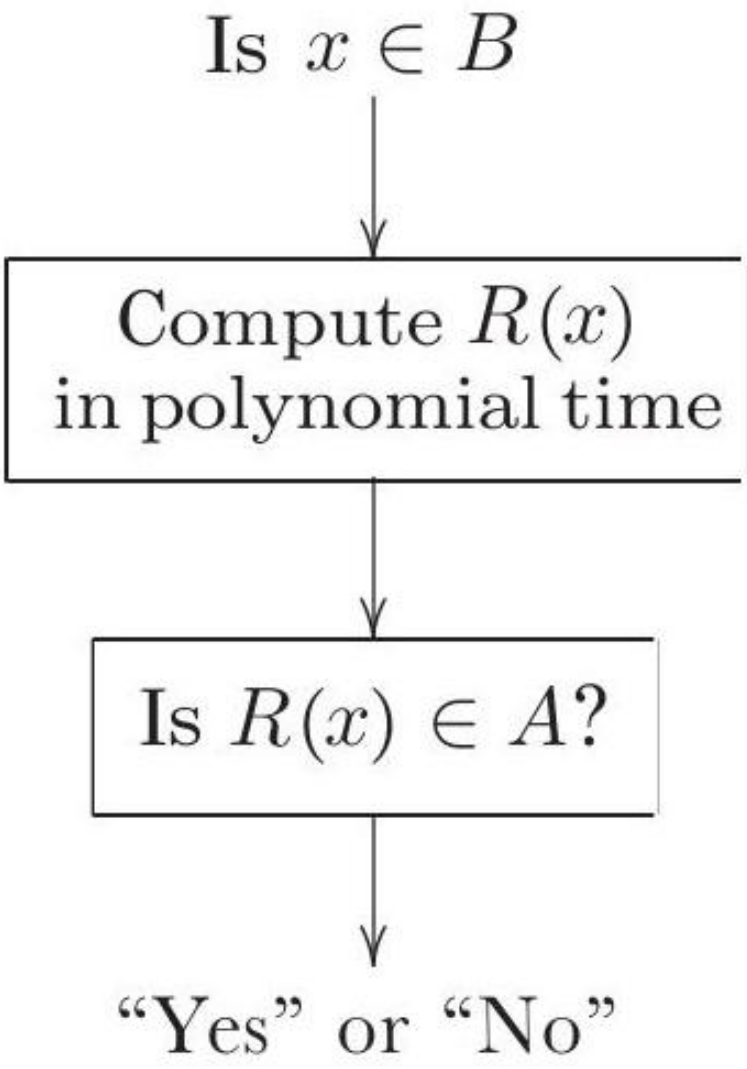


Figure 3.11. Reduction of B to A.

Exercise 3.21: (Transitive property of reduction) Show that if a language L_1 is reducible to the language L_2 and the language L_2 is reducible to L_3 then the language L_1 is reducible to the language L_3.

Some complexity classes have problems which are complete with respect to that complexity class, meaning there is a language L in the complexity class which is the 'most difficult' to decide, in the sense that every other language in the complexity class can be reduced to L. Not all complexity classes have complete problems, but many of the complexity classes we are concerned with do have complete problems. A trivial example is provided by **P**. Let L be any language in **P** which is not empty or equal to the set of all words. That is, there exists a string x_1 such that $x_1 \notin L$ and a string x_2 such that $x_2 \in L$. Then any other language L' in **P** can be reduced to L using the following reduction: given an input x, use the polynomial time decision procedure to determine whether $x \in L'$ or not. If it is not, then set $R(x) = x_1$, otherwise set $R(x) = x_2$.

Exercise 3.22: Suppose L is complete for a complexity class, and L' is another language in the complexity class such that L reduces to L'. Show that L' is complete for the complexity class.

Less trivially, NP also contains complete problems. An important example of such a problem and the prototype for all other NP-complete problems is the circuit satisfiability problem or CSAT: given a Boolean circuit composed of AND, OR and NOT gates, is there an assignment of values to the inputs to the circuit that results in the circuit outputting 1, that is, is the circuit satisfiable for some input? The NP-completeness of CSAT is known as the Cook-Levin theorem, for which we now outline a proof.

Theorem 3.2: (Cook-Levin) CSAT is NP-complete.

Proof

The proof has two parts. The first part of the proof is to show that CSAT is in NP, and the second part is to show that any language in NP can be reduced to CSAT. Both parts of the proof are based on simulation techniques: the first part of the proof is essentially showing that a Turing machine can efficiently simulate a circuit, while the second part of the proof is essentially showing that a circuit can efficiently simulate a Turing machine. Both parts of the proof are quite straightforward; for the purposes of illustration we give the second part in some detail.

The first part of the proof is to show that CSAT is in NP. Given a circuit containing n circuit elements, and a potential witness w, it is obviously easy to check in polynomial time on a Turing machine whether or not w satisfies the circuit, which establishes that CSAT is in NP.

The second part of the proof is to show that any language $L \in \mathbf{NP}$ can be reduced to CSAT. That is, we aim to show that there is a polynomial time computable reduction R such that $x \in L$ if and only if $R(x)$ is a satisfiable circuit. The idea of the reduction is to find a circuit which simulates the action of the machine M which is used to check instance-witness pairs, (x, w), for the language L. The input variables for the circuit will represent the witness; the idea is that finding a witness which satisfies the circuit is equivalent to M accepting (x, w) for some specific witness w. Without loss of generality we may make the following assumptions about M to simplify the construction:

(1) M 's tape alphabet is $\triangleright, 0, 1$ and the blank symbol.

(2) M runs using time at most $t(n)$ and total space at most $s(n)$ where $t(n)$ and $s(n)$ are polynomials in n.

(3) Machine M can actually be assumed to run using time exactly $t(n)$ for all inputs of size n. This is done by adding the lines $\langle q_Y, x, q_Y, x, 0\rangle$, and $\langle q_N, x, q_N, x, 0\rangle$ for each of $x = \triangleright, 0, 1$ and the blank, artificially halting the machine after exactly $t(n)$ steps.

The basic idea of the construction to simulate M is outlined in Figure 3.12. Each internal state

of the Turing machine is represented by a single bit in the circuit. We name the corresponding bits $\tilde{q}_{\mathrm{s}}, \tilde{q}_1, \ldots, \tilde{q}_m, \tilde{q}_{\mathrm{Y}}, \tilde{q}_{\mathrm{N}}$. Initially, $\tilde{q}_{\mathrm{s}}$ is set to one, and all the other bits representing internal states are set to zero. Each square on the Turing machine tape is represented by three bits: two bits to represent the letter of the alphabet ($\triangleright, 0, 1$ or blank) currently residing on the tape, and a single 'flag' bit which is set to one if the read-write head is pointing to the square, and set to zero otherwise. We denote the bits representing the tape contents by $(u_1, v_1), \ldots, \left(u_{s(n)}, v_{s(n)}\right)$ and the corresponding flag bits by $f_1, \ldots, f_{s(n)}$. Initially the u_j and v_j bits are set to represent the inputs x and w, as appropriate, while $f_1 = 1$ and all other $f_j = 0$. There is also a lone extra 'global flag' bit, F, whose function will be explained later. F is initially set to zero. We regard all the bits input to the circuit as fixed, except for those representing the witness w, which are the variable bits for the circuit.

The action of M is obtained by repeating $t(n)$ times a 'simulation step' which simulates the execution of a single program line for the Turing machine. Each simulation step may be broken up into a sequence of steps corresponding in turn to the respective program lines, with a final step which resets the global flag F to zero, as

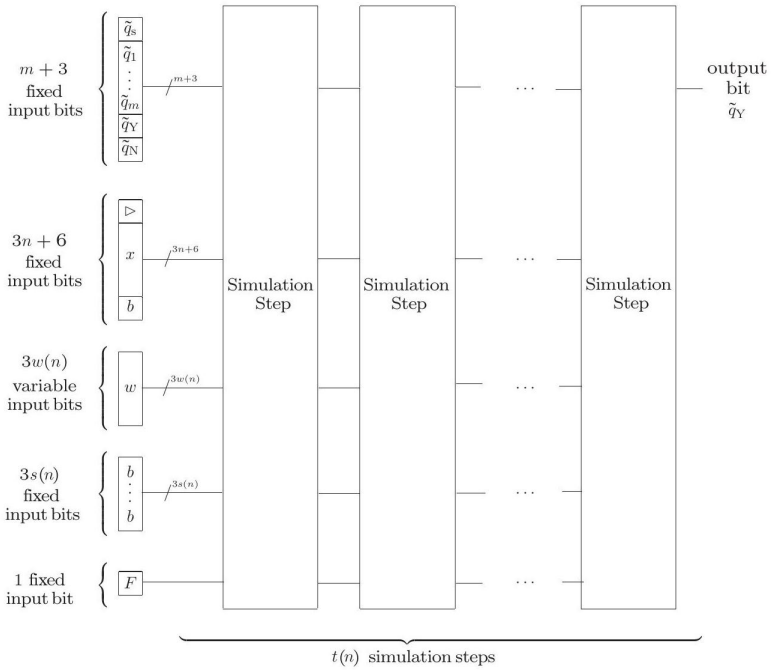


Figure 3.12. Outline of the procedure used to simulate a Turing machine using a circuit.

illustrated in Figure 3.13. To complete the simulation, we only need to simulate a program line of the form $\langle q_i, x, q_j, x', s\rangle$. For convenience, we assume $q_i \neq q_j$, but a similar construction works in the case when $q_i = q_j$. The procedure is as follows:
(1) Check to see that $\tilde{q}_i = 1$, indicating that the current state of the machine is q_i.
(2) For each tape square:
(a) Check to see that the global flag bit is set to zero, indicating that no action has yet been taken by the Turing machine.
(b) Check that the flag bit is set to one, indicating that the tape head is at this tape square.
(c) Check that the simulated tape contents at this point are x.
(d) If all conditions check out, then perform the following steps:

1. Set $\tilde{q}_i = 0$ and $\tilde{q}_j = 1$.

2. Update the simulated tape contents at this tape square to x'.

3. Update the flag bit of this and adjacent 'squares' as appropriate, depending on whether $s = +1, 0, -1$, and whether we are at the left hand end of the tape.

4. Set the global flag bit to one, indicating that this round of computation has been completed.

This is a fixed procedure which involves a constant number of bits, and by the universality result of Section 3.1.2 can be performed using a circuit containing a constant number of gates.

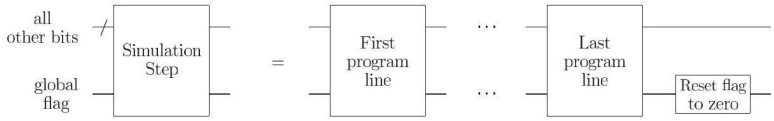


Figure 3.13. Outline of the simulation step used to simulate a Turing machine using a circuit.

The total number of gates in the entire circuit is easily seen to be $O(t(n)(s(n)+n))$, which is polynomial in size. At the end of the circuit, it is clear that $\tilde{q}_Y = 1$ if and only if the machine M accepts (x, w). Thus, the circuit is satisfiable if and only if there exists w such that machine M accepts (x, w), and we have found the desired reduction from L to CSAT. □

CSAT gives us a foot in the door which enables us to easily prove that many other problems are NP-complete. Instead of directly proving that a problem is NP-complete, we can instead prove that it is in NP and that CSAT reduces to it, so by Exercise 3.22 the problem must be NP-complete. A small sample of NP-complete problems is discussed in Box 3.3. An example of another NP-complete problem is the satisfiability problem (sat), which is phrased in terms of a Boolean formula. Recall that a Boolean formula φ is composed of the following elements: a set of Boolean variables, $x_1, x_2, \ldots$; Boolean connectives, that is, a Boolean function with one or two inputs and one output, such as $\wedge$ (AND), $\vee$ (OR), and $\neg$ (NOT); and parentheses. The truth or falsity of a Boolean formula for a given set of Boolean variables is decided according to the usual laws of Boolean algebra. For example, the formula $\varphi = x_1 \vee \neg x_2$ has the satisfying assignment $x_1 = 0$ and $x_2 = 0$, while $x_1 = 0$ and $x_2 = 1$ is not a satisfying assignment. The satisfiability problem is to determine, given a Boolean formula φ, whether or not it is satisfiable by any set of possible inputs.

Exercise 3.23: Show that SAT is NP-complete by first showing that SAT is in NP, and then showing that CSAT reduces to SAT. (Hint: for the reduction it may help to represent each distinct wire in an instance of CSAT by different variables in a Boolean formula.)

An important restricted case of SAT is also NP-complete, the 3-satisfiability problem (3sat), which is concerned with formulae in 3-conjunctive normal form. A formula is said to be in conjunctive normal form if it is the AND of a collection of clauses, each of which is the OR of one or more literals, where a literal is an expression is of the form x or $\neg x$. For example, the formula $(x_1 \vee \neg x_2) \wedge (x_2 \vee x_3 \vee \neg x_4)$ is in conjunctive normal form. A formula is in 3-conjunctive normal form or 3-CNF if each clause has exactly three literals. For example, the formula $(\neg x_1 \vee x_2 \vee \neg x_2) \wedge (\neg x_1 \vee x_3 \vee \neg x_4) \wedge (x_2 \vee x_3 \vee x_4)$ is in 3 -conjunctive normal form. The 3 -satisfiability problem is to determine whether a formula in 3-conjunctive normal form is satisfiable or not.

The proof that 3SAT is NP-complete is straightforward, but is a little too lengthy to justify inclusion in this overview. Even more than CSAT and SAT, 3sat is in some sense
the NP-complete problem, and it is the basis for countless proofs that other problems are NP-complete. We conclude our discussion of NP-completeness with the surprising fact that 2SAT, the analogue of 3SAT in which every clause has two literals, can be solved in polynomial time:

Exercise 3.24: (2SAT has an efficient solution) Suppose φ is a Boolean formula in conjunctive normal form, in which each clause contains only two literals.

(1) Construct a (directed) graph $G(\varphi)$ with directed edges in the following way: the vertices of G correspond to variables x_j and their negations $\neg x_j$ in φ. There is a (directed) edge (α, β) in G if and only if the clause $(\neg\alpha \vee \beta)$ or the clause $(\beta \vee \neg\alpha)$ is present in φ. Show that φ is not satisfiable if and only if there exists a variable x such that there are paths from x to $\neg x$ and from $\neg x$ to x in $G(\varphi)$.
(2) Show that given a directed graph G containing n vertices it is possible to determine whether two vertices v_1 and v_2 are connected in polynomial time.
(3) Find an efficient algorithm to solve 2SAT.

Box 3.3: A zoo of NP-complete problems

The importance of the class NP derives, in part, from the enormous number of computational problems that are known to be NP-complete. We can't possibly hope to survey this topic here (see 'History and further reading'), but the following examples, taken from many distinct areas of mathematics, give an idea of the delicious melange of problems known to be NP-complete.

- Clique (graph theory): A clique in an undirected graph G is a subset of vertices, each pair of which is connected by an edge. The size of a clique is the number of vertices it contains. Given an integer m and a graph G, does G have a clique of size m ?
- SUBSET-SUM (arithmetic): Given a finite collection S of positive integers and a target t, is there any subset of S which sums to t ?
- 0-1 INTEGER PROGRAMMING (linear programming): Given an integer $m \times n$ matrix A and an m-dimensional vector y with integer values, does there exist an n-dimensional vector x with entries in the set $\{0, 1\}$ such that $Ax \leq y$?
- VERTEX COVER (graph theory): A vertex cover for an undirected graph G is a set of vertices V' such that every edge in the graph has one or both vertices contained in V'. Given an integer m and a graph G, does G have a vertex cover V' containing m vertices?

Assuming that $\mathbf{P} \neq \mathbf{NP}$ it is possible to prove that there is a non-empty class of problems NPI (NP intermediate) which are neither solvable with polynomial resources, nor are NP-complete. Obviously, there are no problems known to be in NPI (otherwise we would know that $\mathbf{P} \neq \mathbf{NP}$) but there are several problems which are regarded as being likely candidates. Two of the strongest candidates are the factoring and graph isomorphism problems:

> GRAPH ISOMORPHISM: Suppose G and G' are two undirected graphs over the vertices $V \equiv \{v_1, \ldots, v_n\}$. Are G and G' isomorphic? That is, does there exist a one-to-one function $\varphi : V \to V$ such that the edge (v_i, v_j) is contained in G if and only if $(\varphi(v_i), \varphi(v_j))$ is contained in G ?

Problems in NPI are interesting to researchers in quantum computation and quantum information for two reasons. First, it is desirable to find fast quantum algorithms to solve problems which are not in **P**. Second, many suspect that quantum computers will not be able to efficiently solve all problems in NP, ruling out NP-complete problems. Thus, it is natural to focus on the class NPI. Indeed, a fast quantum algorithm for factoring has been discovered (Chapter 5), and this has motivated the search for fast quantum algorithms for other problems suspected to be in NPI.

7.3.8 3.2.4 A plethora of complexity classes

We have investigated some of the elementary properties of some important complexity classes. A veritable pantheon of complexity classes exists, and there are many non-trivial relationships known or suspected between these classes. For quantum computation and quantum information, it is not necessary to understand all the different complexity classes that have been defined. However, it is useful to have some appreciation for the more important of the complexity classes, many of which have natural analogues in the study of quantum computation and quantum information. Furthermore, if we are to understand how powerful quantum computers are, then it behooves us to understand how the class of problems solvable on a quantum computer fits into the zoo of complexity classes which may be defined for classical computers.

There are essentially three properties that may be varied in the definition of a complexity class: the resource of interest (time, space, . . .), the type of problem being considered (decision problem, optimization problem, ...), and the underlying computational model (deterministic Turing machine, probabilistic Turing machine, quantum computer, . . .). Not surprisingly, this gives us an enormous range to define complexity classes. In this section, we briefly review a few of the more important complexity classes and some of their elementary properties. We begin with a complexity class defined by changing the resource of interest from time to space.

The most natural space-bounded complexity class is the class PSPACE of decision problems which may be solved on a Turing machine using a polynomial number of working bits, with no limitation on the amount of time that may be used by the machine (see Exercise 3.25). Obviously, **P** is included in PSPACE, since a Turing machine that halts after polynomial time can only traverse polynomially many squares, but it is also true that NP is a subset of PSPACE. To see this, suppose L is any language in NP. Suppose problems of size n have witnesses of size at most $p(n)$, where $p(n)$ is some polynomial in n. To determine whether or not the problem has a solution, we may sequentially test all $2^{p(n)}$ possible witnesses. Each test can be run in polynomial time, and therefore polynomial space. If we erase all the intermediate working between tests then we can test all the possibilities using polynomial space.

Unfortunately, at present it is not even known whether PSPACE contains problems which are not in **P** ! This is a pretty remarkable situation - it seems fairly obvious that having unlimited time and polynomial spatial resources must be more powerful than having only a polynomial amount of time. However, despite considerable effort and ingenuity, this has never been shown. We will see later that the class of problems solvable on a quantum computer in polynomial time is a subset of PSPACE, so proving that a problem efficiently solvable on a quantum computer is not efficiently solvable on a classical computer would establish that P $\neq$ PSPACE, and thus solve a major outstanding problem of computer science. An optimistic way of looking at this result is that ideas from quantum computation might be useful in proving that **P** $\neq$ PSPACE. Pessimistically, one might conclude that it will be a long time before anyone rigorously proves that quantum computers can be used to efficiently solve problems that are intractable on a classical computer. Even more pessimistically, it is possible that P = PSPACE, in which case quantum computers offer no advantage over classical computers! However, very few (if any) computational complexity theorists believe that **P = PSPACE**.

Exercise 3.25: (PSPACE $\subseteq$ **EXP**) The complexity class EXP (for exponential time) contains all decision problems which may be decided by a Turing machine running in exponential time, that is time $O\left(2^{n^k}\right)$, where k is any constant. Prove that PSPACE $\subseteq$ EXP. (Hint: If a Turing machine has l internal states, an m letter alphabet, and uses space $p(n)$, argue that the machine can exist in one of at most $lm^{p(n)}$ different states, and that if the Turing machine is to avoid infinite loops then it must halt before revisiting a state.)

Exercise 3.26: (**L** $\subseteq$ **P**) The complexity class **L** (for logarithmic space) contains all decision

problems which may be decided by a Turing machine running in logarithmic space, that is, in space $O(\log(n))$. More precisely, the class **L** is defined using a two-tape Turing machine. The first tape contains the problem instance, of size n, and is a read-only tape, in the sense that only program lines which don't change the contents of the first tape are allowed. The second tape is a working tape which initially contains only blanks. The logarithmic space requirement is imposed on the second, working tape only. Show that $\mathbf{L} \subseteq \mathbf{P}$.

Does allowing more time or space give greater computational power? The answer to this question is yes in both cases. Roughly speaking, the time hierarchy theorem states that TIME($f(n)$) is a proper subset of TIME $\big(f(n)\log^2(f(n))\big)$. Similarly, the space hierarchy theorem states that SPACE($f(n)$) is a proper subset of SPACE($f(n)\log(f(n))$), where SPACE($f(n)$) is, of course, the complexity class consisting of all languages that can be decided with spatial resources $O(f(n))$. The hierarchy theorems have interesting implications with respect to the equality of complexity classes. We know that

$$\mathbf{L} \subseteq \mathbf{P} \subseteq \mathbf{NP} \subseteq \mathbf{PSPACE} \subseteq \mathbf{EXP} \tag{3.1}$$

Unfortunately, although each of these inclusions is widely believed to be strict, none of them has ever been proved to be strict. However, the time hierarchy theorem implies that **P** is a strict subset of EXP, and the space hierarchy theorem implies that **L** is a strict subset of PSPACE! So we can conclude that at least one of the inclusions in (3.1) must be strict, although we do not know which one.

What should we do with a problem once we know that it is NP-complete, or that some other hardness criterion holds? It turns out that this is far from being the end of the story in problem analysis. One possible line of attack is to identify special cases of the problem which may be amenable to attack. For example, in Exercise 3.24 we saw that the 2SAT problem has an efficient solution, despite the NP-completeness of SAT.

Another approach is to change the type of problem which is being considered, a tactic which typically results in the definition of new complexity classes. For example, instead of finding exact solutions to an NP-complete problem, we can instead try to find good algorithms for finding approximate solutions to a problem. For example, the vertex cover problem is an NP-complete problem, yet in Exercise 3.27 we show that it is possible to efficiently find an approximation to the minimal vertex cover which is correct to within a factor two! On the other hand, in Problem 3.6 we show that it is not possible to find approximations to solutions of TSP correct to within any factor, unless $\mathbf{P} = \mathbf{NP}$!

Exercise 3.27: (Approximation algorithm for vertex cover) Let $G = (V, E)$ be an undirected graph. Prove that the following algorithm finds a vertex cover for G that is within a factor two of being a minimal vertex cover:

```
$V C=\emptyset$
$E^{\prime}=E$
do until $E^{\prime}=\emptyset$
    let $(\alpha, \beta)$ be any edge of $E^{\prime}$
    $V C=V C \cup\{\alpha, \beta\}$
    remove from $E^{\prime}$ every edge incident on $\alpha$ or $\beta$
return $V C$.
```

Why is it possible to approximate the solution of one NP-complete problem, but not another? After all, isn't it possible to efficiently transform from one problem to another? This is certainly true, however it is not necessarily true that this transformation preserves the notion of a 'good approximation' to a solution. As a result, the computational complexity theory of approximation algorithms for problems in NP has a structure that goes beyond the structure

of NP proper. An entire complexity theory of approximation algorithms exists, which unfortunately is beyond the scope of this book. The basic idea, however, is to define a notion of reduction that corresponds to being able to efficiently reduce one approximation problem to another, in such a way that the notion of good approximation is preserved. With such a notion, it is possible to define complexity classes such as MAXSNP by analogy to the class NP, as the set of problems for which it is possible to efficiently verify approximate solutions to the problem. Complete problems exist for MAXSNP, just as for NP, and it is an interesting open problem to determine how the class MAXSNP compares to the class of approximation problems which are efficiently solvable.

We conclude our discussion with a complexity class that results when the underlying model of computation itself is changed. Suppose a Turing machine is endowed with the ability to flip coins, using the results of the coin tosses to decide what actions to take during the computation. Such a Turing machine may only accept or reject inputs with a certain probability. The complexity class BPP (for bounded-error probabilistic time) contains all languages L with the property that there exists a probabilistic Turing machine M such that if $x \in L$ then M accepts x with probability at least $3/4$, and if $x \notin L$, then M rejects x with probability at least $3/4$. The following exercise shows that the choice of the constant $3/4$ is essentially arbitrary:

Exercise 3.28: (Arbitrariness of the constant in the definition of BPP) Suppose k is a fixed constant, $1/2 < k \leq 1$. Suppose L is a language such that there exists a Turing machine M with the property that whenever $x \in L, M$ accepts x with probability at least k, and whenever $x \notin L, M$ rejects x with probability at least k. Show that $L \in \mathbf{BPP}$.

Indeed, the Chernoff bound, discussed in Box 3.4, implies that with just a few repetitions of an algorithm deciding a language in BPP the probability of success can be amplified to the point where it is essentially equal to one, for all intents and purposes. For this reason, **BPP** even more than **P** is the class of decision problems which is usually regarded as being efficiently solvable on a classical computer, and it is the quantum analogue of BPP, known as BQP, that is most interesting in our study of quantum algorithms.

7.3.9 3.2.5 Energy and computation

Computational complexity studies the amount of time and space required to solve a computational problem. Another important computational resource is energy. In this section, we study the energy requirements for computation. Surprisingly, it turns out that computation, both classical and quantum, can in principle be done without expending any energy! Energy consumption in computation turns out to be deeply linked to the reversibility of the computation. Consider a gate like the NAND gate, which takes as input two bits, and produces a single bit as output. This gate is intrinsically irreversible because, given the output of the gate, the input is not uniquely determined. For example, if the output of the NAND gate is 1 , then the input could have been any one of 00,01 , or 10 . On the other hand, the not gate is an example of a reversible logic gate because, given the output of the not gate, it is possible to infer what the input must have been.

Another way of understanding irreversibility is to think of it in terms of information erasure. If a logic gate is irreversible, then some of the information input to the gate is lost irretrievably when the gate operates - that is, some of the information has been erased by the gate. Conversely, in a reversible computation, no information is ever erased, because the input can always be recovered from the output. Thus, saying that a computation is reversible is equivalent to saying that no information is erased during the computation.

What is the connection between energy consumption and irreversibility in computation? Landauer's principle provides the connection, stating that, in order to erase information, it is necessary to dissipate energy. More precisely, Landauer's principle may be stated as follows:

Landauer's principle (first form): Suppose a computer erases a single bit of information. The amount of energy dissipated into the environment is at least $k_{\rm B} T \ln 2$, where $k_{\rm B}$ is a universal constant known as Boltzmann's constant, and T is the temperature of the environment of the computer.

According to the laws of thermodynamics, Landauer's principle can be given an alternative form stated not in terms of energy dissipation, but rather in terms of entropy:

Landauer's principle (second form): Suppose a computer erases a single bit of information. The entropy of the environment increases by at least $k_{\rm B} \ln 2$, where $k_{\rm B}$ is Boltzmann's constant.

Justifying Landauer's principle is a problem of physics that lies beyond the scope of this

Box 3.4: BPP and the Chernoff bound

Suppose we have an algorithm for a decision problem which gives the correct answer with probability $1/2 + \epsilon$, and the wrong answer with probability $1/2 - \epsilon$. If we run the algorithm n times, then it seems reasonable to guess that the correct answer is whichever appeared most frequently. How reliably does this procedure work? The Chernoff bound is a simple result from elementary probability which answers this question.

Theorem 3.3: (The Chernoff bound) Suppose $X_1, \ldots, X_n$ are independent and identically distributed random variables, each taking the value 1 with probability $1/2 + \epsilon$, and the value 0 with probability $1/2 - \epsilon$. Then

$$p\left(\sum_{i=1}^{n} X_i \leq n/2\right) \leq e^{-2\epsilon^2 n} \tag{3.2}$$

Proof

Consider any sequence $(x_1, \ldots, x_n)$ containing at most $n/2$ ones. The probability of such a sequence occurring is maximized when it contains $\lfloor n/2 \rfloor$ ones, so

$$p\left(X_1 = x_1, \ldots, X_n = x_n\right) \leq \left(\frac{1}{2} - \epsilon\right)^{\frac{n}{2}} \left(\frac{1}{2} + \epsilon\right)^{\frac{n}{2}} \tag{3.3}$$

$$= \frac{\left(1 - 4\epsilon^2\right)^{\frac{n}{2}}}{2^n}. \tag{3.4}$$

There can be at most 2^n such sequences, so

$$p\left(\sum_i X_i \leq n/2\right) \leq 2^n \times \frac{\left(1 - 4\epsilon^2\right)^{\frac{n}{2}}}{2^n} = \left(1 - 4\epsilon^2\right)^{\frac{n}{2}}. \tag{3.5}$$

Finally, by calculus, $1 - x \leq \exp(-x)$, so

$$p\left(\sum_i X_i \leq n/2\right) \leq e^{-4\epsilon^2 n/2} = e^{-2\epsilon^2 n}. \tag{3.6}$$

What this tells us is that for fixed ϵ, the probability of making an error decreases exponentially quickly in the number of repetitions of the algorithm. In the case of BPP we have $\epsilon = 1/4$, so it takes only a few hundred repetitions of the algorithm to reduce the probability of error below 10^{-20}, at which point an error in one of the computer's components becomes much more likely than an error due to the probabilistic nature of the algorithm.

book - see the end of chapter 'History and further reading' if you wish to understand why Landauer's principle holds. However, if we accept Landauer's principle as given, then it raises a

number of interesting questions. First of all, Landauer's principle only provides a lower bound on the amount of energy that must be dissipated to erase information.

How close are existing computers to this lower bound? Not very, turns out to be the answer - computers circa the year 2000 dissipate roughly $500 k_B T \ln 2$ in energy for each elementary logical operation.

Although existing computers are far from the limit set by Landauer's principle, it is still an interesting problem of principle to understand how much the energy consumption can be reduced. Aside from the intrinsic interest of the problem, a practical reason for the interest follows from Moore's law: if computer power keeps increasing then the amount of energy dissipated must also increase, unless the energy dissipated per operation drops at least as fast as the rate of increase in computing power.

If all computations could be done reversibly, then Landauer's principle would imply no lower bound on the amount of energy dissipated by the computer, since no bits at all are erased during a reversible computation. Of course, it is possible that some other physical principle might require that energy be dissipated during the computation; fortunately, this turns out not to be the case. But is it possible to perform universal computation without erasing any information? Physicists can cheat on this problem to see in advance that the answer to this question must be yes, because our present understanding of the laws of physics is that they are fundamentally reversible. That is, if we know the final state of a closed physical system, then the laws of physics allow us to work out the initial state of the system. If we believe that those laws are correct, then we must conclude that hidden in the irreversible logic gates like AND and OR, there must be some underlying reversible computation. But where is this hidden reversibility, and can we use it to construct manifestly reversible computers?

We will use two different techniques to give reversible circuit-based models capable of universal computation. The first model, a computer built entirely of billiard balls and mirrors, gives a beautiful concrete realization of the principles of reversible computation. The second model, based on a reversible logic gate known as the Toffoli gate (which we first encountered in Section 1.4.1), is a more abstract view of reversible computation that will later be of great use in our discussion of quantum computation. It is also possible to build reversible Turing machines that are universal for computation; however, we won't study these here, since the reversible circuit models turn out to be much more useful for quantum computation.

The basic idea of the billiard ball computer is illustrated in Figure 3.14. Billiard ball 'inputs' enter the computer from the left hand side, bouncing off mirrors and each other, before exiting as 'outputs' on the right hand side. The presence or absence of a billiard ball at a possible input site is used to indicate a logical 1 or a logical 0 , respectively. The fascinating thing about this model is that it is manifestly reversible, insofar as its operation is based on the laws of classical mechanics. Furthermore, this model of computation turns out to be universal in the sense that it can be used to simulate an arbitrary computation in the standard circuit model of computation.

Of course, if a billiard ball computer were ever built it would be highly unstable. As any billiards player can attest, a billiard ball rolling frictionlessly over a smooth surface is easily knocked off course by small perturbations. The billiard ball model of computation depends on perfect operation, and the absence of external perturbations such as those caused by thermal noise. Periodic corrections can be performed, but information gained by doing this would have to be erased, requiring work to be performed. Expenditure of energy thus serves the purpose of reducing this susceptibility to noise, which is necessary for a practical, real-world computational machine. For the purposes of this introduction,

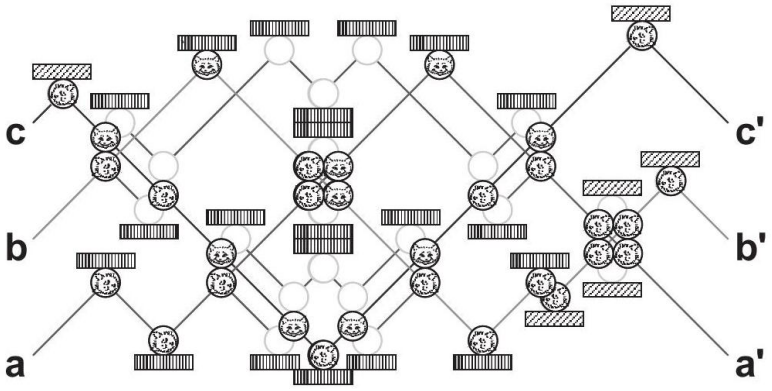


Figure 3.14. A simple billiard ball computer, with three input bits and three output bits, shown entering on the left and leaving on the right, respectively. The presence or absence of a billiard ball indicates a 1 or a 0 , respectively. Empty circles illustrate potential paths due to collisions. This particular computer implements the Fredkin classical reversible logic gate, discussed in the text.

we will ignore the effects of noise on the billiard ball computer, and concentrate on understanding the essential elements of reversible computation.

The billiard ball computer provides an elegant means for implementing a reversible universal logic gate known as the Fredkin gate. Indeed, the properties of the Fredkin gate provide an informative overview of the general principles of reversible logic gates and circuits. The Fredkin gate has three input bits and three output bits, which we refer to as a, b, c and a', b', c', respectively. The bit c is a control bit, whose value is not changed by the action of the Fredkin gate, that is, $c' = c$. The reason c is called the control bit is because it controls what happens to the other two bits, a and b. If c is set to 0 then a and b are left alone, $a' = a, b' = b$. If c is set to $1, a$ and b are swapped, $a' = b, b' = a$. The explicit truth table for the Fredkin gate is shown in Figure 3.15. It is easy to see that the Fredkin gate is reversible, because given the output a', b', c', we can determine the inputs a, b, c. In fact, to recover the original inputs a, b and c we need only apply another Fredkin gate to a', b', c' :

Exercise 3.29: (Fredkin gate is self-inverse) Show that applying two consecutive Fredkin gates gives the same outputs as inputs.

Examining the paths of the billiard balls in Figure 3.14, it is not difficult to verify that this billiard ball computer implements the Fredkin gate:

Exercise 3.30: Verify that the billiard ball computer in Figure 3.14 computes the Fredkin gate.

In addition to reversibility, the Fredkin gate also has the interesting property that the number of 1 s is conserved between the input and output. In terms of the billiard ball computer, this corresponds to the number of billiard balls going into the Fredkin gate being equal to the number coming out. Thus, it is sometimes referred to as being a conservative reversible logic gate. Such reversibility and conservative properties are interesting to a physicist because they can be motivated by fundamental physical princi-

Inputs			Outputs		
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	1	0	1
1	0	0	1	0	0
1	0	1	0	1	1
1	1	0	1	1	0
1	1	1	1	1	1

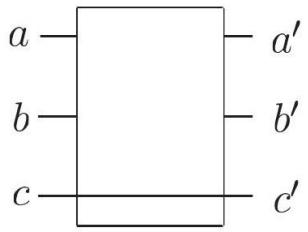


Figure 3.15. Fredkin gate truth table and circuit representation. The bits a and b are swapped if the control bit c is set, and otherwise are left alone.

ples. The laws of Nature are reversible, with the possible exception of the measurement postulate of quantum mechanics, discussed in Section 2.2.3 on page 84. The conservative property can be thought of as analogous to properties such as conservation of mass, or conservation of energy. Indeed, in the billiard ball model of computation the conservative property corresponds exactly to conservation of mass.

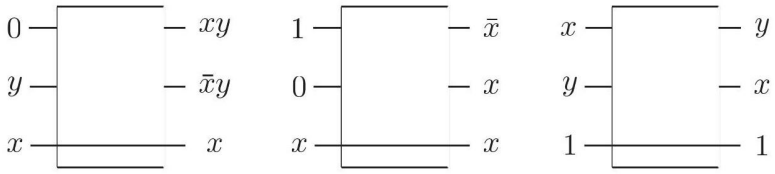


Figure 3.16. Fredkin gate configured to perform the elementary gates AND (left), NOT (middle), and a primitive routing function, the CROSSOVER (right). The middle gate also serves to perform the fanout operation, since it produces two copies of x at the output. Note that each of these configurations requires the use of extra 'ancilla' bits prepared in standard states - for example, the 0 input on the first line of the AND gate - and in general the output contains 'garbage' not needed for the remainder of the computation.

The Fredkin gate is not only reversible and conservative, it's a universal logic gate as well! As illustrated in Figure 3.16, the Fredkin gate can be configured to simulate and, not, crossover and fanout functions, and thus can be cascaded to simulate any classical circuit whatsoever.

To simulate irreversible gates such as AND using the Fredkin gate, we made use of two ideas. First, we allowed the input of 'ancilla' bits to the Fredkin gate, in specially prepared states, either 0 or 1 . Second, the output of the Fredkin gate contained extraneous 'garbage' not needed for the remainder of the computation. These ancilla and garbage bits are not directly important to the computation. Their importance lies in the fact that they make the computation reversible. Indeed the irreversibility of gates like the AND and OR may be viewed as a consequence of the ancilla and garbage bits being 'hidden'. Summarizing, given any classical circuit computing a function $f(x)$, we can build a reversible circuit made entirely of Fredkin gates, which on input of x, together with some ancilla bits
in a standard state a, computes $f(x)$, together with some extra 'garbage' output, $g(x)$. Therefore, we represent the action of the computation as $(x, a) \rightarrow (f(x), g(x))$.

We now know how to compute functions reversibly. Unfortunately, this computation produces unwanted garbage bits. With some modifications it turns out to be possible to perform

the computation so that any garbage bits produced are in a standard state. This construction is crucial for quantum computation, because garbage bits whose value depends upon x will in general destroy the interference properties crucial to quantum computation. To understand how this works it is convenient to assume that the not gate is available in our repertoire of reversible gates, so we may as well assume that the ancilla bits a all start out as 0 s , with not gates being added where necessary to turn the ancilla 0 s into 1 s . It will also be convenient to assume that the classical controlled-not gate is available, defined in a manner analogous to the quantum definition of Section 1.3.2, that is, the inputs (c, t) are taken to ($c, t \oplus c$), where $\oplus$ denotes addition modulo 2 . Notice that $t = 0$ gives $(c, 0) \rightarrow (c, c)$, so the controlled-not can be thought of as a reversible copying gate or fanout, which leaves no garbage bits at the output.

With the additional not gates appended at the beginning of the circuit, the action of the computation may be written as $(x, 0) \rightarrow (f(x), g(x))$. We could also have added CNOT gates to the beginning of the circuit, in order to create a copy of x which is not changed during the subsequent computation. With this modification, the action of the circuit may be written

$$(x, 0, 0) \rightarrow (x, f(x), g(x)). \tag{3.7}$$

Equation (3.7) is a very useful way of writing the action of the reversible circuit, because it allows an idea known as uncomputation to be used to get rid of the garbage bits, for a small cost in the running time of the computation. The idea is the following. Suppose we start with a four register computer in the state ($x, 0, 0, y$). The second register is used to store the result of the computation, and the third register is used to provide workspace for the computation, that is, the garbage bits $g(x)$. The use of the fourth register is described shortly, and we assume it starts in an arbitrary state y.

We begin as before, by applying a reversible circuit to compute f, resulting in the state ($x, f(x), g(x), y$). Next, we use CNOTs to add the result $f(x)$ bitwise to the fourth register, leaving the machine in the state $(x, f(x), g(x), y \oplus f(x))$. However, all the steps used to compute $f(x)$ were reversible and did not affect the fourth register, so by applying the reverse of the circuit used to compute f we come to the state ($x, 0, 0, y \oplus f(x)$). Typically, we omit the ancilla 0 s from the description of the function evaluation, and just write the action of the circuit as

$$(x, y) \rightarrow (x, y \oplus f(x)). \tag{3.8}$$

In general we refer to this modified circuit computing f as the reversible circuit computing f, even though in principle there are many other reversible circuits which could be used to compute f.

What resource overhead is involved in doing reversible computation? To analyze this question, we need to count the number of extra ancilla bits needed in a reversible circuit, and compare the gate counts with classical models. It ought to be clear that the number of gates in a reversible circuit is the same as in an irreversible circuit to within the constant factor which represents the number of Fredkin gates needed to simulate a single element of the irreversible circuit, and an additional factor of two for uncomputation, with an
overhead for the extra CNOT operations used in reversible computation which is linear in the number of bits involved in the circuit. Similarly, the number of ancilla bits required scales at most linearly with the number of gates in the irreversible circuit, since each element in the irreversible circuit can be simulated using a constant number of ancilla bits. As a result, natural complexity classes such as **P** and **NP** are the same no matter whether a reversible or irreversible model of computation is used. For more elaborate complexity classes like PSPACE the situation is not so immediately clear; see Problem 3.9 and 'History and further reading' for a discussion of some such subtleties.

Exercise 3.31: (Reversible half-adder) Construct a reversible circuit which, when two bits x and y are input, outputs $(x, y, c, x \oplus y)$, where c is the carry bit when x and y are added.

The Fredkin gate and its implementation using the billiard ball computer offers a beautiful paradigm for reversible computation. There is another reversible logic gate, the Toffoli gate, which is also universal for classical computation. While the Toffoli gate does not have quite the same elegant physical simplicity as the billiard ball implementation of the Fredkin gate, it will be more useful in the study of quantum computation. We have already met the Toffoli gate in Section 1.4.1, but for convenience we review its properties here.

The Toffoli gate has three input bits, a, b and c.a and b are known as the first and second control bits, while c is the target bit. The gate leaves both control bits unchanged, flips the target bit if both control bits are set, and otherwise leaves the target bit alone. The truth table and circuit representation for the Toffoli gate are shown in Figure 3.17.

Inputs			Outputs		
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

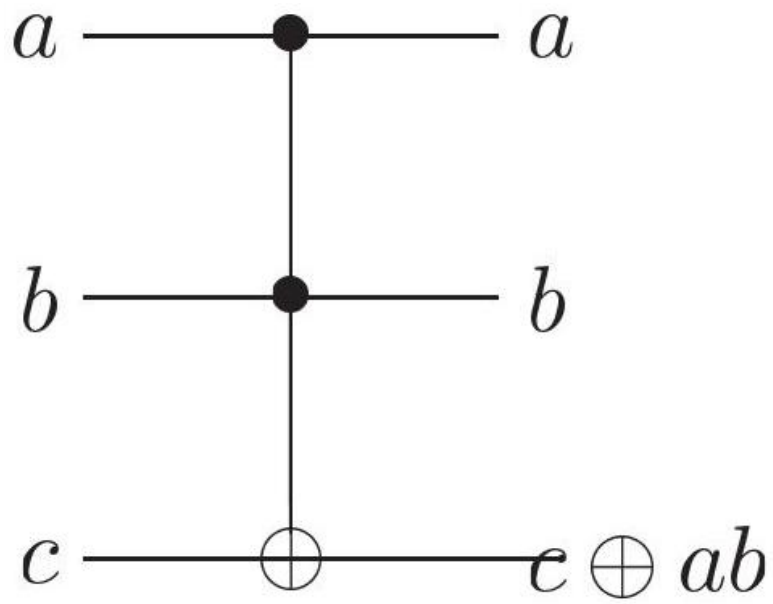


Figure 3.17. Truth table and circuit representation of the Toffoli gate.

How can the Toffoli gate be used to do universal computation? Suppose we wish to nand the bits a and b. To do this using the Toffoli gate, we input a and b as control bits, and send in an ancilla bit set to 1 as the target bit, as shown in Figure 3.18. The NAND of a and b is output as the target bit. As expected from our study of the Fredkin gate, the Toffoli gate simulation of a NAND requires the use of a special ancilla input, and some of the outputs from the simulation are garbage bits.

The Toffoli gate can also be used to implement the fanout operation by inputting an ancilla 1 to the first control bit, and a to the second control bit, producing the output $1, a, a$. This is illustrated in Figure 3.19. Recalling that NAND and FANOUT are together

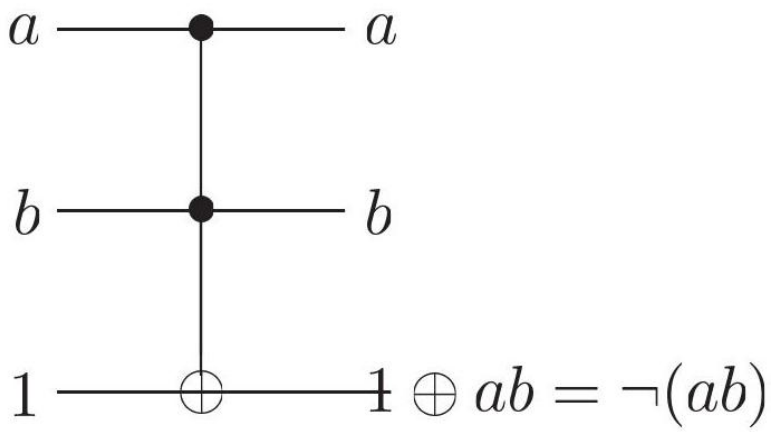


Figure 3.18. Implementing a NAND gate using a Toffoli gate. The top two bits represent the input to the NAND, while the third bit is prepared in the standard state 1, sometimes known as an ancilla state. The output from the NAND is on the third bit.

universal for computation, we see that an arbitrary circuit can be efficiently simulated using a reversible circuit consisting only of Toffoli gates and ancilla bits, and that useful additional techniques such as uncomputation may be achieved using the same methods as were employed with the Fredkin gate.

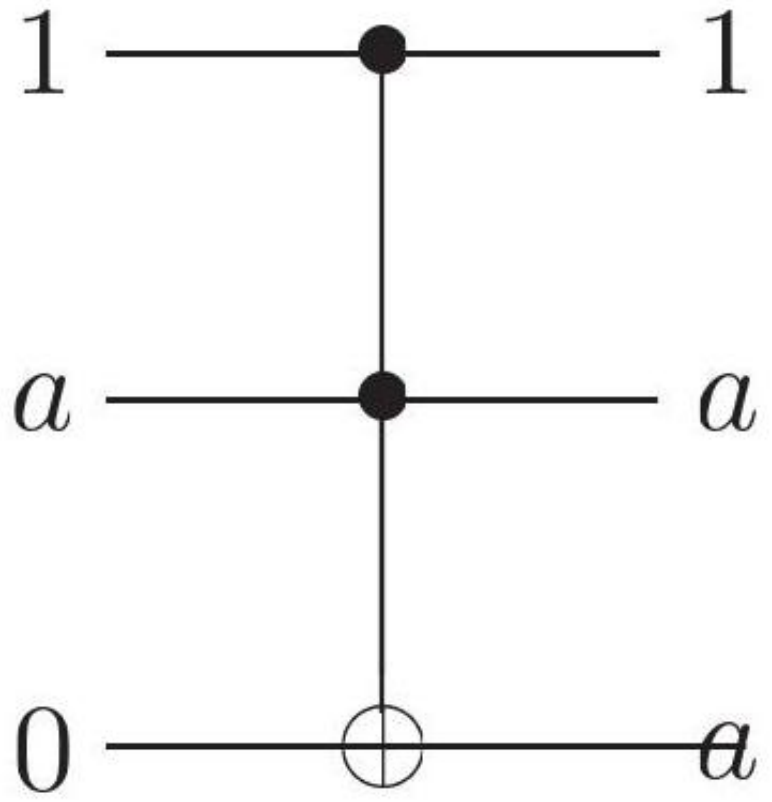


Figure 3.19. fanout with the Toffoli gate, with the second bit being the input to the fanout, and the other two bits standard ancilla states. The output from fanout appears on the second and third bits.

Our interest in reversible computation was motivated by our desire to understand the energy requirements for computation. It is clear that the noise-free billiard ball model of computation

requires no energy for its operation; what about models based upon the Toffoli gate? This can only be determined by examining specific models for the computation of the Toffoli gate. In Chapter 7, we examine several such implementations, and it turns out that, indeed, the Toffoli gate can be implemented in a manner which does not require the expenditure of energy.

There is a significant caveat attached to the idea that computation can be done without the expenditure of energy. As we noted earlier, the billiard ball model of computation is highly sensitive to noise, and this is true of many other models of reversible computation. To nullify the effects of noise, some form of error-correction needs to be done. Such error-correction typically involves the performance of measurements on the system to determine whether the system is behaving as expected, or if an error has occurred. Because the computer's memory is finite, the bits used to store the measurement results utilized in error-correction must eventually be erased to make way for new measurement results. According to Landauer's principle, this erasure carries an associated energy cost
that must be accounted for when tallying the total energy cost of the computation. We analyze the energy cost associated with error-correction in more detail in Section 12.4.4.

What can we conclude from our study of reversible computation? There are three key ideas. First, reversibility stems from keeping track of every bit of information; irreversibility occurs only when information is lost or erased. Second, by doing computation reversibly, we obviate the need for energy expenditure during computation. All computations can be done, in principle, for zero cost in energy. Third, reversible computation can be done efficiently, without the production of garbage bits whose value depends upon the input to the computation. That is, if there is an irreversible circuit computing a function f, then there is an efficient simulation of this circuit by a reversible circuit with action $(x, y) \rightarrow (x, y \oplus f(x))$.

What are the implications of these results for physics, computer science, and for quantum computation and quantum information? From the point of view of a physicist or hardware engineer worried about heat dissipation, the good news is that, in principle, it is possible to make computation dissipation-free by making it reversible, although in practice energy dissipation is required for system stability and immunity from noise. At an even more fundamental level, the ideas leading to reversible computation also lead to the resolution of a century-old problem in the foundations of physics, the famous problem of Maxwell's demon. The story of this problem and its resolution is outlined in Box 3.5 on page 162. From the point of view of a computer scientist, reversible computation validates the use of irreversible elements in models of computation such as the Turing machine (since using them or not gives polynomially equivalent models). Moreover, since the physical world is fundamentally reversible, one can argue that complexity classes based upon reversible models of computation are more natural than complexity classes based upon irreversible models, a point revisited in Problem 3.9 and 'History and further reading'. From the point of view of quantum computation and quantum information, reversible computation is enormously important. To harness the full power of quantum computation, any classical subroutines in a quantum computation must be performed reversibly and without the production of garbage bits depending on the classical input.

Exercise 3.32: (From Fredkin to Toffoli and back again) What is the smallest number of Fredkin gates needed to simulate a Toffoli gate? What is the smallest number of Toffoli gates needed to simulate a Fredkin gate?

7.3.10 3.3 Perspectives on computer science

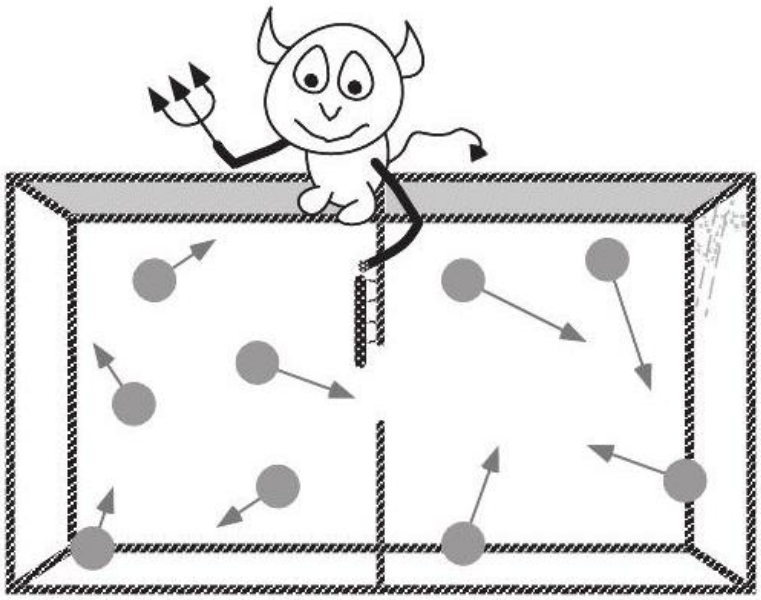
In a short introduction such as this chapter, it is not remotely possible to cover in detail all the great ideas of a field as rich as computer science. We hope to have conveyed to you something of what it means to think like a computer scientist, and provided a basic vocabulary and overview of some of the fundamental concepts important in the understanding of computation.

To conclude this chapter, we briefly touch on some more general issues, in order to provide some perspective on how quantum computation and quantum information fits into the overall picture of computer science.

Our discussion has revolved around the Turing machine model of computation. How does the computational power of unconventional models of computation such as massively parallel computers, DNA computers and analog computers compare with the standard

Box 3.5: Maxwell's demon

The laws of thermodynamics govern the amount of work that can be performed by a physical system at thermodynamic equilibrium. One of these laws, the second law of thermodynamics, states that the entropy in a closed system can never decrease. In 1871, James Clerk Maxwell proposed the existence of a machine that apparently violated this law. He envisioned a miniature little 'demon', like that shown in the figure below, which could reduce the entropy of a gas cylinder initially at equilibrium by individually separating the fast and slow molecules into the two halves of the cylinder. This demon would sit at a little door at the middle partition. When a fast molecule approaches from the left side the demon opens a door between the partitions, allowing the molecule through, and then closes the door. By doing this many times the total entropy of the cylinder can be decreased, in apparent violation of the second law of thermodynamics.



The resolution to the Maxwell's demon paradox lies in the fact that the demon must perform measurements on the molecules moving between the partitions, in order to determine their velocities. The result of this measurement must be stored in the demon's memory. Because any memory is finite, the demon must eventually begin erasing information from its memory, in order to have space for new measurement results. By Landauer's principle, this act of erasing information increases the total entropy of the combined system - demon, gas cylinder, and their environments. In fact, a complete analysis shows that Landauer's principle implies that the entropy of the combined system is increased at least as much by this act of erasing information as the entropy of the combined system is decreased by the actions of the demon, thus ensuring that the second law of thermodynamics is obeyed.

Turing machine model of computation and, implicitly, with quantum computation? Let's begin with parallel computing architectures. The vast majority of computers in existence are serial computers, processing instructions one at a time in some central processing unit. By contrast, parallel computers can process more than one instruction at a time, leading to a substantial savings in time and money for some applications. Nevertheless, parallel process-

ing does not offer any fundamental advantage over the standard Turing machine model when issues of efficiency are concerned, because a Turing machine can simulate a parallel computer with polynomially equivalent total physical resources - the total space and time used by the computation. What a parallel computer gains in time,
it loses in the total spatial resources required to perform the computation, resulting in a net of no essential change in the power of the computing model.

An interesting specific example of massively parallel computing is the technique of DNA computing. A strand of DNA, deoxyribonucleic acid, is a molecule composed of a sequence (a polymer) of four kinds of nucleotides distinguished by the bases they carry, denoted by the letter A (adenine), C (cytosine), G (guanine) and T (thymine). Two strands, under certain circumstances, can anneal to form a double strand, if the respective base pairs form complements of each other (A matches T and G matches C). The ends are also distinct and must match appropriately. Chemical techniques can be used to amplify the number of strands beginning or ending with specific sequences (polymerase chain reaction), separate the strands by length (gel electrophoresis), dissolve double strands into single strands (changing temperature and pH), read the sequence on a strand, cut strands at a specific position (restriction enzymes), and detect if a certain sequence of DNA is in a test tube. The procedure for using these mechanisms in a robust manner is rather involved, but the basic idea can be appreciated from an example.

The directed Hamiltonian path problem is a simple and equivalently hard variant of the Hamiltonian cycle problem of Section 3.2.2, in which the goal is to determine if a path exists or not between two specified vertices j_1 and j_N in a directed graph G of N vertices, entering each vertex exactly once, and following only allowed edge directions. This problem can be solved with a DNA computer using the following five steps, in which x_j are chosen to be unique sequences of bases (and $\bar{x}_j$ their complements), DNA strands $x_j x_k$ encode edges, and strands $\bar{x}_j \bar{x}_j$ encode vertices. (1) Generate random paths through G, by combining a mixture of all possible vertex and edge DNA strands, and waiting for the strands to anneal. (2) Keep only the paths beginning with j_1 and ending with j_N, by amplifying only the double strands beginning with $\bar{x}_{j_1}$ and ending with $\bar{x}_{j_N}$. (3) Select only paths of length N, by separating the strands according to their length. (4) Select only paths which enter each vertex at least once, by dissolving the DNA into single strands, and annealing with all possible vertex strands one at a time and filtering out only those strands which anneal. And (5) detect if any strands have survived the selection steps; if so, then a path exists, and otherwise, it does not. To ensure the answer is correct with sufficiently high probability, x_j may be chosen to contain many (≈ 30) bases, and a large number ($\approx 10^{14}$ or more are feasible) of strands are used in the reaction.

Heuristic methods are available to improve upon this basic idea. Of course, exhaustive search methods such as this only work as long as all possible paths can be generated efficiently, and thus the number of molecules used must grow exponentially as the size of the problem (the number of vertices in the example above). DNA molecules are relatively small and readily synthesized, and the huge number of DNA combinations one can fit into a test tube can stave off the exponential complexity cost increase for a while - up to a few dozen vertices - but eventually the exponential cost limits the applicability of this method. Thus, while DNA computing offers an attractive and physically realizable model of computation for the solution of certain problems, it is a classical computing technique and offers no essential improvement in principle over a Turing machine.

Analog computers offer a yet another paradigm for performing computation. A computer is analog when the physical representation of information it uses for computation is based on continuous degrees of freedom, instead of zeroes and ones. For example, a thermometer is an analog computer. Analog circuitry, using resistors, capacitors, and amplifiers, is also said to perform analog computation. Such machines have an infinite
resource to draw upon in the ideal limit, since continuous variables like position and voltage can

store an unlimited amount of information. But this is only true in the absence of noise. The presence of a finite amount of noise reduces the number of distinguishable states of a continuous variable to a finite number - and thus restricts analog computers to the representation of a finite amount of information. In practice, noise reduces analog computers to being no more powerful than conventional digital computers, and through them Turing machines. One might suspect that quantum computers are just analog computers, because of the use of continuous parameters in describing qubit states; however, it turns out that the effects of noise on a quantum computer can effectively be digitized. As a result, their computational advantages remain even in the presence of a finite amount of noise, as we shall see in Chapter 10.

What of the effects of noise on digital computers? In the early days of computation, noise was a very real problem for computers. In some of the original computers a vacuum tube would malfunction every few minutes. Even today, noise is a problem for computational devices such as modems and hard drives. Considerable effort was devoted to the problem of understanding how to construct reliable computers from unreliable components. It was proven by von Neumann that this is possible with only a polynomial increase in the resources required for computation. Ironically, however, modern computers use none of those results, because the components of modern computers are fantastically reliable. Failure rates of 10^{-17} and even less are common in modern electronic components. For this reason, failures happen so rarely that the extra effort required to protect against them is not regarded as being worth making. On the other hand, we shall find that quantum computers are very delicate machines, and will likely require substantial application of error-correction techniques.

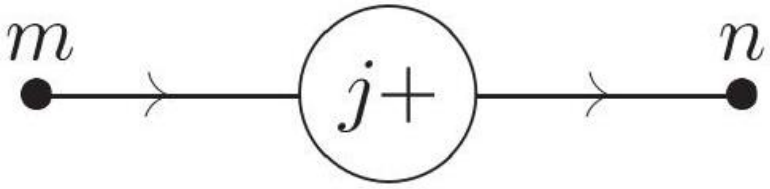
Different architectures may change the effects of noise. For example, if the effect of noise is ignored, then changing to a computer architecture in which many operations are performed in parallel may not change the number of operations which need to be done. However, a parallel system may be substantially more resistant to noise, because the effects of noise have less time to accumulate. Therefore, in a realistic analysis, the parallel version of an algorithm may have some substantial advantages over a serial implementation. Architecture design is a well developed field of study for classical computers. Hardly anything similar has been developed along the same lines for quantum computers, but the study of noise already suggests some desirable traits for future quantum computer architectures, such as a high level of parallelism.

A fourth model of computation is distributed computation, in which two or more spatially separated computational units are available to solve a computational problem. Obviously, such a model of computation is no more powerful than the Turing machine model in the sense that it can be efficiently simulated on a Turing machine. However, distributed computation gives rise to an intriguing new resource challenge: how best to utilize multiple computational units when the cost of communication between the units is high. This problem of distributed computation becomes especially interesting as computers are connected through high speed networks; although the total computational capacity of all the computers on a network might be extremely large, utilization of that potential is difficult. Most interesting problems do not divide easily into independent chunks that can be solved separately, and may frequently require global communication between different computational subsystems to exchange intermediate results or synchronize status. The field of communication complexity has been developed to address such issues, by
quantifying the cost of communication requirements in solving problems. When quantum resources are available and can be exchanged between distributed computers, the communication costs can sometimes be greatly reduced.

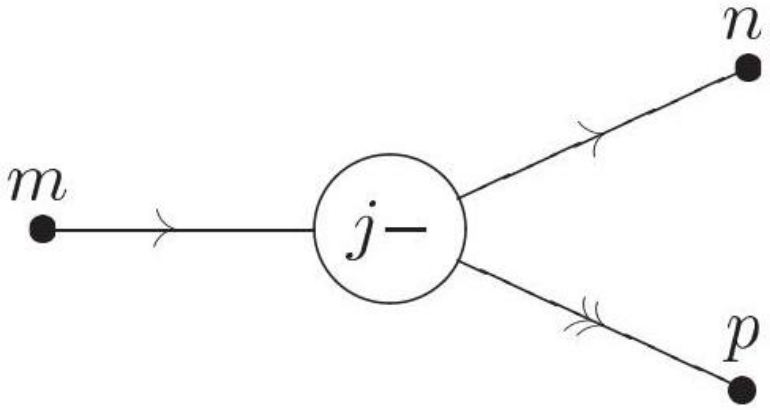
A recurring theme through these concluding thoughts and through the entire book is that despite the traditional independence of computer science from physical constraints, ultimately physical laws have tremendous impact not only upon how computers are realized, but also the class of problems they are capable of solving. The success of quantum computation and quan-

tum information as a physically reasonable alternative model of computation questions closely held tenets of computer science, and thrusts notions of computer science into the forefront of physics. The task of the remainder of this book is to stir together ideas from these disparate fields, and to delight in what results!

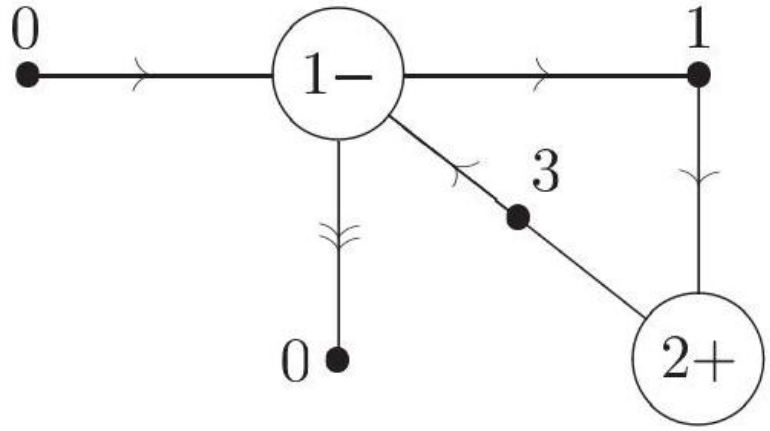
Problem 3.1: (Minsky machines) A Minsky machine consists of a finite set of registers, $r_1, r_2, \ldots, r_k$, each capable of holding an arbitrary non-negative integer, and a program, made up of orders of one of two types. The first type has the form:



The interpretation is that at point m in the program register r_j is incremented by one, and execution proceeds to point n in the program. The second type of order has the form:



The interpretation is that at point m in the program, register r_j is decremented if it contains a positive integer, and execution proceeds to point n in the program. If register r_j is zero then execution simply proceeds to point p in the program. The program for the Minsky machine consists of a collection of such orders, of a form like:



The starting and all possible halting points for the program are conventionally labeled zero. This program takes the contents of register r_1 and adds them to register r_2, while decrementing r_1 to zero.

(1) Prove that all (Turing) computable functions can be computed on a Minsky machine, in the sense that given a computable function $f(\cdot)$ there is a Minsky machine program that when the registers start in the state $(n, 0, \ldots, 0)$ gives as output $(f(n), 0, \ldots, 0)$.

(2) Sketch a proof that any function which can be computed on a Minsky machine, in the sense just defined, can also be computed on a Turing machine.

Problem 3.2: (Vector games) A vector game is specified by a finite list of vectors, all of the

same dimension, and with integer co-ordinates. The game is to start with a vector x of non-negative integer co-ordinates and to add to x the first vector from the list which preserves the non-negativity of all the components, and to repeat this process until it is no longer possible. Prove that for any computable function $f(\cdot)$ there is a vector game which when started with the vector $(n, 0, \ldots, 0)$ reaches $(f(n), 0, \ldots, 0)$. (Hint: Show that a vector game in $k+2$ dimensions can simulate a Minsky machine containing k registers.)

Problem 3.3: (Fractran) A Fractran program is defined by a list of positive rational numbers $q_1, \ldots, q_n$. It acts on a positive integer m by replacing it by $q_i m$, where i is the least number such that $q_i m$ is an integer. If there is ever a time when there is no i such that $q_i m$ is an integer, then execution stops. Prove that for any computable function $f(\cdot)$ there is a Fractran program which when started with 2^n reaches $2^{f(n)}$ without going through any intermediate powers of 2 . (Hint: use the previous problem.)

Problem 3.4: (Undecidability of dynamical systems) A Fractran program is essentially just a very simple dynamical system taking positive integers to positive integers. Prove that there is no algorithm to decide whether such a dynamical system ever reaches 1 .

Problem 3.5: (Non-universality of two bit reversible logic) Suppose we are trying to build circuits using only one and two bit reversible logic gates, and ancilla bits. Prove that there are Boolean functions which cannot be computed in this fashion. Deduce that the Toffoli gate cannot be simulated using one and two bit reversible gates, even with the aid of ancilla bits.

Problem 3.6: (Hardness of approximation of TSP) Let $r \geq 1$ and suppose that there is an approximation algorithm for TSP which is guaranteed to find the shortest tour among n cities to within a factor r. Let $G = (V, E)$ be any graph on n vertices. Define an instance of TSP by identifying cities with vertices in V, and defining the distance between cities i and j to be 1 if (i, j) is an edge of G, and to be $\lceil r \rceil |V| + 1$ otherwise. Show that if the approximation algorithm is applied to this instance of TSP then it returns a Hamiltonian cycle for G if one exists, and otherwise returns a tour of length more than $\lceil r \rceil |V|$. From the NP-completeness of HC it follows that no such approximation algorithm can exist unless $\mathbf{P} = \mathbf{N}$.

Problem 3.7: (Reversible Turing machines)

(1) Explain how to construct a reversible Turing machine that can compute the same class of functions as is computable on an ordinary Turing machine.
(Hint: It may be helpful to use multi-tape construction.)
(2) Give general space and time bounds for the operation of your reversible Turing machine, in terms of the time $t(x)$ and space $s(x)$ required on an ordinary single-tape Turing machine to compute a function $f(x)$.

Problem 3.8: (Find a hard-to-compute class of functions (Research)) Find a natural class of functions on n inputs which requires a super-polynomial number of Boolean gates to compute.

Problem 3.9: (Reversible PSPACE = PSPACE) It can be shown that the problem 'quantified satisfiability', or QSAT, is PSPACE-complete. That is, every other language in PSPACE can be reduced to QSAT in polynomial time. The language QSAT is defined to consist of all Boolean formulae φ in n variables $x_1, \ldots, x_n$, and in conjunctive normal form, such that:

$$\exists_{x_1} \forall x_2 \exists x_{x_3} \ldots \forall_{x_n} \varphi \text{ if } n \text{ is even;} \tag{3.9}$$

$$\exists_{x_1} \forall_{x_2} \exists_{x_3} \ldots \exists_{x_n} \varphi \text{ if } n \text{ is odd.} \tag{3.10}$$

Prove that a reversible Turing machine operating in polynomial space can be used to solve qsat. Thus, the class of languages decidable by a computer operating reversibly in polynomial space is equal to PSPACE.

Problem 3.10: (Ancilla bits and efficiency of reversible computation) Let p_m be the m th prime number. Outline the construction of a reversible circuit which, upon input of m and n

such that $n > m$, outputs the product $p_m p_n$, that is $(m, n) \rightarrow (p_m p_n, g(m, n))$, where $g(m, n)$ is the final state of the ancilla bits used by the circuit. Estimate the number of ancilla qubits your circuit requires. Prove that if a polynomial (in $\log n$) size reversible circuit can be found that uses $O(\log(\log n))$ ancilla bits then the problem of factoring a product of two prime numbers is in **P**.

History and further reading

Computer science is a huge subject with many interesting subfields. We cannot hope for any sort of completeness in this brief space, but instead take the opportunity to recommend a few titles of general interest, and some works on subjects of specific interest in relation to topics covered in this book, with the hope that they may prove stimulating.

Modern computer science dates to the wonderful 1936 paper of Turing [Tur36]. The Church-Turing thesis was first stated by Church [Chu36] in 1936, and was then given a more complete discussion from a different point of view by Turing. Several other researchers found their way to similar conclusions at about the same time. Many of these contributions and a discussion of the history may be found in a volume edited by Davis [Dav65] . Provocative discussions of the Church-Turing thesis and undecidability may be found in Hofstadter [Hof79] and Penrose[[Pen89].

There are many excellent books on algorithm design. We mention only three. First, there is the classic series by Knuth[Knu97, Knu98a, Knu98b] which covers an enormous portion of computer science. Second, there is the marvelous book by Cormen, Leiserson, and Rivest [CLR90] . This huge book contains a plethora of well-written material on many areas of algorithm design. Finally, the book of Motwani and Raghavan [MR95] is an excellent survey of the field of randomized algorithms.

The modern theory of computational complexity was especially influenced by the papers of Cook[Coo71] and Karp[Kar72]. Many similar ideas were arrived at independently in Russia by Levin [Lev73] , but unfortunately took time to propagate to the West. The classic book by Garey and Johnson [GJ79] has also had an enormous influence on the field. More recently, Papadimitriou [Pap94] has written a beautiful book that surveys many of the main ideas of computational complexity theory. Much of the material in this chapter is based upon Papadimitriou's book. In this chapter we considered only one type of reducibility between languages, polynomial time reducibility. There are many other notions of reductions between languages. An early survey of these notions was given by Ladner, Lynch and Selman [LLS75] . The study of different notions of reducibility later blossomed into a subfield of research known as structural complexity, which has been reviewed by Balcázar, Diaz, and Gabarró[BDG88a, BDG88b].

The connection between information, energy dissipation, and computation has a long history. The modern understanding is due to a 1961 paper by Landauer [Lan61] , in which Landauer's principle was first formulated. A paper by Szilard [Szi29] and a 1949 lecture by von Neumann [von66] (page 66) arrive at conclusions close to Landauer's principle, but do not fully grasp the essential point that it is the erasure of information that requires dissipation.

Reversible Turing machines were invented by Lecerf [Lec63] and later, but independently, in an influential paper by Bennett[Ben73]. Fredkin and Toffoli [FT82] introduced reversible circuit models of computation. Two interesting historical documents are Barton's May, 1978 MIT 6.895 term paper [Bar78], and Ressler's 1981 Master's thesis [Res81], which contain designs for a reversible PDP-10! Today, reversible logic is potentially important in implementations of low-power CMOS circuitry [YK95].

Maxwell's demon is a fascinating subject, with a long and intricate history. Maxwell proposed his demon in 1871[Max71]. Szilard published a key paper in 1929[Szi29] which anticipated many of the details of the final resolution of the problem of Maxwell's demon. In 1965 Feynman [FLS65b] resolved a special case of Maxwell's demon. Bennett, building on Landauer's

work [Lan61], wrote two beautiful papers on the subject [BBBW82, Ben87] which completed the resolution of the problem. An interesting book about the history of Maxwell's demon and its exorcism is the collection of papers by Leff and Rex [$LR90$].

DNA computing was invented by Adleman, and the solution of the directed Hamiltonian path problem we describe is his [Ad194]. Lipton has also shown how 3sat and circuit satisfiability can be solved in this model[Lip95]. A good general article is Adleman's Scientific American article [Ad198]; for an insightful look into the universality of DNA operations, see Winfree [$Win98$]. An interesting place to read about performing reliable computation in the presence of noise is the book by Winograd and Cowan [$WC67$]. This topic will be addressed again in Chapter 10. A good textbook on computer architecture is by Hennessey, Goldberg, and Patterson. [HGP96].

Problems 3.1 through 3.4 explore a line of thought originated by Minsky (in his beautiful book on computational machines [Min67]) and developed by Conway [Con72, $Con86$]. The Fractran programming language is certainly one of the most beautiful and elegant universal computational models known, as demonstrated by the following example, known as PRIMEGAME [Con86]. PRIMEGAME is defined by the list of rational numbers:

$$\frac{17}{91}; \frac{78}{85}; \frac{19}{51}; \frac{23}{38}; \frac{29}{33}; \frac{77}{29}; \frac{95}{23}; \frac{77}{19}; \frac{1}{17}; \frac{11}{13}; \frac{13}{11}; \frac{15}{2}; \frac{1}{7}; \frac{55}{1}. \tag{3.11}$$

Amazingly, when PRIMEGAME is started at 2 , the other powers of 2 that appear, namely, $2^2, 2^3, 2^5, 2^7, 2^{11}, 2^{13}, \ldots$, are precisely the prime powers of 2 , with the powers stepping through the prime numbers, in order. Problem 3.9 is a special case of the more general subject of the spatial requirements for reversible computation. See the papers by Bennett[Ben89], and by Li, Tromp and Vitanyi[LV96, LTV98].

8 II Quantum computation by Nielsen, Chang

8.1 4 Quantum circuits

> The theory of computation has traditionally been studied almost entirely in the abstract, as a topic in pure mathematics. This is to miss the point of it. Computers are physical objects, and computations are physical processes. What computers can or cannot compute is determined by the laws of physics alone, and not by pure mathematics.
>
> - David Deutsch
>
> Like mathematics, computer science will be somewhat different from the other sciences, in that it deals with artificial laws that can be proved, instead of natural laws that are never known with certainty.
>
> - Donald Knuth
>
> The opposite of a profound truth may well be another profound truth. - Niels Bohr

This chapter begins Part II of the book, in which we explore quantum computation in detail. The chapter develops the fundamental principles of quantum computation, and establishes the basic building blocks for quantum circuits, a universal language for describing sophisticated quantum computations. The two fundamental quantum algorithms known to date are constructed from these circuits in the following two chapters. Chapter 5 presents the quantum Fourier transform and its applications to phase estimation, order-finding and factoring. Chapter 6 describes the quantum search algorithm, and its applications to database search, counting

and speedup of solutions to NP-complete problems. Chapter 7 concludes Part II with a discussion of how quantum computation may one day be experimentally realized. Two other topics of great interest for quantum computation, quantum noise and quantum error-correction, are deferred until Part III of the book, in view of their wide interest also outside quantum computation.

There are two main ideas introduced in this chapter. First, we explain in detail the fundamental model of quantum computation, the quantum circuit model. Second, we demonstrate that there exists a small set of gates which are universal, that is, any quantum computation whatsoever can be expressed in terms of those gates. Along the way we also have occasion to describe many other basic results of quantum computation. Section 4.1 begins the chapter with an overview of quantum algorithms, focusing on what algorithms are known, and the unifying techniques underlying their construction. Section 4.2 is a detailed study of single qubit operations. Despite their simplicity, single qubit operations offer a rich playground for the construction of examples and techniques, and it is essential to understand them in detail. Section 4.3 shows how to perform multi-qubit controlled unitary operations, and Section 4.4 discusses the description of measurement in the quantum circuits model. These elements are then brought together in Section 4.5 for the statement and proof of the universality theorem. We summarize all the basic elements
of quantum computation in Section 4.6, and discuss possible variants of the model, and the important question of the relationship in computational power between classical and quantum computers. Section 4.7 concludes the chapter with an important and instructive application of quantum computation to the simulation of real quantum systems.

This chapter is perhaps the most reader-intensive of all the chapters in the book, with a high density of exercises for you to complete, and it is worth explaining the reason for this intensity. Obtaining facility with the basic elements of the quantum circuit model of computation is quite easy, but requires assimilating a large number of simple results and techniques that must become second nature if one is to progress to the more difficult problem of designing quantum algorithms. For this reason we take an example-oriented approach in this chapter, and ask you to fill in many of the details, in order to acquire such a facility. A less intensive, but somewhat superficial overview of the basic elements of quantum computation may be obtained by skipping to Section 4.6.

8.1.1 4.1 Quantum algorithms

What is a quantum computer good for? We're all familiar with the frustration of needing more computer resources to solve a computational problem. Practically speaking, many interesting problems are impossible to solve on a classical computer, not because they are in principle insoluble, but because of the astronomical resources required to solve realistic cases of the problem.

The spectacular promise of quantum computers is to enable new algorithms which render feasible problems requiring exorbitant resources for their solution on a classical computer. At the time of writing, two broad classes of quantum algorithms are known which fulfill this promise. The first class of algorithms is based upon Shor's quantum Fourier transform, and includes remarkable algorithms for solving the factoring and discrete logarithm problems, providing a striking exponential speedup over the best known classical algorithms. The second class of algorithms is based upon Grover's algorithm for performing quantum searching. These provide a less striking but still remarkable quadratic speedup over the best possible classical algorithms. The quantum searching algorithm derives its importance from the widespread use of search-based techniques in classical algorithms, which in many instances allows a straightforward adaptation of the classical algorithm to give a faster quantum algorithm.

Figure 4.1 sketches the state of knowledge about quantum algorithms at the time of writing, including some sample applications of those algorithms. Naturally, at the core of the diagram are the quantum Fourier transform and the quantum searching algorithm. Of particular interest in the figure is the quantum counting algorithm. This algorithm is a clever combination of the quantum searching and Fourier transform algorithms, which can be used to estimate the number of solutions to a search problem more quickly than is possible on a classical computer.

The quantum searching algorithm has many potential applications, of which but a few are illustrated. It can be used to extract statistics, such as the minimal element, from an unordered data set, more quickly than is possible on a classical computer. It can be used to speed up algorithms for some problems in NP - specifically, those problems for which a straightforward search for a solution is the best algorithm known. Finally, it can be used to speed up the search for keys to cryptosystems such as the widely used Data Encryption Standard (DES). These and other applications are explained in Chapter 6.

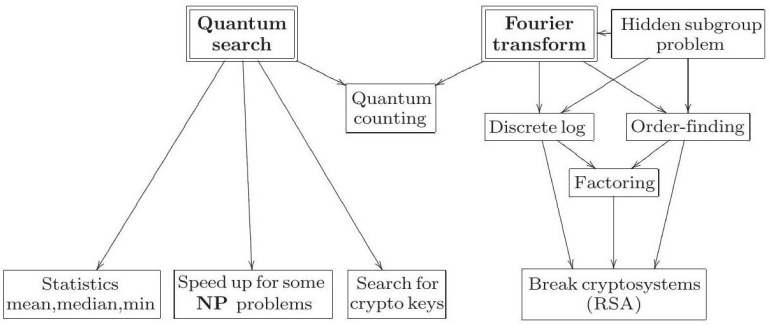


Figure 4.1. The main quantum algorithms and their relationships, including some notable applications.

The quantum Fourier transform also has many interesting applications. It can be used to solve the discrete logarithm and factoring problems. These results, in turn, enable a quantum computer to break many of the most popular cryptosystems now in use, including the RSA cryptosystem. The Fourier transform also turns out to be closely related to an important problem in mathematics, finding a hidden subgroup (a generalization of finding the period of a periodic function). The quantum Fourier transform and several of its applications, including fast quantum algorithms for factoring and discrete logarithm, are explained in Chapter 5.

Why are there so few quantum algorithms known which are better than their classical counterparts? The answer is that coming up with good quantum algorithms seems to be a difficult problem. There are at least two reasons for this. First, algorithm design, be it classical or quantum, is not an easy business! The history of algorithms shows us that considerable ingenuity is often required to come up with near optimal algorithms, even for apparently very simple problems, like the multiplication of two numbers. Finding good quantum algorithms is made doubly difficult because of the additional constraint that we want our quantum algorithms to be better than the best known classical algorithms. A second reason for the difficulty of finding good quantum algorithms is that our intuitions are much better adapted to the classical world than they are to the quantum world. If we think about problems using our native intuition, then the algorithms which we come up with are going to be classical algorithms. It takes special insights and special tricks to come up with good quantum algorithms.

Further study of quantum algorithms will be postponed until the next chapter. In this chapter we provide an efficient and powerful language for describing quantum algorithms, the language of quantum circuits - assemblies of discrete sets of components which describe computational procedures. This construction will enable us to quantify the cost of an algorithm

in terms of things like the total number of gates required, or the circuit depth. The circuit language also comes with a toolbox of tricks that simplifies algorithm design and provides ready conceptual understanding.

8.1.2 4.2 Single qubit operations

The development of our quantum computational toolkit begins with operations on the simplest quantum system of all - a single qubit. Single qubit gates were introduced in Section 1.3.1. Let us quickly summarize what we learned there; you may find it useful to refer to the notes on notation on page xxiii as we go along.

A single qubit is a vector $|\psi\rangle = a|0\rangle + b|1\rangle$ parameterized by two complex numbers satisfying $|a|^2 + |b|^2 = 1$. Operations on a qubit must preserve this norm, and thus are described by 2×2 unitary matrices. Of these, some of the most important are the Pauli matrices; it is useful to list them again here:

$$X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}; \quad Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}; \quad Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{4.1}$$

Three other quantum gates will play a large part in what follows, the Hadamard gate (denoted H), phase gate (denoted S), and $\pi/8$ gate (denoted T):

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}; \quad S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}; \quad T = \begin{bmatrix} 1 & 0 \\ 0 & \exp(i\pi/4) \end{bmatrix}. \tag{4.2}$$

A couple of useful algebraic facts to keep in mind are that $H = (X + Z)/\sqrt{2}$ and $S = T^2$. You might wonder why the T gate is called the $\pi/8$ gate when it is $\pi/4$ that appears in the definition. The reason is that the gate has historically often been referred to as the $\pi/8$ gate, simply because up to an unimportant global phase T is equal to a gate which has $\exp(\pm i\pi/8)$ appearing on its diagonals.

$$T = \exp(i\pi/8) \begin{bmatrix} \exp(-i\pi/8) & 0 \\ 0 & \exp(i\pi/8) \end{bmatrix}. \tag{4.3}$$

Nevertheless, the nomenclature is in some respects rather unfortunate, and we often refer to this gate as the T gate.

Recall also that a single qubit in the state $a|0\rangle + b|1\rangle$ can be visualized as a point (θ, φ) on the unit sphere, where $a = \cos(\theta/2), b = e^{i\varphi}\sin(\theta/2)$, and a can be taken to be real because the overall phase of the state is unobservable. This is called the Bloch sphere representation, and the vector ($\cos\varphi\sin\theta, \sin\varphi\sin\theta, \cos\theta$) is called the Bloch vector. We shall return to this picture often as an aid to intuition.

Exercise 4.1: In Exercise 2.11, which you should do now if you haven't already done it, you computed the eigenvectors of the Pauli matrices. Find the points on the Bloch sphere which correspond to the normalized eigenvectors of the different Pauli matrices.

The Pauli matrices give rise to three useful classes of unitary matrices when they are exponentiated, the rotation operators about the $\hat{x}, \hat{y}$, and $\hat{z}$ axes, defined by the equations:

$$R_x(\theta) \equiv e^{-i\theta X/2} = \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2} X = \begin{bmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix} \tag{4.4}$$

$$R_y(\theta) \equiv e^{-i\theta Y/2} = \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2} Y = \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix} \tag{4.5}$$

$$R_z(\theta) \equiv e^{-i\theta Z/2} = \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2} Z = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix}. \tag{4.6}$$

Exercise 4.2: Let x be a real number and A a matrix such that $A^2 = I$. Show that

$$\exp(iAx) = \cos(x)I + i\sin(x)A \tag{4.7}$$

Use this result to verify Equations (4.4) through (4.6).
Exercise 4.3: Show that, up to a global phase, the $\pi/8$ gate satisfies $T = R_z(\pi/4)$.
Exercise 4.4: Express the Hadamard gate H as a product of R_x and R_z rotations and $e^{i\varphi}$ for some φ.

If $\hat{n} = (n_x, n_y, n_z)$ is a real unit vector in three dimensions then we generalize the previous definitions by defining a rotation by θ about the $\hat{n}$ axis by the equation

$$R_{\hat{n}}(\theta) \equiv \exp(-i\theta\hat{n}\cdot\vec{\sigma}/2) = \cos\left(\frac{\theta}{2}\right) I - i\sin\left(\frac{\theta}{2}\right)(n_x X + n_y Y + n_z Z) \tag{4.8}$$

where $\vec{\sigma}$ denotes the three component vector (X, Y, Z) of Pauli matrices.
Exercise 4.5: Prove that $(\hat{n}\cdot\vec{\sigma})^2 = I$, and use this to verify Equation (4.8).
Exercise 4.6: (Bloch sphere interpretation of rotations) One reason why the $R_{\hat{n}}(\theta)$ operators are referred to as rotation operators is the following fact, which you are to prove. Suppose a single qubit has a state represented by the Bloch vector $\vec{\lambda}$. Then the effect of the rotation $R_{\hat{n}}(\theta)$ on the state is to rotate it by an angle θ about the $\hat{n}$ axis of the Bloch sphere. This fact explains the rather mysterious looking factor of two in the definition of the rotation matrices.

Exercise 4.7: Show that $XYX = -Y$ and use this to prove that
$XR_y(\theta)X = R_y(-\theta)$.
Exercise 4.8: An arbitrary single qubit unitary operator can be written in the form

$$U = \exp(i\alpha)R_{\hat{n}}(\theta) \tag{4.9}$$

for some real numbers α and θ, and a real three-dimensional unit vector $\hat{n}$.

1. Prove this fact.
2. Find values for α, θ, and $\hat{n}$ giving the Hadamard gate H.
3. Find values for α, θ, and $\hat{n}$ giving the phase gate

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \tag{4.10}$$

An arbitrary unitary operator on a single qubit can be written in many ways as a combination of rotations, together with global phase shifts on the qubit. The following theorem provides a means of expressing an arbitrary single qubit rotation that will be particularly useful in later applications to controlled operations.

Theorem 4.1: ($Z - Y$ decomposition for a single qubit) Suppose U is a unitary operation on a single qubit. Then there exist real numbers α, β, γ and δ such that

$$U = e^{i\alpha}R_z(\beta)R_y(\gamma)R_z(\delta) \tag{4.11}$$

Proof

Since U is unitary, the rows and columns of U are orthonormal, from which it follows that there exist real numbers α, β, γ, and δ such that

$$U = \begin{bmatrix} e^{i(\alpha-\beta/2-\delta/2)}\cos\frac{\gamma}{2} & -e^{i(\alpha-\beta/2+\delta/2)}\sin\frac{\gamma}{2} \\ e^{i(\alpha+\beta/2-\delta/2)}\sin\frac{\gamma}{2} & e^{i(\alpha+\beta/2+\delta/2)}\cos\frac{\gamma}{2} \end{bmatrix}. \tag{4.12}$$

Equation (4.11) now follows immediately from the definition of the rotation matrices and matrix multiplication. □

Exercise 4.9: Explain why any single qubit unitary operator may be written in the form (4.12).

Exercise 4.10: ($X - Y$ decomposition of rotations) Give a decomposition analogous to Theorem 4.1 but using R_x instead of R_z.

Exercise 4.11: Suppose $\hat{m}$ and $\hat{n}$ are non-parallel real unit vectors in three dimensions. Use Theorem 4.1 to show that an arbitrary single qubit unitary U may be written

$$U = e^{i\alpha} R_{\hat{n}}(\beta) R_{\hat{m}}(\gamma) R_{\hat{n}}(\delta), \tag{4.13}$$

for appropriate choices of α, β, γ and δ.

The utility of Theorem 4.1 lies in the following mysterious looking corollary, which is the key to the construction of controlled multi-qubit unitary operations, as explained in the next section.

Corollary 4.2: Suppose U is a unitary gate on a single qubit. Then there exist unitary operators A, B, C on a single qubit such that $ABC = I$ and $U = e^{i\alpha} AXBXC$, where α is some overall phase factor.

Proof

In the notation of Theorem 4.1, set $A \equiv R_z(\beta) R_y(\gamma/2), B \equiv R_y(-\gamma/2) R_z(-(\delta+\beta)/2)$ and $C \equiv R_z((\delta-\beta)/2)$. Note that

$$ABC = R_z(\beta) R_y\left(\frac{\gamma}{2}\right) R_y\left(-\frac{\gamma}{2}\right) R_z\left(-\frac{\delta+\beta}{2}\right) R_z\left(\frac{\delta-\beta}{2}\right) = I. \tag{4.14}$$

Since $X^2 = I$, and using Exercise 4.7, we see that

$$XBX = X R_y\left(-\frac{\gamma}{2}\right) X X R_z\left(-\frac{\delta+\beta}{2}\right) X = R_y\left(\frac{\gamma}{2}\right) R_z\left(\frac{\delta+\beta}{2}\right). \tag{4.15}$$

Thus

$$AXBXC = R_z(\beta) R_y\left(\frac{\gamma}{2}\right) R_y\left(\frac{\gamma}{2}\right) R_z\left(\frac{\delta+\beta}{2}\right) R_z\left(\frac{\delta-\beta}{2}\right) \tag{4.16}$$

$$= R_z(\beta) R_y(\gamma) R_z(\delta) \tag{4.17}$$

Thus $U = e^{i\alpha} AXBXC$ and $ABC = I$, as required. □

Exercise 4.12: Give A, B, C, and α for the Hadamard gate.

Exercise 4.13: (Circuit identities) It is useful to be able to simplify circuits by inspection, using well-known identities. Prove the following three identities:

$$HXH = Z; \quad HYH = -Y; \quad HZH = X. \tag{4.18}$$

Exercise 4.14: Use the previous exercise to show that $HTH = R_x(\pi/4)$, up to a global phase.

Exercise 4.15: (Composition of single qubit operations) The Bloch representation gives a nice way to visualize the effect of composing two rotations.

(1) Prove that if a rotation through an angle β_1 about the axis $\hat{n}_1$ is followed by a rotation through an angle β_2 about an axis $\hat{n}_2$, then the overall rotation is through an angle β_{12} about an axis $\hat{n}_{12}$ given by

$$c_{12} = c_1 c_2 - s_1 s_2 \hat{n}_1 \cdot \hat{n}_2 \tag{4.19}$$
$$s_{12}\hat{n}_{12} = s_1 c_2 \hat{n}_1 + c_1 s_2 \hat{n}_2 - s_1 s_2 \hat{n}_2 \times \hat{n}_1 \tag{4.20}$$

where $c_i = \cos(\beta_i/2)$, $s_i = \sin(\beta_i/2)$, $c_{12} = \cos(\beta_{12}/2)$, and $s_{12} = \sin(\beta_{12}/2)$.
(2) Show that if $\beta_1 = \beta_2$ and $\hat{n}_1 = \hat{z}$ these equations simplify to

$$c_{12} = c^2 - s^2 \hat{z} \cdot \hat{n}_2 \tag{4.21}$$
$$s_{12}\hat{n}_{12} = sc(\hat{z} + \hat{n}_2) - s^2 \hat{n}_2 \times \hat{z}, \tag{4.22}$$

where $c = c_1$ and $s = s_1$.
Symbols for the common single qubit gates are shown in Figure 4.2. Recall the basic properties of quantum circuits: time proceeds from left to right; wires represent qubits, and a '/' may be used to indicate a bundle of qubits.

Hadamard	$-\boxed{H}-$	$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Pauli- X	$-\boxed{X}-$	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli- Y	$-\boxed{Y}-$	$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli- Z	$-\boxed{Z}-$	$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Phase	$-\boxed{S}-$	$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$	$-\boxed{T}-$	$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$

Figure 4.2. Names, symbols, and unitary matrices for the common single qubit gates.

8.1.3 4.3 Controlled operations

'If A is true, then do B '. This type of controlled operation is one of the most useful in computing, both classical and quantum. In this section we explain how complex controlled operations may be implemented using quantum circuits built from elementary operations.

The prototypical controlled operation is the controlled-not, which we met in Section 1.2.1. Recall that this gate, which we'll often refer to as CNOT, is a quantum gate with two input qubits, known as the control qubit and target qubit, respectively. It is drawn as shown in Figure 4.3. In terms of the computational basis, the action of the CNOT is given by $|c\rangle|t\rangle \rightarrow |c\rangle|t \oplus c\rangle$; that is, if the control qubit is set to $|1\rangle$ then the target qubit is flipped, otherwise the target qubit is left alone. Thus, in the computational basis $|\text{control, target}\rangle$ the matrix representation of CNOT is

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \tag{4.23}$$

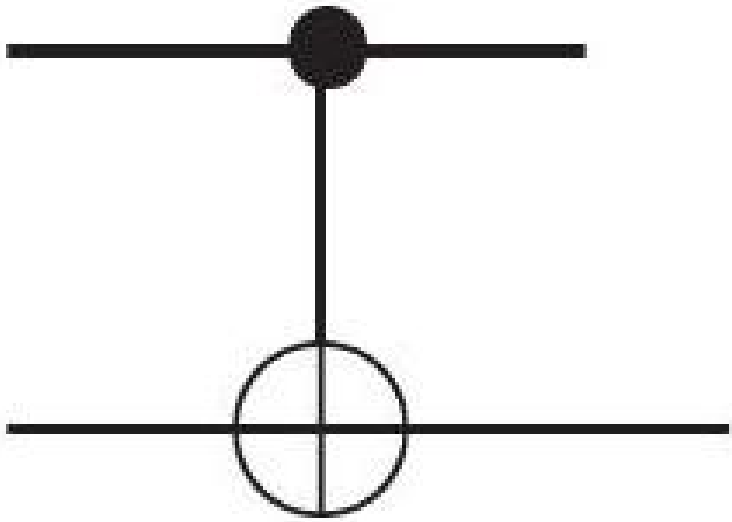


Figure 4.3. Circuit representation for the controlled-not gate. The top line represents the control qubit, the bottom line the target qubit.

More generally, suppose U is an arbitrary single qubit unitary operation. A controlled$U$ operation is a two qubit operation, again with a control and a target qubit. If the control qubit is set then U is applied to the target qubit, otherwise the target qubit is left alone; that is, $|c\rangle|t\rangle \rightarrow |c\rangle U^c|t\rangle$. The controlled- U operation is represented by the circuit shown in Figure 4.4.

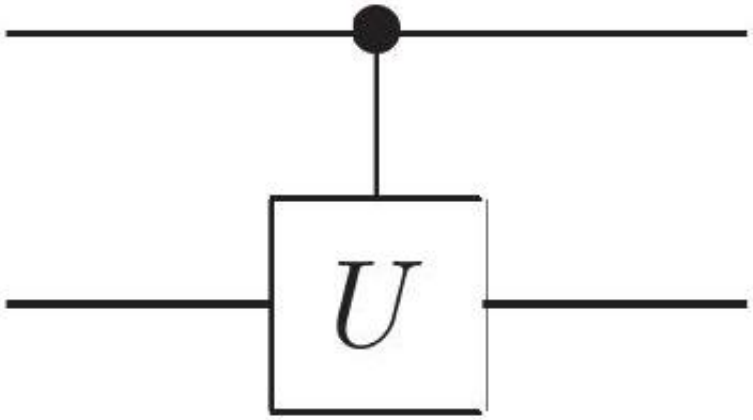


Figure 4.4. Controlled- U operation. The top line is the control qubit, and the bottom line is the target qubit. If the control qubit is set then U is applied to the target, otherwise it is left alone.

Exercise 4.16: (Matrix representation of multi-qubit gates) What is the 4×4 unitary matrix for the circuit

$$x_2 - H -$$
$$x_1 -$$

in the computational basis? What is the unitary matrix for the circuit

$$x_2$$
$$x_1 - H -$$

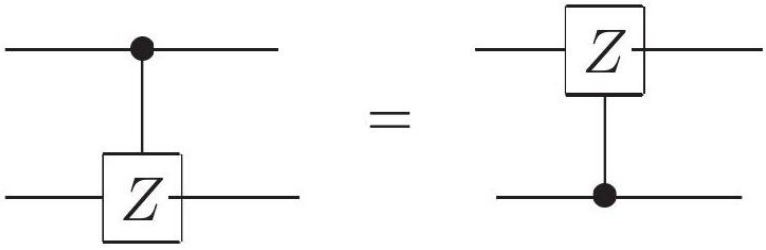
in the computational basis?

Exercise 4.17: (Building CNOT from controlled- Z gates) Construct a CNOT gate from one controlled- Z gate, that is, the gate whose action in the computational basis is specified by the unitary matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix},$$

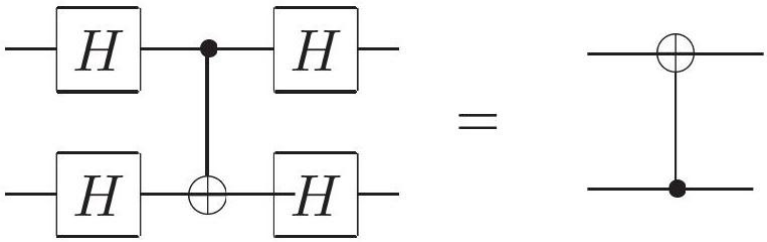
and two Hadamard gates, specifying the control and target qubits.

Exercise 4.18: Show that



Exercise 4.19: (CNOT action on density matrices) The CNOT gate is a simple permutation whose action on a density matrix ρ is to rearrange the elements in the matrix. Write out this action explicitly in the computational basis.

Exercise 4.20: (CNOT basis transformations) Unlike ideal classical gates, ideal quantum gates do not have (as electrical engineers say) 'high-impedance' inputs. In fact, the role of 'control' and 'target' are arbitrary - they depend on what basis you think of a device as operating in. We have described how the CNOT behaves with respect to the computational basis, and in this description the state of the control qubit is not changed. However, if we work in a different basis then the control qubit does change: we will show that its phase is flipped depending on the state of the 'target' qubit! Show that



Introducing basis states $|\pm\rangle \equiv (|0\rangle \pm |1\rangle)/\sqrt{2}$, use this circuit identity to show that the effect of a CNOT with the first qubit as control and the second qubit as target is as follows:

$$|+\rangle|+\rangle \rightarrow |+\rangle|+\rangle \tag{4.24}$$
$$|-\rangle|+\rangle \rightarrow |-\rangle|+\rangle \tag{4.25}$$
$$|+\rangle|-\rangle \rightarrow |-\rangle|-\rangle \tag{4.26}$$
$$|-\rangle|-\rangle \rightarrow |+\rangle|-\rangle \tag{4.27}$$

Thus, with respect to this new basis, the state of the target qubit is not changed, while the state of the control qubit is flipped if the target starts as $|-\rangle$, otherwise
it is left alone. That is, in this basis, the target and control have essentially interchanged roles!

Our immediate goal is to understand how to implement the controlled- U operation for arbitrary single qubit U, using only single qubit operations and the cNOT gate. Our strategy is a two-part procedure based upon the decomposition $U = e^{i\alpha}AXBXC$ given in Corollary 4.2 on page 176.

Our first step will be to apply the phase shift $\exp(i\alpha)$ on the target qubit, controlled by the control qubit. That is, if the control qubit is $|0\rangle$, then the target qubit is left alone, while if the control qubit is $|1\rangle$, a phase shift $\exp(i\alpha)$ is applied to the target. A circuit implementing this operation using just a single qubit unitary gate is depicted on the right hand side of Figure 4.5. To verify that this circuit works correctly, note that the effect of the circuit on the right hand side is

$$|00\rangle \rightarrow |00\rangle, \quad |01\rangle \rightarrow |01\rangle, \quad |10\rangle \rightarrow e^{i\alpha}|10\rangle, \quad |11\rangle \rightarrow e^{i\alpha}|11\rangle, \tag{4.28}$$

which is exactly what is required for the controlled operation on the left hand side.

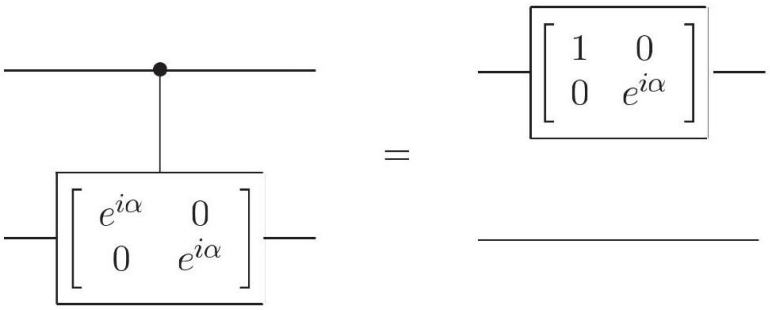


Figure 4.5. Controlled phase shift gate and an equivalent circuit for two qubits.

We may now complete the construction of the controlled- U operation, as shown in Figure 4.6. To understand why this circuit works, recall from Corollary 4.2 that U may be written in the form $U = e^{i\alpha}AXBXC$, where A, B and C are single qubit operations such that $ABC = I$. Suppose that the control qubit is set. Then the operation $e^{i\alpha}AXBXC = U$ is applied to the second qubit. If, on the other hand, the control qubit is not set, then the operation $ABC = I$ is applied to the second qubit; that is, no change is made. That is, this circuit implements the controlled- U operation.

Now that we know how to condition on a single qubit being set, what about conditioning on multiple qubits? We've already met one example of multiple qubit conditioning, the Toffoli gate, which flips the third qubit, the target qubit, conditioned on the first two qubits, the control qubits, being set to one. More generally, suppose we have $n + k$ qubits, and U is a k qubit unitary operator. Then we define the controlled operation $C^n(U)$ by the equation

$$C^n(U)\,|x_1x_2\ldots x_n\rangle\,|\psi\rangle = |x_1x_2\ldots x_n\rangle\,U^{x_1x_2\ldots x_n}|\psi\rangle, \tag{4.29}$$

where $x_1x_2\ldots x_n$ in the exponent of U means the product of the bits $x_1, x_2, \ldots, x_n$. That is, the operator U is applied to the last k qubits if the first n qubits are all equal to one, and otherwise, nothing is done. Such conditional operations are so useful that we

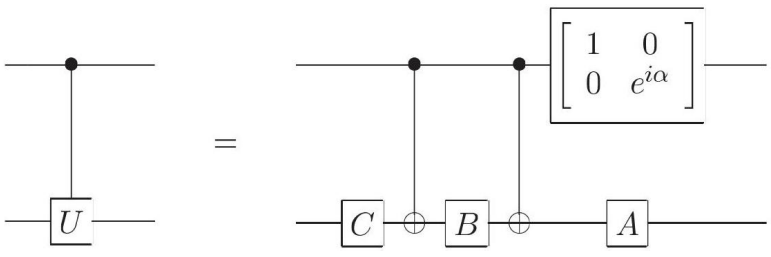


Figure 4.6. Circuit implementing the controlled- U operation for single qubit U, α, A, B and C satisfy $U = \exp(i\alpha)AXBXC, ABC = I$.

introduce a special circuit notation for them, illustrated in Figure 4.7. For the following we assume that $k = 1$, for simplicity. Larger k can be dealt with using essentially the same methods, however for $k \geq 2$ there is the added complication that we don't (yet) know how to perform arbitrary operations on k qubits.

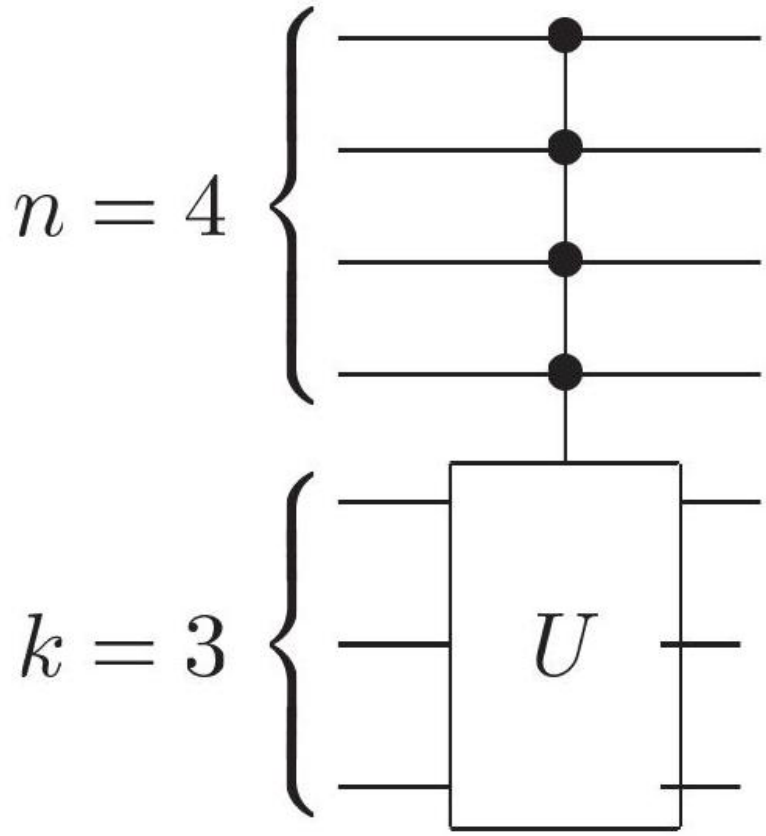


Figure 4.7. Sample circuit representation for the $C^{n}(U)$ operation, where U is a unitary operator on k qubits, for $n = 4$ and $k = 3$.}

Suppose U is a single qubit unitary operator, and V is a unitary operator chosen so that $V^2 = U$. Then the operation $C^2(U)$ may be implemented using the circuit shown in Figure 4.8.

Exercise 4.21: Verify that Figure 4.8 implements the $C^2(U)$ operation.

Exercise 4.22: Prove that a $C^2(U)$ gate (for any single qubit unitary U) can be constructed using at most eight one-qubit gates, and six controlled-nots.

Exercise 4.23: Construct a $C^1(U)$ gate for $U = R_x(\theta)$ and $U = R_y(\theta)$, using only CNOT and single qubit gates. Can you reduce the number of single qubit gates needed in the construction from three to two?

The familiar Toffoli gate is an especially important special case of the $C^2(U)$ operation,

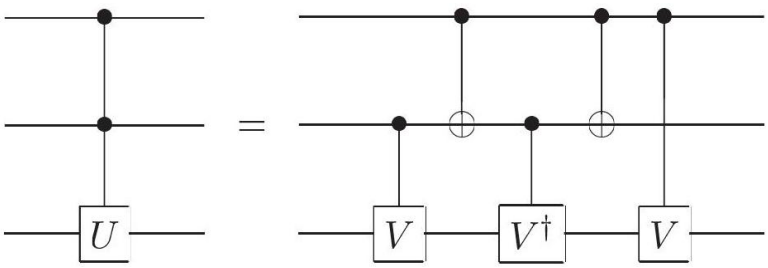


Figure 4.8. Circuit for the $C^{2}(U)$ gate. V is any unitary operator satisfying $V^2 = U$. The special case $V \equiv (1-i)(I+iX)/2$ corresponds to the Toffoli gate.}

the case $C^2(X)$. Defining $V \equiv (1-i)(I+iX)/2$ and noting that $V^2 = X$, we see that Figure 4.8 gives an implementation of the Toffoli gate in terms of one and two qubit operations. From a classical viewpoint this is a remarkable result; recall from Problem 3.5 that one and two bit classical reversible gates are not sufficient to implement the Toffoli gate, or, more generally, universal computation. By contrast, in the quantum case we see that one and two qubit reversible gates are sufficient to implement the Toffoli gate, and will eventually prove that they suffice for universal computation.

Ultimately we will show that any unitary operation can be composed to an arbitrarily good approximation from just the Hadamard, phase, controlled-not and $\pi/8$ gates. Because of the great usefulness of the Toffoli gate it is interesting to see how it can be built from just this gate set. Figure 4.9 illustrates a simple circuit for the Toffoli gate made up of just Hadamard, phase, controlled-not and $\pi/8$ gates.

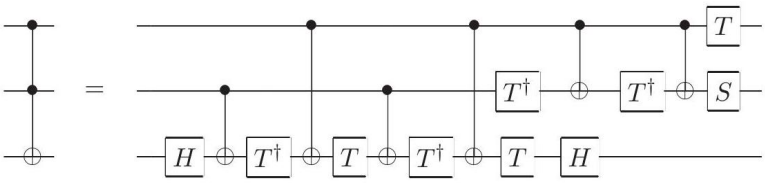


Figure 4.9. Implementation of the Toffoli gate using Hadamard, phase, controlled-NOT and $\pi/8$ gates.

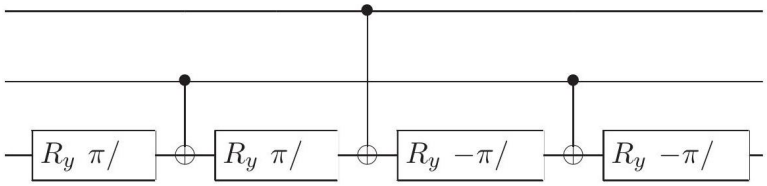
Exercise 4.24: Verify that Figure 4.9 implements the Toffoli gate.
Exercise 4.25: (Fredkin gate construction) Recall that the Fredkin (controlled-swap) gate performs the transform

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}. \tag{4.30}$$

(1) Give a quantum circuit which uses three Toffoli gates to construct the Fredkin gate (Hint: think of the swap gate construction - you can control each gate, one at a time).
(2) Show that the first and last Toffoli gates can be replaced by cNOT gates.

(3) Now replace the middle Toffoli gate with the circuit in Figure 4.8 to obtain a Fredkin gate construction using only six two-qubit gates.
(4) Can you come up with an even simpler construction, with only five two-qubit gates?

Exercise 4.26: Show that the circuit:



differs from a Toffoli gate only by relative phases. That is, the circuit takes $|c_1, c_2, t\rangle$ to $e^{i\theta(c_1,c_2,t)}|c_1, c_2, t \oplus c_1 \cdot c_2\rangle$, where $e^{i\theta(c_1,c_2,t)}$ is some relative phase factor. Such gates can sometimes be useful in experimental implementations, where it may be much easier to implement a gate that is the same as the Toffoli up to relative phases than it is to do the Toffoli directly.

Exercise 4.27: Using just CNOTs and Toffoli gates, construct a quantum circuit to perform the transformation

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}. \tag{4.31}$$

This kind of partial cyclic permutation operation will be useful later, in Chapter 7.

How may we implement $C^n(U)$ gates using our existing repertoire of gates, where U is an arbitrary single qubit unitary operation? A particularly simple circuit for achieving this task is illustrated in Figure 4.10. The circuit divides up into three stages, and makes use of a small number $(n-1)$ of working qubits, which all start and end in the state $|0\rangle$. Suppose the control qubits are in the computational basis state $|c_1, c_2, \ldots, c_n\rangle$. The first stage of the circuit is to reversibly and all the control bits $c_1, \ldots, c_n$ together to produce the product $c_1 \cdot c_2 \ldots c_n$. To do this, the first gate in the circuit ANDs c_1 and c_2 together, using a Toffoli gate, changing the state of the first work qubit to $|c_1 \cdot c_2\rangle$. The next Toffoli gate ands c_3 with the product $c_1 \cdot c_2$, changing the state of the second work qubit to $|c_1 \cdot c_2 \cdot c_3\rangle$. We continue applying Toffoli gates in this fashion, until the final work qubit is in the state $|c_1 \cdot c_2 \ldots c_n\rangle$. Next, a U operation on the target qubit is
performed, conditional on the final work qubit being set to one. That is, U is applied if and only if all of c_1 through c_n are set. Finally, the last part of the circuit just reverses the steps of the first stage, returning all the work qubits to their initial state, $|0\rangle$. The combined result, therefore, is to apply the unitary operator U to the target qubit, if and only if all the control bits c_1 through c_n are set, as desired.

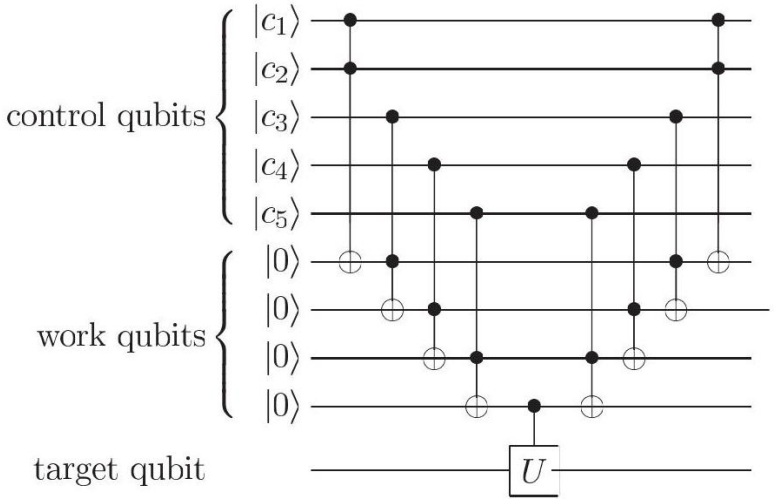


Figure 4.10. Network implementing the $C^{n}(U)$ operation, for the case $n = 5$.

Exercise 4.28: For $U = V^2$ with V unitary, construct a $C^5(U)$ gate analogous to that in Figure 4.10, but using no work qubits. You may use controlled- V and controlled- $V^\dagger$ gates.

Exercise 4.29: Find a circuit containing $O(n^2)$ Toffoli, CNOT and single qubit gates which implements a $C^n(X)$ gate (for $n > 3$), using no work qubits.

Exercise 4.30: Suppose U is a single qubit unitary operation. Find a circuit containing $O(n^2)$ Toffoli, CNOT and single qubit gates which implements a $C^n(U)$ gate (for $n > 3$), using no work qubits.

In the controlled gates we have been considering, conditional dynamics on the target qubit occurs if the control bits are set to one. Of course, there is nothing special about one, and it is often useful to consider dynamics which occur conditional on the control bit being set to zero. For instance, suppose we wish to implement a two qubit gate in which the second ('target') qubit is flipped, conditional on the first ('control') qubit being set to zero. In Figure 4.11 we introduce a circuit notation for this gate, together with an equivalent circuit in terms of the gates we have already introduced. Generically we shall use the open circle notation to indicate conditioning on the qubit being set to zero, while a closed circle indicates conditioning on the qubit being set to one.

A more elaborate example of this convention, involving three control qubits, is illustrated in Figure 4.12. The operation U is applied to the target qubit if the first and third qubits are set to zero, and the second qubit is set to one. It is easy to verify by inspection that the circuit on the right hand side of the figure implements the desired operation. More generally, it is easy to move between circuits which condition on qubits being set

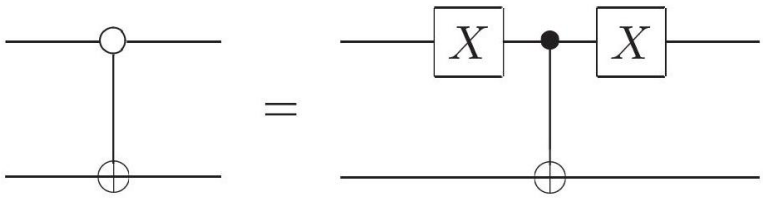


Figure 4.11. Controlled operation with a not gate being performed on the second qubit, conditional on the first qubit being set to zero.

to one and circuits which condition on qubits being set to zero, by insertion of X gates in

appropriate locations, as illustrated in Figure 4.12.

Another convention which is sometimes useful is to allow controlled-not gates to have multiple targets, as shown in Figure 4.13. This natural notation means that when the control qubit is 1 , then all the qubits marked with $\mathfrak{a}$ are flipped, and otherwise nothing happens. It is convenient to use, for example, in constructing classical functions such as permutations, or in encoders and decoders for quantum error-correction circuits, as we shall see in Chapter 10.

Exercise 4.31: (More circuit identities) Let subscripts denote which qubit an operator acts on, and let C be a CNOT with qubit 1 the control qubit and qubit 2 the target qubit. Prove the following identities:

$$CX_1C = X_1X_2 \tag{4.32}$$
$$CY_1C = Y_1X_2 \tag{4.33}$$
$$CZ_1C = Z_1 \tag{4.34}$$
$$CX_2C = X_2 \tag{4.35}$$
$$CY_2C = Z_1Y_2 \tag{4.36}$$
$$CZ_2C = Z_1Z_2 \tag{4.37}$$
$$R_{z,1}(\theta)C = CR_{z,1}(\theta) \tag{4.38}$$
$$R_{x,2}(\theta)C = CR_{x,2}(\theta) \tag{4.39}$$

8.1.4 4.4 Measurement

A final element used in quantum circuits, almost implicitly sometimes, is measurement. In our circuits, we shall denote a projective measurement in the computational basis (Section 2.2.5) using a 'meter' symbol, illustrated in Figure 4.14. In the theory of quantum circuits it is conventional to not use any special symbols to denote more general measurements, because, as explained in Chapter 2, they can always be represented by unitary transforms with ancilla qubits followed by projective measurements.

There are two important principles that it is worth bearing in mind about quantum circuits. Both principles are rather obvious; however, they are of such great utility that they are worth emphasizing early. The first principle is that classically conditioned operations can be replaced by quantum conditioned operations:

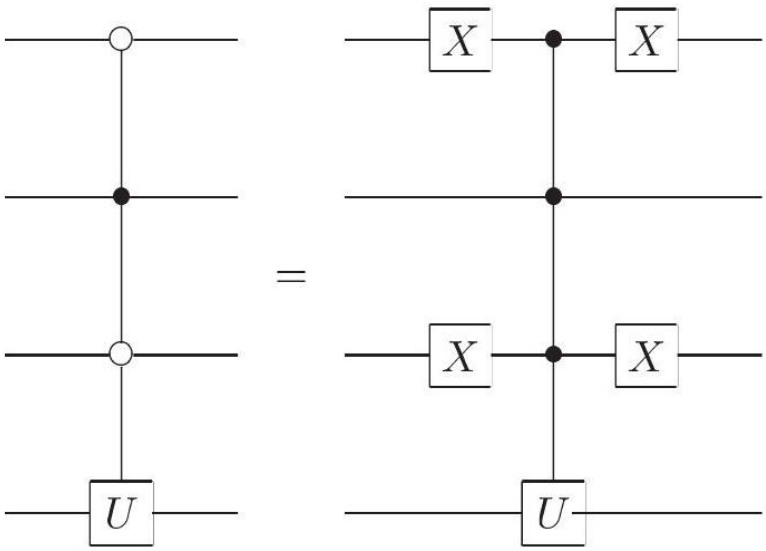


Figure 4.12. Controlled- U operation and its equivalent in terms of circuit elements we already know how to implement. The fourth qubit has U applied if the first and third qubits are set to zero, and the second qubit is set to one.

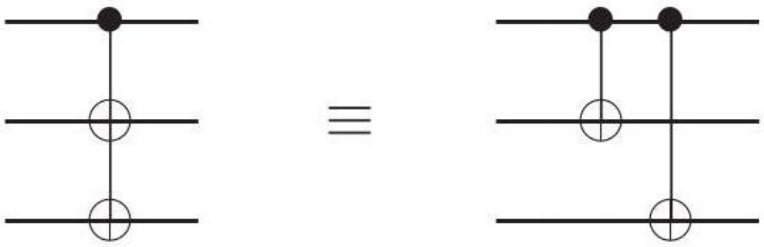


Figure 4.13. Controlled-not gate with multiple targets.

Principle of deferred measurement: Measurements can always be moved from an intermediate stage of a quantum circuit to the end of the circuit; if the measurement results are used at any stage of the circuit then the classically controlled operations can be replaced by conditional quantum operations.

Often, quantum measurements are performed as an intermediate step in a quantum circuit, and the measurement results are used to conditionally control subsequent quantum gates. This is the case, for example, in the teleportation circuit of Figure 1.13 on page 27. However, such measurements can always be moved to the end of the circuit. Figure 4.15 illustrates how this may be done by replacing all the classical conditional operations by corresponding quantum conditional operations. (Of course, some of the interpretation of this circuit as performing 'teleportation' is lost, because no classical information is transmitted from Alice to Bob, but it is clear that the overall action of the two quantum circuits is the same, which is the key point.)

The second principle is even more obvious - and surprisingly useful!

Figure 4.14. Symbol for projective measurement on a single qubit. In this circuit nothing further is done with the measurement result, but in more general quantum circuits it is possible to change later parts of the quantum circuit, conditional on measurement outcomes in earlier parts of the circuit. Such a usage of classical information is depicted using wires drawn with double lines (not shown here).

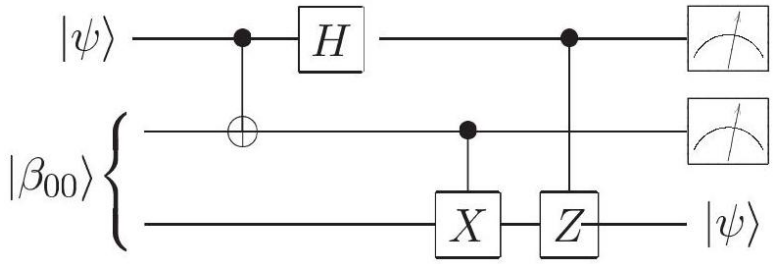


Figure 4.15. Quantum teleportation circuit in which measurements are done at the end, instead of in the middle of the circuit. As in Figure 1.13, the top two qubits belong to Alice, and the bottom one to Bob.

Principle of implicit measurement: Without loss of generality, any unterminated quantum wires (qubits which are not measured) at the end of a quantum circuit may be assumed to be measured.

To understand why this is true, imagine you have a quantum circuit containing just two qubits, and only the first qubit is measured at the end of the circuit. Then the measurement statistics observed at this time are completely determined by the reduced density matrix of the first qubit. However, if a measurement had also been performed on the second qubit, then it would be highly surprising if that measurement could change the statistics of measurement on the first qubit. You'll prove this in Exercise 4.32 by showing that the reduced density matrix of the first qubit is not affected by performing a measurement on the second.

As you consider the role of measurements in quantum circuits, it is important to keep in mind that in its role as an interface between the quantum and classical worlds, measurement is generally considered to be an irreversible operation, destroying quantum information and replacing it with classical information. In certain carefully designed cases, however, this need not be true, as is vividly illustrated by teleportation and quantum error-correction (Chapter 10). What teleportation and quantum error-correction have in common is that in neither instance does the measurement result reveal any information about the identity of the quantum state being measured. Indeed, we will see in Chapter 10 that this is a more general feature of measurement - in order for a measurement to be reversible, it must reveal no information about the quantum state being measured!

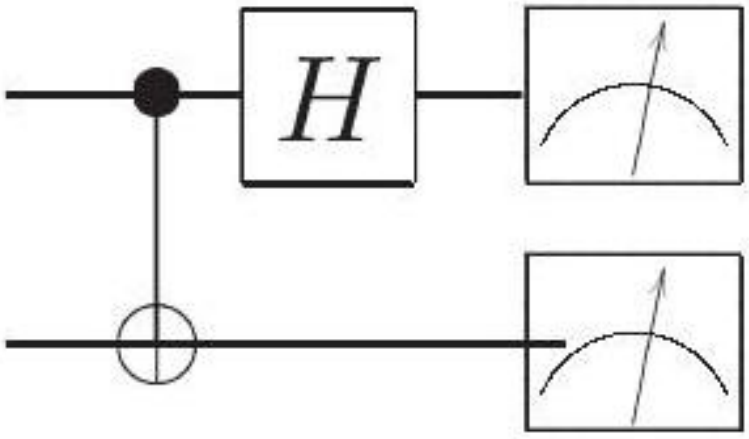
Exercise 4.32: Suppose ρ is the density matrix describing a two qubit system.
Suppose we perform a projective measurement in the computational basis of the second qubit. Let $P_0 = |0\rangle\langle 0|$ and $P_1 = |1\rangle\langle 1|$ be the projectors onto the $|0\rangle$ and $|1\rangle$ states of the second

qubit, respectively. Let ρ' be the density matrix which would be assigned to the system after the measurement by an observer who did not learn the measurement result. Show that

$$\rho' = P_0 \rho P_0 + P_1 \rho P_1. \tag{4.40}$$

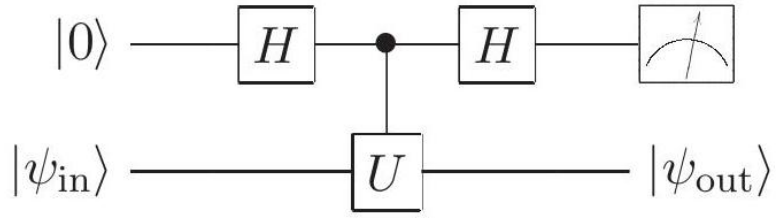
Also show that the reduced density matrix for the first qubit is not affected by the measurement, that is, $\mathrm{tr}_2(\rho) = \mathrm{tr}_2(\rho')$.

Exercise 4.33: (Measurement in the Bell basis) The measurement model we have specified for the quantum circuit model is that measurements are performed only
in the computational basis. However, often we want to perform a measurement in some other basis, defined by a complete set of orthonormal states. To perform this measurement, simply unitarily transform from the basis we wish to perform the measurement in to the computational basis, then measure. For example, show that the circuit

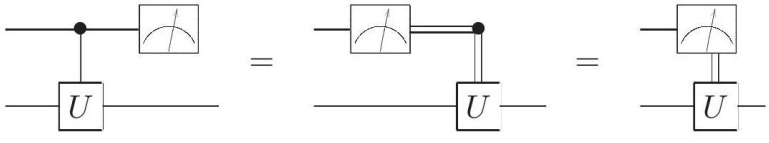


performs a measurement in the basis of the Bell states. More precisely, show that this circuit results in a measurement being performed with corresponding POVM elements the four projectors onto the Bell states. What are the corresponding measurement operators?

Exercise 4.34: (Measuring an operator) Suppose we have a single qubit operator U with eigenvalues ± 1, so that U is both Hermitian and unitary, so it can be regarded both as an observable and a quantum gate. Suppose we wish to measure the observable U. That is, we desire to obtain a measurement result indicating one of the two eigenvalues, and leaving a post-measurement state which is the corresponding eigenvector. How can this be implemented by a quantum circuit? Show that the following circuit implements a measurement of U :



Exercise 4.35: (Measurement commutes with controls) A consequence of the principle of deferred measurement is that measurements commute with quantum gates when the qubit being measured is a control qubit, that is:



(Recall that the double lines represent classical bits in this diagram.) Prove the first equality. The rightmost circuit is simply a convenient notation to depict the use of a measurement result to classically control a quantum gate.

8.1.5 4.5 Universal quantum gates

A small set of gates (e.g. AND, OR, NOT) can be used to compute an arbitrary classical function, as we saw in Section 3.1.2. We say that such a set of gates is universal for classical computation. In fact, since the Toffoli gate is universal for classical computation, quantum circuits subsume classical circuits. A similar universality result is true for quantum computation, where a set of gates is said to be universal for quantum computation if any unitary operation may be approximated to arbitrary accuracy by a quantum circuit
involving only those gates. We now describe three universality constructions for quantum computation. These constructions build upon each other, and culminate in a proof that any unitary operation can be approximated to arbitrary accuracy using Hadamard, phase, cnot, and $\pi/8$ gates. You may wonder why the phase gate appears in this list, since it can be constructed from two $\pi/8$ gates; it is included because of its natural role in the fault-tolerant constructions described in Chapter 10.

The first construction shows that an arbitrary unitary operator may be expressed *ex* actly as a product of unitary operators that each acts non-trivially only on a subspace spanned by two computational basis states. The second construction combines the first construction with the results of the previous section to show that an arbitrary unitary operator may be expressed exactly using single qubit and CNOT gates. The third construction combines the second construction with a proof that single qubit operation may be approximated to arbitrary accuracy using the Hadamard, phase, and $\pi/8$ gates. This in turn implies that any unitary operation can be approximated to arbitrary accuracy using Hadamard, phase, cNOT, and $\pi/8$ gates.

Our constructions say little about efficiency - how many (polynomially or exponentially many) gates must be composed in order to create a given unitary transform. In Section 4.5.4 we show that there exist unitary transforms which require exponentially many gates to approximate. Of course, the goal of quantum computation is to find interesting families of unitary transformations that can be performed efficiently.

Exercise 4.36: Construct a quantum circuit to add two two-bit numbers x and y modulo 4. That is, the circuit should perform the transformation $|x, y\rangle \rightarrow |x, x + y \bmod 4\rangle$.

8.1.6 4.5.1 Two-level unitary gates are universal

Consider a unitary matrix U which acts on a d-dimensional Hilbert space. In this section we explain how U may be decomposed into a product of two-level unitary matrices; that is, unitary matrices which act non-trivially only on two-or-fewer vector components. The essential idea behind this decomposition may be understood by considering the case when U is 3×3, so suppose that U has the form

$$U = \begin{bmatrix} a & d & g \\ b & e & h \\ c & f & j \end{bmatrix} \tag{4.41}$$

We will find two-level unitary matrices $U_1, \ldots, U_3$ such that

$$U_3 U_2 U_1 U = I \tag{4.42}$$

It follows that

$$U = U_1^\dagger U_2^\dagger U_3^\dagger \tag{4.43}$$

U_1, U_2 and U_3 are all two-level unitary matrices, and it is easy to see that their inverses, $U_1^\dagger, U_2^\dagger$ and $U_3^\dagger$ are also two-level unitary matrices. Thus, if we can demonstrate (4.42), then we will have shown how to break U up into a product of two-level unitary matrices.

Use the following procedure to construct U_1 : if $b = 0$ then set

$$U_1 \equiv \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \tag{4.44}$$

If $b \neq 0$ then set

$$U_1 \equiv \begin{bmatrix} \frac{a^*}{\sqrt{|a|^2+|b|^2}} & \frac{b^*}{\sqrt{|a|^2+|b|^2}} & 0 \\ \frac{b}{\sqrt{|a|^2+|b|^2}} & \frac{-a}{\sqrt{|a|^2+|b|^2}} & 0 \\ 0 & 0 & 1 \end{bmatrix} \tag{4.45}$$

Note that in either case U_1 is a two-level unitary matrix, and when we multiply the matrices out we get

$$U_1 U = \begin{bmatrix} a' & d' & g' \\ 0 & e' & h' \\ c' & f' & j' \end{bmatrix} \tag{4.46}$$

The key point to note is that the middle entry in the left hand column is zero. We denote the other entries in the matrix with a generic prime ' ; their actual values do not matter.

Now apply a similar procedure to find a two-level matrix U_2 such that $U_2 U_1 U$ has no entry in the bottom left corner. That is, if $c' = 0$ we set

$$U_2 \equiv \begin{bmatrix} a'^* & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \tag{4.47}$$

while if $c' \neq 0$ then we set

$$U_2 \equiv \begin{bmatrix} \frac{a'^*}{\sqrt{|a'|^2+|c'|^2}} & 0 & \frac{c'^*}{\sqrt{|a'|^2+|c'|^2}} \\ 0 & 1 & 0 \\ \frac{c'}{\sqrt{|a'|^2+|c'|^2}} & 0 & \frac{-a'}{\sqrt{|a'|^2+|c'|^2}} \end{bmatrix} \tag{4.48}$$

In either case, when we carry out the matrix multiplication we find that

$$U_2 U_1 U = \begin{bmatrix} 1 & d'' & g'' \\ 0 & e'' & h'' \\ 0 & f'' & j'' \end{bmatrix} \tag{4.49}$$

Since U, U_1 and U_2 are unitary, it follows that $U_2 U_1 U$ is unitary, and thus $d'' = g'' = 0$, since the first row of $U_2 U_1 U$ must have norm 1. Finally, set

$$U_3 \equiv \begin{bmatrix} 1 & 0 & 0 \\ 0 & e''^* & f''^* \\ 0 & h''^* & j''^* \end{bmatrix}. \tag{4.50}$$

It is now easy to verify that $U_3 U_2 U_1 U = I$, and thus $U = U_1^\dagger U_2^\dagger U_3^\dagger$, which is a decomposition of U into two-level unitaries.

More generally, suppose U acts on a d-dimensional space. Then, in a similar fashion to the 3×3 case, we can find two-level unitary matrices $U_1, \ldots, U_{d-1}$ such that the matrix

$U_{d-1}U_{d-2}\ldots U_1U$ has a one in the top left hand corner, and all zeroes elsewhere in the first row and column. We then repeat this procedure for the $d-1$ by $d-1$ unitary submatrix in the lower right hand corner of $U_{d-1}U_{d-2}\ldots U_1U$, and so on, with the end result that an arbitrary $d \times d$ unitary matrix may be written

$$U = V_1 \ldots V_k \tag{4.51}$$

where the matrices V_i are two-level unitary matrices, and $k \leq (d-1) + (d-2) + \cdots + 1 = d(d-1)/2$.

Exercise 4.37: Provide a decomposition of the transform

$$\frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix} \tag{4.52}$$

into a product of two-level unitaries. This is a special case of the quantum Fourier transform, which we study in more detail in the next chapter.

A corollary of the above result is that an arbitrary unitary matrix on an n qubit system may be written as a product of at most $2^{n-1}(2^n - 1)$ two-level unitary matrices. For specific unitary matrices, it may be possible to find much more efficient decompositions, but as you will now show there exist matrices which cannot be decomposed as a product of fewer than $d-1$ two-level unitary matrices!

Exercise 4.38: Prove that there exists a $d \times d$ unitary matrix U which cannot be decomposed as a product of fewer than $d-1$ two-level unitary matrices.

8.1.7 4.5.2 Single qubit and CNOT gates are universal

We have just shown that an arbitrary unitary matrix on a d-dimensional Hilbert space may be written as a product of two-level unitary matrices. Now we show that single qubit and CNOT gates together can be used to implement an arbitrary two-level unitary operation on the state space of n qubits. Combining these results we see that single qubit and CNOT gates can be used to implement an arbitrary unitary operation on n qubits, and therefore are universal for quantum computation.

Suppose U is a two-level unitary matrix on an n qubit quantum computer. Suppose in particular that U acts non-trivially on the space spanned by the computational basis states $|s\rangle$ and $|t\rangle$, where $s = s_1 \ldots s_n$ and $t = t_1 \ldots t_n$ are the binary expansions for s and t. Let $\tilde{U}$ be the non-trivial 2×2 unitary submatrix of U; $\tilde{U}$ can be thought of as a unitary operator on a single qubit.

Our immediate goal is to construct a circuit implementing U, built from single qubit and cNOT gates. To do this, we need to make use of Gray codes. Suppose we have distinct binary numbers, s and t. A Gray code connecting s and t is a sequence of binary numbers, starting with s and concluding with t, such that adjacent members of the list differ in exactly one bit. For instance, with $s = 101001$ and $t = 110011$ we have the Gray
code

$$\begin{matrix} 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 \end{matrix}$$

Let g_1 through g_m be the elements of a Gray code connecting s and t, with $g_1 = s$ and $g_m = t$. Note that we can always find a Gray code such that $m \leq n+1$ since s and t can differ in at most n locations.

The basic idea of the quantum circuit implementing U is to perform a sequence of gates effecting the state changes $|g_1\rangle \rightarrow |g_2\rangle \rightarrow \ldots \rightarrow |g_{m-1}\rangle$, then to perform a controlled- $\tilde{U}$ operation, with the target qubit located at the single bit where g_{m-1} and g_m differ, and then to undo the first stage, transforming $|g_{m-1}\rangle \rightarrow |g_{m-2}\rangle \rightarrow \ldots \rightarrow |g_1\rangle$. Each of these steps can be easily implemented using operations developed earlier in this chapter, and the final result is an implementation of U.

A more precise description of the implementation is as follows. The first step is to swap the states $|g_1\rangle$ and $|g_2\rangle$. Suppose g_1 and g_2 differ at the i th digit. Then we accomplish the swap by performing a controlled bit flip on the i th qubit, conditional on the values of the other qubits being identical to those in both g_1 and g_2. Next we use a controlled operation to swap $|g_2\rangle$ and $|g_3\rangle$. We continue in this fashion until we swap $|g_{m-2}\rangle$ with $|g_{m-1}\rangle$. The effect of this sequence of $m-2$ operations is to achieve the operation

$$|g_1\rangle \rightarrow |g_{m-1}\rangle \tag{4.54}$$
$$|g_2\rangle \rightarrow |g_1\rangle \tag{4.55}$$
$$|g_3\rangle \rightarrow |g_2\rangle \tag{4.56}$$
$$\ldots\ldots$$
$$|g_{m-1}\rangle \rightarrow |g_{m-2}\rangle\,. \tag{4.57}$$

All other computational basis states are left unchanged by this sequence of operations. Next, suppose g_{m-1} and g_m differ in the j th bit. We apply a controlled- $\tilde{U}$ operation with the j th qubit as target, conditional on the other qubits having the same values as appear in both g_m and g_{m-1}. Finally, we complete the U operation by undoing the swap operations: we swap $|g_{m-1}\rangle$ with $|g_{m-2}\rangle$, then $|g_{m-2}\rangle$ with $|g_{m-3}\rangle$ and so on, until we swap $|g_2\rangle$ with $|g_1\rangle$.

A simple example illuminates the procedure further. Suppose we wish to implement the two-level unitary transformation

$$U = \begin{bmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & c \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ b & 0 & 0 & 0 & 0 & 0 & 0 & d \end{bmatrix}. \tag{4.58}$$

Here, a, b, c and d are any complex numbers such that $\tilde{U} \equiv \begin{bmatrix} a & c \\ b & d \end{bmatrix}$ is a unitary matrix.

Notice that U acts non-trivially only on the states $|000\rangle$ and $|111\rangle$. We write a Gray code connecting 000 and 111:

A	B	C
0	0	0
0	0	1
0	1	1
1	1	1

.

From this we read off the required circuit, shown in Figure 4.16. The first two gates shuffle the states so that $|000\rangle$ gets swapped with $|011\rangle$. Next, the operation $\tilde{U}$ is applied to the first qubit of the states $|011\rangle$ and $|111\rangle$, conditional on the second and third qubits being in the state $|11\rangle$. Finally, we unshuffle the states, ensuring that $|011\rangle$ gets swapped back with the state $|000\rangle$.

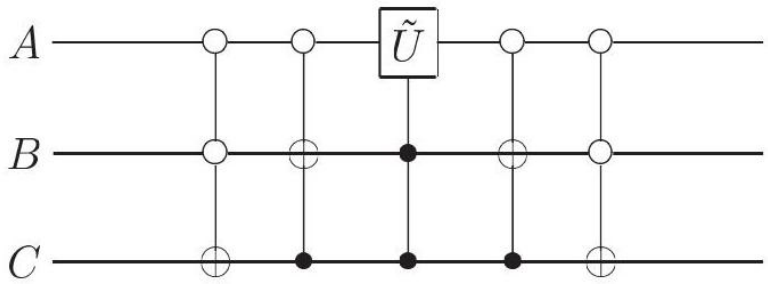


Figure 4.16. Circuit implementing the two-level unitary operation defined by (4.58).

Returning to the general case, we see that implementing the two-level unitary operation U requires at most $2(n-1)$ controlled operations to swap $|g_1\rangle$ with $|g_{m-1}\rangle$ and then back again. Each of these controlled operations can be realized using $O(n)$ single qubit and cNOT gates; the controlled- $\tilde{U}$ operation also requires $O(n)$ gates. Thus, implementing U requires $O\left(n^2\right)$ single qubit and cNOT gates. We saw in the previous section that an arbitrary unitary matrix on the 2^n-dimensional state space of n qubits may be written as a product of $O\left(2^{2n}\right) = O\left(4^n\right)$ two-level unitary operations. Combining these results, we see that an arbitrary unitary operation on n qubits can be implemented using a circuit containing $O\left(n^2 4^n\right)$ single qubit and CNOT gates. Obviously, this construction does not provide terribly efficient quantum circuits! However, we show in Section 4.5.4 that the construction is close to optimal in the sense that there are unitary operations that require an exponential number of gates to implement. Thus, to find fast quantum algorithms we will clearly need a different approach than is taken in the universality construction.

Exercise 4.39: Find a quantum circuit using single qubit operations and CNOTs to implement the transformation

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & a & 0 & 0 & 0 & 0 & c \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & b & 0 & 0 & 0 & 0 & d \end{bmatrix}, \tag{4.60}$$

where $\tilde{U} = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$ is an arbitrary 2×2 unitary matrix.

8.1.8 4.5.3 A discrete set of universal operations

In the previous section we proved that the CNOT and single qubit unitaries together form a universal set for quantum computation. Unfortunately, no straightforward method is known to implement all these gates in a fashion which is resistant to errors. Fortunately, in this section

we'll find a discrete set of gates which can be used to perform universal quantum computation, and in Chaper 10 we'll show how to perform these gates in an error-resistant fashion, using quantum error-correcting codes.

Approximating unitary operators

Obviously, a discrete set of gates can't be used to implement an arbitrary unitary operation exactly, since the set of unitary operations is continuous. Rather, it turns out that a discrete set can be used to approximate any unitary operation. To understand how this works, we first need to study what it means to approximate a unitary operation. Suppose U and V are two unitary operators on the same state space. U is the target unitary operator that we wish to implement, and V is the unitary operator that is actually implemented in practice. We define the error when V is implemented instead of U by

$$E(U,V) \equiv \max_{|\psi\rangle} \|(U-V)|\psi\rangle\|, \tag{4.61}$$

where the maximum is over all normalized quantum states $|\psi\rangle$ in the state space. In Box 4.1 on page 195 we show that this measure of error has the interpretation that if $E(U,V)$ is small, then any measurement performed on the state $V|\psi\rangle$ will give approximately the same measurement statistics as a measurement of $U|\psi\rangle$, for any initial state $|\psi\rangle$. More precisely, we show that if M is a POVM element in an arbitrary POVM, and P_U (or P_V) is the probability of obtaining this outcome if U (or V) were performed with a starting state $|\psi\rangle$, then

$$|P_U - P_V| \leq 2E(U,V). \tag{4.62}$$

Thus, if $E(U,V)$ is small, then measurement outcomes occur with similar probabilities, regardless of whether U or V were performed. Also shown in Box 4.1 is that if we perform a sequence of gates $V_1,\ldots,V_m$ intended to approximate some other sequence of gates $U_1,\ldots,U_m$, then the errors add at most linearly,

$$E\left(U_m U_{m-1}\ldots U_1, V_m V_{m-1}\ldots V_1\right) \leq \sum_{j=1}^{m} E\left(U_j, V_j\right) \tag{4.63}$$

The approximation results (4.62) and (4.63) are extremely useful. Suppose we wish to perform a quantum circuit containing m gates, U_1 through U_m. Unfortunately, we are only able to approximate the gate U_j by the gate V_j. In order that the probabilities of different measurement outcomes obtained from the approximate circuit be within a tolerance $\Delta > 0$ of the correct probabilities, it suffices that $E\left(U_j, V_j\right) \leq \Delta/(2m)$, by the results (4.62) and (4.63).

Universality of Hadamard + phase + CNOT + $\pi/8$ gates

We're now in a good position to study the approximation of arbitrary unitary operations by discrete sets of gates. We're going to consider two different discrete sets of gates, both

Box 4.1: Approximating quantum circuits

Suppose a quantum system starts in the state $|\psi\rangle$, and we perform either the unitary operation U, or the unitary operation V. Following this, we perform a measurement. Let M be a POVM element associated with the measurement, and let P_U (or P_V) be the probability of obtaining the corresponding measurement outcome if the operation U (or V) was performed. Then

$$|P_U - P_V| = \left|\langle\psi|U^\dagger M U\big|\,\psi\right\rangle - \langle\psi|V^\dagger M V|\psi\rangle\,|\,. \tag{4.64}$$

Let $|\Delta\rangle \equiv (U-V)|\psi\rangle$. Simple algebra and the Cauchy-Schwarz inequality show that

$$\begin{aligned} |P_U - P_V| &= \left|\langle\psi|U^\dagger M\right| \Delta\rangle + \langle\Delta|MV|\psi\rangle \mid . && (4.65)\\ &\leq \left|\langle\psi|U^\dagger M\right| \Delta\rangle \mid + |\langle\Delta|MV|\psi\rangle \mid && (4.66)\\ &\leq \||\Delta\rangle\| + \||\Delta\rangle\| && (4.67)\\ &\leq 2E(U,V). && (4.68) \end{aligned}$$

The inequality $|P_U - P_V| \leq 2E(U,V)$ gives quantitative expression to the idea that when the error $E(U,V)$ is small, the difference in probabilities between measurement outcomes is also small.
Suppose we perform a sequence $V_1, V_2, \ldots, V_m$ of gates intended to approximate some other sequence of gates, $U_1, U_2, \ldots, U_m$. Then it turns out that the error caused by the entire sequence of imperfect gates is at most the sum of the errors in the individual gates,

$$E\left(U_m U_{m-1} \ldots U_1, V_m V_{m-1} \ldots V_1\right) \leq \sum_{j=1}^{m} E\left(U_j, V_j\right) \tag{4.69}$$

To prove this we start with the case $m = 2$. Note that for some state $|\psi\rangle$ we have

$$\begin{aligned} E\left(U_2U_1, V_2V_1\right) &= \left\| \left(U_2U_1 - V_2V_1\right)|\psi\rangle \right\| && (4.70)\\ &= \left\| \left(U_2U_1 - V_2U_1\right)|\psi\rangle + \left(V_2U_1 - V_2V_1\right)|\psi\rangle \right\|. && (4.71) \end{aligned}$$

Using the triangle inequality $\||a\rangle + |b\rangle\| \leq \||a\rangle\| + \||b\rangle\|$, we obtain

$$\begin{aligned} E\left(U_2U_1, V_2V_1\right) &\leq \left\| \left(U_2 - V_2\right)U_1|\psi\rangle \right\| + \left\| V_2\left(U_1 - V_1\right)|\psi\rangle \right\| && (4.72)\\ &\leq E\left(U_2, V_2\right) + E\left(U_1, V_1\right) && (4.73) \end{aligned}$$

which was the desired result. The result for general m follows by induction.
of which are universal. The first set, the standard set of universal gates, consists of the Hadamard, phase, controlled-NOT and $\pi/8$ gates. We provide fault-tolerant constructions for these gates in Chapter 10; they also provide an exceptionally simple universality construction. The second set of gates we consider consists of the Hadamard gate, phase gate, the controlled-NOT gate, and the Toffoli gate. These gates can also all be done faulttolerantly; however, the universality proof and fault-tolerance construction for these gates is a little less appealing.

We begin the universality proof by showing that the Hadamard and $\pi/8$ gates can be used to approximate any single qubit unitary operation to arbitrary accuracy. Consider the gates T and $HTH.T$ is, up to an unimportant global phase, a rotation by $\pi/4$ radians around the $\hat{z}$ axis on the Bloch sphere, while HTH is a rotation by $\pi/4$ radians around the $\hat{x}$ axis on the Bloch sphere (Exercise 4.14). Composing these two operations gives, up to a global phase,

$$\begin{aligned} \exp\left(-i\frac{\pi}{8}Z\right)\exp\left(-i\frac{\pi}{8}X\right) &= \left[\cos\frac{\pi}{8}I - i\sin\frac{\pi}{8}Z\right]\left[\cos\frac{\pi}{8}I - i\sin\frac{\pi}{8}X\right] && (4.74)\\ &= \cos^2\frac{\pi}{8}I - i\left[\cos\frac{\pi}{8}(X+Z) + \sin\frac{\pi}{8}Y\right]\sin\frac{\pi}{8} && (4.75) \end{aligned}$$

This is a rotation of the Bloch sphere about an axis along $\vec{n} = \left(\cos\frac{\pi}{8}, \sin\frac{\pi}{8}, \cos\frac{\pi}{8}\right)$ with corresponding unit vector $\hat{n}$, and through an angle θ defined by $\cos(\theta/2) \equiv \cos^2\frac{\pi}{8}$. That is,

using only the Hadamard and $\pi/8$ gates we can construct $R_{\hat{n}}(\theta)$. Moreover, this θ can be shown to be an irrational multiple of 2π. Proving this latter fact is a little beyond our scope; see the end of chapter 'History and further reading'.

Next, we show that repeated iteration of $R_{\hat{n}}(\theta)$ can be used to approximate to arbitrary accuracy any rotation $R_{\hat{n}}(\alpha)$. To see this, let $\delta > 0$ be the desired accuracy, and let N be an integer larger than $2\pi/\delta$. Define θ_k so that $\theta_k \in [0, 2\pi)$ and $\theta_k = (k\theta) \bmod 2\pi$. Then the pigeonhole principle implies that there are distinct j and k in the range $1, \ldots, N$ such that $|\theta_k - \theta_j| \leq 2\pi/N < \delta$. Without loss of generality assume that $k > j$, so we have $|\theta_{k-j}| < \delta$. Since $j \neq k$ and θ is an irrational multiple of 2π we must have $\theta_{k-j} \neq 0$. It follows that the sequence $\theta_{l(k-j)}$ fills up the interval $[0, 2\pi)$ as l is varied, so that adjacent members of the sequence are no more than δ apart. It follows that for any $\epsilon > 0$ there exists an n such that

$$E\left(R_{\hat{n}}(\alpha), R_{\hat{n}}(\theta)^n\right) < \frac{\epsilon}{3}. \tag{4.76}$$

Exercise 4.40: For arbitrary α and β show that

$$E\left(R_{\hat{n}}(\alpha), R_{\hat{n}}(\alpha+\beta)\right) = |1 - \exp(i\beta/2)|, \tag{4.77}$$

and use this to justify (4.76).

We are now in position to verify that any single qubit operation can be approximated to arbitrary accuracy using the Hadamard and $\pi/8$ gates. Simple algebra implies that for any α

$$HR_{\hat{n}}(\alpha)H = R_{\hat{m}}(\alpha), \tag{4.78}$$

where $\hat{m}$ is a unit vector in the direction $(\cos\frac{\pi}{8}, -\sin\frac{\pi}{8}, \cos\frac{\pi}{8})$, from which it follows that

$$E\left(R_{\hat{m}}(\alpha), R_{\hat{m}}(\theta)^n\right) < \frac{\epsilon}{3}. \tag{4.79}$$

But by Exercise 4.11 an arbitrary unitary U on a single qubit may be written as

$$U = R_{\hat{n}}(\beta)R_{\hat{m}}(\gamma)R_{\hat{n}}(\delta), \tag{4.80}$$

up to an unimportant global phase shift. The results (4.76) and (4.79), together with the chaining inequality (4.63) therefore imply that for suitable positive integers n_1, n_2, n_3,

$$E\left(U, R_{\hat{n}}(\theta)^{n_1} H R_{\hat{n}}(\theta)^{n_2} H R_{\hat{n}}(\theta)^{n_3}\right) < \epsilon \tag{4.81}$$

That is, given any single qubit unitary operator U and any $\epsilon > 0$ it is possible to approximate U to within ϵ using a circuit composed of Hadamard gates and $\pi/8$ gates alone.

Since the $\pi/8$ and Hadamard gates allow us to approximate any single qubit unitary operator, it follows from the arguments of Section 4.5.2 that we can approximate any m gate quantum circuit, as follows. Given a quantum circuit containing m gates, either CNOTS or single qubit unitary gates, we may approximate it using Hadamard, controlled-not and $\pi/8$ gates (later, we will find that phase gates make it possible to do the appoximation fault-tolerantly, but for the present universality argument they are not strictly necessary). If we desire an accuracy of ϵ for the entire circuit, then this may be achieved by approximating each single qubit unitary using the above procedure to within ϵ/m and applying the chaining inequality (4.63) to obtain an accuracy of ϵ for the entire circuit.

How efficient is this procedure for approximating quantum circuits using a discrete set of gates? This is an important question. Suppose, for example, that approximating an arbitrary single qubit unitary to within a distance ϵ were to require $\Omega\left(2^{1/\epsilon}\right)$ gates from the discrete set. Then to approximate the m gate quantum circuit considered in the previous paragraph would require $\Omega\left(m2^{m/\epsilon}\right)$ gates, an exponential increase over the original circuit size! Fortunately, the

rate of convergence is much better than this. Intuitively, it is plausible that the sequence of angles θ_k 'fills in' the interval $[0, 2\pi)$ in a more or less uniform fashion, so that to approximate an arbitrary single qubit gate ought to take roughly $\Theta(1/\epsilon)$ gates from the discrete set. If we use this estimate for the number of gates required to approximate an arbitrary single qubit gate, then the number required to approximate an m gate circuit to accuracy ϵ becomes $\Theta\left(m^2/\epsilon\right)$. This is a quadratic increase over the original size of the circuit, m, which for many applications may be sufficient.

Rather remarkably, however, a much faster rate of convergence can be proved. The Solovay-Kitaev theorem, proved in Appendix 3, implies that an arbitrary single qubit gate may be approximated to an accuracy ϵ using $O\left(\log^c(1/\epsilon)\right)$ gates from our discrete set, where c is a constant approximately equal to 2 . The Solovay-Kitaev theorem therefore implies that to approximate a circuit containing m CNOTs and single qubit unitaries to an accuracy ϵ requires $O\left(m \log^c(m/\epsilon)\right)$ gates from the discrete set, a polylogarithmic increase over the size of the original circuit, which is likely to be acceptable for virtually all applications.

To sum up, we have shown that the Hadamard, phase, controlled-not and $\pi/8$ gates are universal for quantum computation in the sense that given a circuit containing CNOTS and arbitrary single qubit unitaries it is possible to simulate this circuit to good accuracy using only this discrete set of gates. Moreover, the simulation can be performed efficiently, in the sense that the overhead required to perform the simulation is polynomial in $\log(m/\epsilon)$, where m is the number of gates in the original circuit, and ϵ is the desired accuracy of the simulation.

Exercise 4.41: This and the next two exercises develop a construction showing that the Hadamard, phase, controlled-not and Toffoli gates are universal. Show that

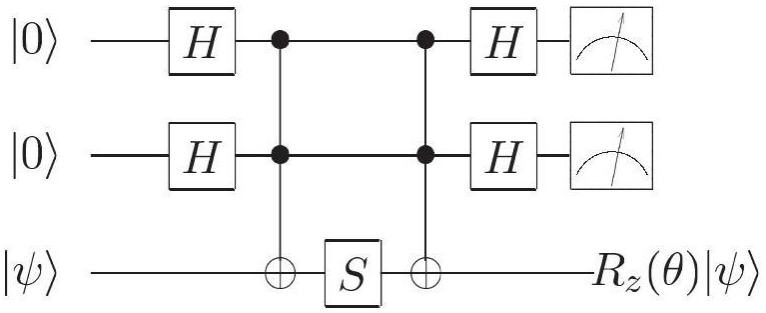


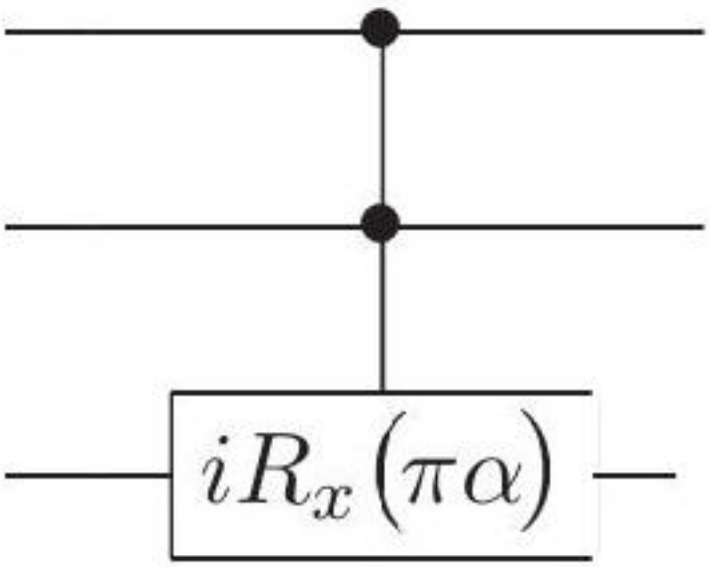
Figure 4.17. Provided both measurement outcomes are 0 this circuit applies $R_{z(\theta)}$ to the target, where $\cos\theta = 3/5$. If some other measurement outcome occurs then the circuit applies Z to the target.}

the circuit in Figure 4.17 applies the operation $R_z(\theta)$ to the third (target) qubit if the measurement outcomes are both 0 , where $\cos\theta = 3/5$, and otherwise applies Z to the target qubit. Show that the probability of both measurement outcomes being 0 is 5/8, and explain how repeated use of this circuit and $Z = S^2$ gates may be used to apply a $R_z(\theta)$ gate with probability approaching 1 .

Exercise 4.42: (Irrationality of θ) Suppose $\cos\theta = 3/5$. We give a proof by contradiction that θ is an irrational multiple of 2π.
(1) Using the fact that $e^{i\theta} = (3 + 4i)/5$, show that if θ is rational, then there must exist a positive integer m such that $(3 + 4i)^m = 5^m$.
(2) Show that $(3 + 4i)^m = 3 + 4i(\mathrm{mod}5)$ for all $m > 0$, and conclude that no m such that $(3 + 4i)^m = 5^m$ can exist.

Exercise 4.43: Use the results of the previous two exercises to show that the Hadamard, phase, controlled-NOT and Toffoli gates are universal for quantum computation.

Exercise 4.44: Show that the three qubit gate G defined by the circuit:



is universal for quantum computation whenever α is irrational.
Exercise 4.45: Suppose U is a unitary transform implemented by an n qubit quantum circuit constructed from H, S, CNOT and Toffoli gates. Show that U is of the form $2^{-k/2}M$, for some integer k, where M is a $2^n \times 2^n$ matrix with only complex integer entries. Repeat this exercise with the Toffoli gate replaced by the $\pi/8$ gate.

8.1.9 4.5.4 Approximating arbitrary unitary gates is generically hard

We've seen that any unitary transformation on n qubits can be built up out of a small set of elementary gates. Is it always possible to do this efficiently? That is, given a unitary transformation U on n qubits does there always exist a circuit of size polynomial in n approximating U ? The answer to this question turns out to be a resounding no: in fact, most unitary transformations can only be implemented very inefficiently. One way to see
this is to consider the question: how many gates does it take to generate an arbitrary state of n qubits? A simple counting argument shows that this requires exponentially many operations, in general; it immediately follows that there are unitary operations requiring exponentially many operations. To see this, suppose we have g different types of gates available, and each gate works on at most f input qubits. These numbers, f and g, are fixed by the computing hardware we have available, and may be considered to be constants. Suppose we have a quantum circuit containing m gates, starting from the computational basis state $|0\rangle^{\otimes n}$. For any particular gate in the circuit there are therefore at most $\left[\begin{array}{c} n \\ f \end{array} \right]^g = O\left(n^{fg}\right)$ possible choices. It follows that at most $O\left(n^{fgm}\right)$ different states may be computed using m gates.

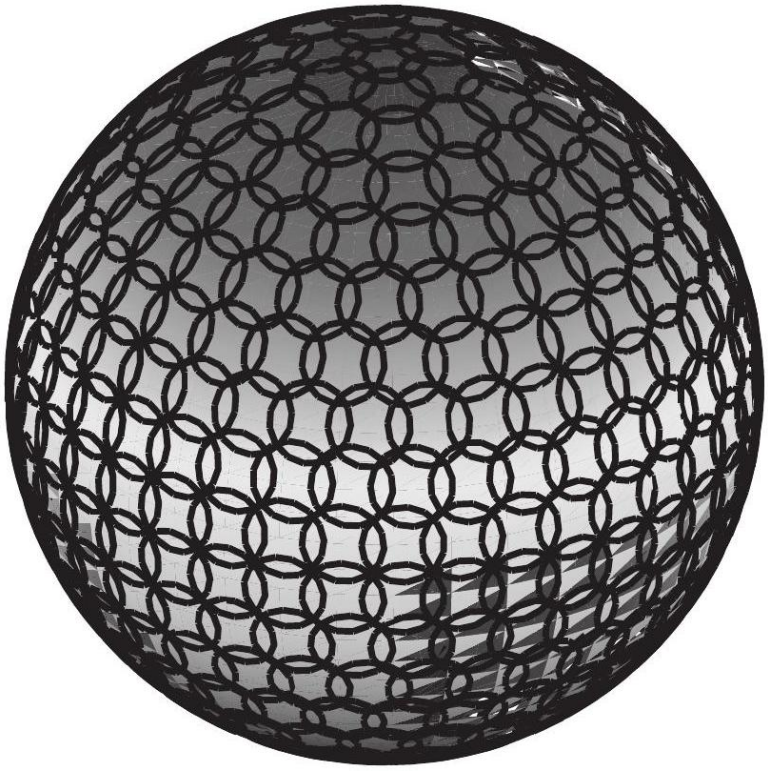


Figure 4.18. Visualization of covering the set of possible states with patches of constant radius.

Suppose we wish to approximate a particular state, $|\psi\rangle$, to within a distance ϵ. The idea of the proof is to cover the set of all possible states with a collection of 'patches,' each of radius ϵ (Figure 4.18), and then to show that the number of patches required rises doubly exponentially in n; comparing with the exponential number of different states that may be computed using m gates will imply the result. The first observation we need is that the space of state vectors of n qubits can be regarded as just the unit $(2^{n+1}-1)$-sphere. To see this, suppose the n qubit state has amplitudes $\psi_j = X_j + iY_j$, where X_j and Y_j are the real and imaginary parts, respectively, of the j th amplitude. The normalization condition for quantum states can be written $\sum_j \left(X_j^2 + Y_j^2\right) = 1$, which is just the condition for a point to be on the unit sphere in 2^{n+1} real dimensions, that is, the unit ($2^{n+1}-1$)-sphere. Similarly, the surface area of radius ϵ near $|\psi\rangle$ is approximately the same as the volume of a $(2^{n+1}-2)$-sphere of radius ϵ. Using the formula $S_k(r) = 2\pi^{(k+1)/2} r^k / \Gamma((k+1)/2)$ for the surface area of a k-sphere of radius r, and $V_k(r) = 2\pi^{(k+1)/2} r^{k+1} / [(k+1)\Gamma((k+1)/2)]$ for the volume of a k-sphere of radius r, we see that the number of patches needed to
cover the state space goes like

$$\frac{S_{2^{n+1}-1}(1)}{V_{2^{n+1}-2}(\epsilon)} = \frac{\sqrt{\pi}\Gamma\left(2^n - \frac{1}{2}\right)\left(2^{n+1}-1\right)}{\Gamma\left(2^n\right)\epsilon^{2^{n+1}-1}} \tag{4.82}$$

where Γ is the usual generalization of the factorial function. But $\Gamma\left(2^n - 1/2\right) \geq \Gamma\left(2^n\right)/2^n$, so the number of patches required to cover the space is at least

$$\Omega\left(\frac{1}{\epsilon^{2^{n+1}-1}}\right) \tag{4.83}$$

Recall that the number of patches which can be reached in m gates is $O\left(n^{fgm}\right)$, so in order to reach all the ϵ-patches we must have

$$O\left(n^{fgm}\right) \geq \Omega\left(\frac{1}{\epsilon^{2^{n+1}-1}}\right) \tag{4.84}$$

which gives us

$$m = \Omega\left(\frac{2^n \log(1/\epsilon)}{\log(n)}\right) \tag{4.85}$$

That is, there are states of n qubits which take $\Omega\left(2^n \log(1/\epsilon)/\log(n)\right)$ operations to approximate to within a distance ϵ. This is exponential in n, and thus is 'difficult', in the sense of computational complexity introduced in Chapter 3. Furthermore, this immediately implies that there are unitary transformations U on n qubits which take $\Omega\left(2^n \log(1/\epsilon)/\log(n)\right)$ operations to approximate by a quantum circuit implementing an operation V such that $E(U,V) \leq \epsilon$. By contrast, using our universality constructions and the Solovay-Kitaev theorem it follows that an arbitrary unitary operation U on n qubits may be approximated to within a distance ϵ using $O\left(n^2 4^n \log^c\left(n^2 4^n/\epsilon\right)\right)$ gates. Thus, to within a polynomial factor the construction for universality we have given is optimal; unfortunately, it does not address the problem of determining which families of unitary operations can be computed efficiently in the quantum circuits model.

8.1.10 4.5.5 Quantum computational complexity

In Chapter 3 we described a theory of 'computational complexity' for classical computers that classified the resource requirements to solve computational problems on classical computers. Not surprisingly there is considerable interest in developing a theory of quantum computational complexity, and relating it to classical computational complexity theory. Although only first steps have been taken in this direction, it will doubtless be an enormously fruitful direction for future researchers. We content ourselves with presenting one result about quantum complexity classes, relating the quantum complexity class BQP to the classical complexity class PSPACE. Our discussion of this result is rather informal; for more details you are referred to the paper of Bernstein and Vazirani referenced in the end of chapter 'History and further reading'.

Recall that PSPACE was defined in Chapter 3 as the class of decision problems which can be solved on a Turing machine using space polynomial in the problem size and an arbitrary amount of time. BQP is an essentially quantum complexity class consisting of those decision problems that can be solved with bounded probability of error using a polynomial size quantum circuit. Slightly more formally, we say a language L is in BQP if there is a family of polynomial size quantum circuits which decides the language,
accepting strings in the language with probability at least 3/4, and rejecting strings which aren't in the language with probability at least 3/4. In practice, what this means is that the quantum circuit takes as input binary strings, and tries to determine whether they are elements of the language or not. At the conclusion of the circuit one qubit is measured, with 0 indicating that the string has been accepted, and 1 indicating rejection. By testing the string a few times to determine whether it is in L, we can determine with very high probability whether a given string is in L.

Of course, a quantum circuit is a fixed entity, and any given quantum circuit can only decide whether strings up to some finite length are in L. For this reason, we use an entire family of circuits in the definition of **BQP**; for every possible input length there is a different circuit in the family. We place two restrictions on the circuit in addition to the acceptance / rejection criterion already described. First, the size of the circuits should only grow polynomially with the size of the input string x for which we are trying to determine whether $x \in L$. Second, we require that the circuits be uniformly generated, in a sense similar to that described in Section

3.1.2. This uniformity requirement arises because, in practice, given a string x of some length n, somebody will have to build a quantum circuit capable of deciding whether x is in L. To do so, they will need to have a clear set of instructions - an algorithm - for building the circuit. For this reason, we require that our quantum circuits be uniformly generated, that is, there is a Turing machine capable of efficiently outputting a description of the quantum circuit. This restriction may seem rather technical, and in practice is nearly always satisfied trivially, but it does save us from pathological examples such as that described in Section 3.1.2. (You might also wonder if it matters whether the Turing machine used in the uniformity requirement is a quantum or classical Turing machine; it turns out that it doesn't matter - see 'History and further reading'.)

One of the most significant results in quantum computational complexity is that **BQP** $\subseteq$ **PSPACE**. It is clear that **BPP** $\subseteq$ **BQP**, where **BPP** is the classical complexity class of decision problems which can be solved with bounded probability of error using polynomial time on a classical Turing machine. Thus we have the chain of inclusions BPP $\subseteq$ **BQP** $\subseteq$ **PSPACE**. Proving that **BQP** $\neq$ **BPP**– intuitively the statement that quantum computers are more powerful than classical computers - will therefore imply that BPP $\neq$ PSPACE. However, it is not presently known whether BPP $\neq$ PSPACE, and proving this would represent a major breakthrough in classical computer science! So proving that quantum computers are more powerful than classical computers would have some very interesting implications for classical computational complexity! Unfortunately, it also means that providing such a proof may be quite difficult.

Why is it that **BQP** $\subseteq$ **PSPACE** ? Here is an intuitive outline of the proof (a rigorous proof is left to the references in 'History and further reading'). Suppose we have an n qubit quantum computer, and do a computation involving a sequence of $p(n)$ gates, where $p(n)$ is some polynomial in n. Supposing the quantum circuit starts in the state $|0\rangle$ we will explain how to evaluate in polynomial space on a classical computer the probability that it ends up in the state $|y\rangle$. Suppose the gates that are executed on the quantum computer are, in order, $U_1, U_2, \ldots, U_{p(n)}$. Then the probability of ending up in the state $|y\rangle$ is the modulus squared of

$$\langle y|U_{p(n)} \cdots U_2 U_1|0\rangle. \tag{4.86}$$

This quantity may be estimated in polynomial space on a classical computer. The basic idea is to insert the completeness relation $\sum_x |x\rangle\langle x| = I$ between each term in (4.86), obtaining

$$\langle y|U_{p(n)} \cdots U_2 U_1|0\rangle = \sum_{x_1,\ldots,x_{p(n)-1}} \langle y|U_{p(n)} \left|x_{p(n)-1}\right\rangle \left\langle x_{p(n)-1}\right| U_{p(n)-2} \ldots U_2 \left|x_1\right\rangle \left\langle x_1\right| U_1|0\rangle. \tag{4.87}$$

Given that the individual unitary gates appearing in this sum are operations such as the Hadamard gate, CNOT, and so on, it is clear that each term in the sum can be calculated to high accuracy using only polynomial space on a classical computer, and thus the sum as a whole can be calculated using polynomial space, since individual terms in the sum can be erased after being added to the running total. Of course, this algorithm is rather slow, since there are exponentially many terms in the sum which need to be calculated and added to the total; however, only polynomially much space is consumed, and thus **BQP** $\subseteq$ **PSPACE**, as we set out to show.

A similar procedure can be used to simulate an arbitrary quantum computation on a classical computer, no matter the length of the quantum computation. Therefore, the class of problems solvable on a quantum computer with unlimited time and space resources is no larger than the class of problems solvable on a classical computer. Stated another way, this means that quantum computers do not violate the Church-Turing thesis that any algorithmic process can be simulated efficiently using a Turing machine. Of course, quantum computers may be much

more efficient than their classical counterparts, thereby challenging the strong Church-Turing thesis that any algorithmic process can be simulated efficiently using a probabilistic Turing machine.

8.1.11 4.6 Summary of the quantum circuit model of computation

In this book the term 'quantum computer' is synonymous with the quantum circuit model of computation. This chapter has provided a detailed look at quantum circuits, their basic elements, universal families of gates, and some applications. Before we move on to more sophisticated applications, let us summarize the key elements of the quantum circuit model of computation:
(1) Classical resources: A quantum computer consists of two parts, a classical part and a quantum part. In principle, there is no need for the classical part of the computer, but in practice certain tasks may be made much easier if parts of the computation can be done classically. For example, many schemes for quantum error-correction (Chapter 10) are likely to involve classical computations in order to maximize efficiency. While classical computations can always be done, in principle, on a quantum computer, it may be more convenient to perform the calculations on a classical computer.
(2) A suitable state space: A quantum circuit operates on some number, n, of qubits. The state space is thus a 2^n-dimensional complex Hilbert space. Product states of the form $|x_1, \ldots, x_n\rangle$, where $x_i = 0, 1$, are known as computational basis states of the computer. $|x\rangle$ denotes a computational basis state, where x is the number whose binary representation is $x_1 \ldots x_n$.
(3) Ability to prepare states in the computational basis: It is assumed that any computational basis state $|x_1, \ldots, x_n\rangle$ can be prepared in at most n steps.
(4) Ability to perform quantum gates: Gates can be applied to any subset of qubits as desired, and a universal family of gates can be implemented. For example, it should be possible to apply the CNOT gate to any pair of qubits in the quantum computer. The Hadamard, phase, cNOT and $\pi/8$ gates form a family of gates from which any unitary operation can be approximated, and thus is a universal set of gates. Other universal families exist.
(5) Ability to perform measurements in the computational basis: Measurements may be performed in the computational basis of one or more of the qubits in the computer.

The quantum circuit model of quantum computation is equivalent to many other models of computation which have been proposed, in the sense that other models result in essentially the same resource requirements for the same problems. As a simple example which illustrates the basic idea, one might wonder whether moving to a design based on three-level quantum systems, rather than the two-level qubits, would confer any computational advantage. Of course, although there may be some slight advantage in using three-level quantum systems (qutrits) over two-level systems, any difference will be essentially negligible from the theoretical point of view. At a less trivial level, the 'quantum Turing machine' model of computation, a quantum generalization of the classical Turing machine model, has been shown to be equivalent to the model based upon quantum circuits. We do not consider that model of computation in this book, but the reader interested in learning more about quantum Turing machines may consult the references given in the end of chapter 'History and further reading'.

Despite the simplicity and attraction of the quantum circuit model, it is useful to keep in mind possible criticisms, modifications, and extensions. For example, it is by no means clear that the basic assumptions underlying the state space and starting conditions in the quantum circuit model are justified. Everything is phrased in terms of finite dimensional state spaces. Might there be anything to be gained by using systems whose state space is infinite dimensional? Assuming that the starting state of the computer is a computational basis state is also not necessary; we know that many systems in Nature 'prefer' to sit in highly entangled states of

many systems; might it be possible to exploit this preference to obtain extra computational power? It might be that having access to certain states allows particular computations to be done much more easily than if we are constrained to start in the computational basis. Likewise, the ability to efficiently perform entangling measurements in multi-qubit bases might be as useful as being able to perform just entangling unitary operations. Indeed, it may be possible to harness such measurements to perform tasks intractable within the quantum circuit model.

A detailed examination and attempted justification of the physics underlying the quantum circuit model is outside the scope of the present discussion, and, indeed, outside the scope of present knowledge! By raising these issues we wish to introduce the question of the completeness of the quantum circuit model, and re-emphasize the fundamental point that information is physical. In our attempts to formulate models for information processing we should always attempt to go back to fundamental physical laws. For the purposes of this book, we shall stay within the quantum circuit model of computation. It offers a rich and powerful model of computation that exploits the properties of quantum mechanics to perform amazing feats of information processing, without classical prece-
dent. Whether physically reasonable models of computation exist which go beyond the quantum circuit model is a fascinating question which we leave open for you.

8.1.12 4.7 Simulation of quantum systems

> Perhaps [...] we need a mathematical theory of quantum automata. [...] the quantum state space has far greater capacity than the classical one: for a classical system with N states, its quantum version allowing superposition accommodates c^N states. When we join two classical systems, their number of states N_1 and N_2 are multiplied, and in the quantum case we get the exponential growth $c^{N_1 N_2}$.[. . .] These crude estimates show that the quantum behavior of the system might be much more complex than its classical simulation.
>
> - Yu Manin (1980)[Man80], as translated in [Man99]

> The quantum-mechanical computation of one molecule of methane requires 10^{42} grid points. Assuming that at each point we have to perform only 10 elementary operations, and that the computation is performed at the extremely low temperature $T = 3 \times 10^{-3} K$, we would still have to use all the energy produced on Earth during the last century.
>
> - R. P. Poplavskii (1975)[Pop75], as quoted by Manin

> Can physics be simulated by a universal computer? [...] the physical world is quantum mechanical, and therefore the proper problem is the simulation of quantum physics [...] the full description of quantum mechanics for a large system with R particles [...] has too many variables, it cannot be simulated with a normal computer with a number of elements proportional to R[. . . but it can be simulated with] quantum computer elements. [...] Can a quantum system be probabilistically simulated by a classical (probabilistic, I'd assume) universal computer? [...] If you take the computer to be the classical kind I've described so far [..] the answer is certainly, No!
>
> - Richard P. Feynman (1982)[Fey82]

Let us close out this chapter by providing an interesting and useful application of the quantum circuit model. One of the most important practical applications of computation is the simulation of physical systems. For example, in the engineering design of a new building, finite element analysis and modeling is used to ensure safety while minimizing cost. Cars are made lightweight, structurally sound, attractive, and inexpensive, by using computer aided design. Modern aeronautical engineering depends heavily on computational fluid dynamics simulations for aircraft designs. Nuclear weapons are no longer exploded (for the most part), but rather, tested by exhaustive computational modeling. Examples abound, because of the tremendous practical applications of predictive simulations. We begin by describing some instances of the simulation problem, then we present a quantum algorithm for simulation and an illustrative example, concluding with some perspective on this application.

8.1.13 4.7.1 Simulation in action

The heart of simulation is the solution of differential equations which capture the physical laws governing the dynamical behavior of a system. Some examples include Newton's law,

$$\frac{d}{dt}\left(m\frac{dx}{dt}\right) = F \tag{4.88}$$

Poisson's equation,

$$-\vec{\nabla}\cdot(k\vec{\nabla}\vec{u}) = \vec{Q}, \tag{4.89}$$

the electromagnetic vector wave equation,

$$\vec{\nabla}\cdot\vec{\nabla}\vec{E} = \epsilon_0\mu_0\frac{\partial^2\vec{E}}{\partial t^2}, \tag{4.90}$$

and the diffusion equation,

$$\vec{\nabla}^2\psi = \frac{1}{a^2}\frac{\partial\psi}{\partial t}, \tag{4.91}$$

just to name a very few. The goal is generally: given an initial state of the system, what is the state at some other time and/or position? Solutions are usually obtained by approximating the state with a digital representation, then discretizing the differential equation in space and time such that an iterative application of a procedure carries the state from the initial to the final conditions. Importantly, the error in this procedure is bounded, and known not to grow faster than some small power of the number of iterations. Furthermore, not all dynamical systems can be simulated efficiently: generally, only those systems which can be described efficiently can be simulated efficiently.

Simulation of quantum systems by classical computers is possible, but generally only very inefficiently. The dynamical behavior of many simple quantum systems is governed by Schrödinger's equation,

$$i\hbar\frac{d}{dt}|\psi\rangle = H|\psi\rangle. \tag{4.92}$$

We will find it convenient to absorb $\hbar$ into H, and use this convention for the rest of this section. For a typical Hamiltonian of interest to physicists dealing with real particles in space (rather than abstract systems such as qubits, which we have been dealing with!), this reduces to

$$i\frac{\partial}{\partial t}\psi(x) = \left[-\frac{1}{2m}\frac{\partial^2}{\partial x^2} + V(x)\right]\psi(x), \tag{4.93}$$

using a convention known as the position representation $\langle x \mid \psi\rangle = \psi(x)$. This is an elliptical equation very much like Equation (4.91). So just simulating Schrödinger's equation is not the especial difficulty faced in simulating quantum systems. What is the difficulty?

The key challenge in simulating quantum systems is the exponential number of differential equations which must be solved. For one qubit evolving according to the Schrödinger equation, a system of two differential equations must be solved; for two qubits, four equations; and for n qubits, 2^n equations. Sometimes, insightful approximations can be made which reduce the effective number of equations involved, thus making classical simulation of the quantum system feasible. However, there are many physically interesting quantum systems for which no such approximations are known.

Exercise 4.46: (Exponential complexity growth of quantum systems) Let ρ be a density matrix describing the state of n qubits. Show that describing ρ requires $4^n - 1$ independent real numbers.

The reader with a physics background may appreciate that there are many important quantum systems for which classical simulation is intractable. These include the Hubbard model, a model of interacting fermionic particles with the Hamiltonian

$$H = \sum_{k=1}^{n} V_0 n_{k\uparrow} n_{k\downarrow} + \sum_{k,j \text{ neighbors, } \sigma} t_0 c^*_{k\sigma} c_{j\sigma}, \tag{4.94}$$

which is useful in the study of superconductivity and magnetism, the Ising model,

$$H = \sum_{k=1}^{n} \vec{\sigma}_k \cdot \vec{\sigma}_{k+1} \tag{4.95}$$

and many others. Solutions to such models give many physical properties such as the dielectric constant, conductivity, and magnetic susceptibility of materials. More sophisticated models such as quantum electrodynamics (QED) and quantum chromodynamics (QCD) can be used to compute constants such as the mass of the proton.

Quantum computers can efficiently simulate quantum systems for which there is no known efficient classical simulation. Intuitively, this is possible for much the same reason any quantum circuit can be constructed from a universal set of quantum gates. Moreover, just as there exist unitary operations which cannot be efficiently approximated, it is possible in principle to imagine quantum systems with Hamiltonians which cannot be efficiently simulated on a quantum computer. Of course, we believe that such systems aren't actually realized in Nature, otherwise we'd be able to exploit them to do information processing beyond the quantum circuit model.

8.1.14 4.7.2 The quantum simulation algorithm

Classical simulation begins with the realization that in solving a simple differential equation such as $dy/dt = f(y)$, to first order, it is known that $y(t + \Delta t) \approx y(t) + f(y)\Delta t$. Similarly, the quantum case is concerned with the solution of $id|\psi\rangle/dt = H|\psi\rangle$, which, for a time-independent H, is just

$$|\psi(t)\rangle = e^{-iHt}|\psi(0)\rangle. \tag{4.96}$$

Since H is usually extremely difficult to exponentiate (it may be sparse, but it is also exponentially large), a good beginning is the first order solution $|\psi(t+\Delta t)\rangle \approx (I - iH\Delta t)|\psi(t)\rangle$.

This is tractable, because for many Hamiltonians H it is straightforward to compose quantum gates to efficiently approximate $I - iH\Delta t$. However, such first order solutions are generally not very satisfactory.

Efficient approximation of the solution to Equation (4.96), to high order, is possible for many classes of Hamiltonian. For example, in most physical systems, the Hamiltonian can be written as a sum over many local interactions. Specifically, for a system of n particles,

$$H = \sum_{k=1}^{L} H_k, \tag{4.97}$$

where each H_k acts on at most a constant c number of systems, and L is a polynomial in n. For example, the terms H_k are often just two-body interactions such as $X_i X_j$ and onebody Hamiltonians such as X_i. Both the Hubbard and Ising models have Hamiltonians of this form. Such locality is quite physically reasonable, and originates in many systems
from the fact that most interactions fall off with increasing distance or difference in energy. There are sometimes additional global symmetry constraints such as particle statistics; we shall come to those shortly. The important point is that although e^{-iHt} is difficult to compute, $e^{-iH_k t}$ acts on a much smaller subsystem, and is straightforward to approximate using quantum circuits. But because $[H_j, H_k] \neq 0$ in general, $e^{-iHt} \neq \prod_k e^{-iH_k t}$! How, then, can $e^{-iH_k t}$ be useful in constructing e^{-iHt} ?

Exercise 4.47: For $H = \sum_k^L H_k$, prove that $e^{-iHt} = e^{-iH_1 t} e^{-iH_2 t} \ldots e^{-iH_L t}$ for all t if $[H_j, H_k] = 0$, for all j, k.

Exercise 4.48: Show that the restriction of H_k to involve at most c particles implies that in the sum (4.97), L is upper bounded by a polynomial in n.

The heart of quantum simulation algorithms is the following asymptotic approximation theorem:

Theorem 4.3: (Trotter formula) Let A and B be Hermitian operators. Then for any real t,

$$\lim_{n \to \infty} \left(e^{iAt/n} e^{iBt/n} \right)^n = e^{i(A+B)t} \tag{4.98}$$

Note that (4.98) is true even if A and B do not commute. Even more interestingly, perhaps, it can be generalized to hold for A and B which are generators of certain kinds of semigroups, which correspond to general quantum operations; we shall describe such generators (the 'Lindblad form') in Section 8.4.1 of Chapter 8. For now, we only consider the case of A and B being Hermitian matrices.

Proof

By definition,

$$e^{iAt/n} = I + \frac{1}{n} iAt + O\left(\frac{1}{n^2}\right), \tag{4.99}$$

and thus

$$e^{iAt/n} e^{iBt/n} = I + \frac{1}{n} i(A+B)t + O\left(\frac{1}{n^2}\right). \tag{4.100}$$

Taking products of these gives us

$$\left(e^{iAt/n} e^{iBt/n} \right)^n = I + \sum_{k=1}^{n} \binom{n}{k} \frac{1}{n^k} [i(A+B)t]^k + O\left(\frac{1}{n}\right), \tag{4.101}$$

and since $\binom{n}{k} \frac{1}{n^k} = \left(1 + O\left(\frac{1}{n}\right)\right)/k!$, this gives

$$\lim_{n\to\infty}\left(e^{iAt/n}e^{iBt/n}\right)^n = \lim_{n\to\infty}\sum_{k=0}^{n}\frac{(i(A+B)t)^k}{k!}\left(1+O\left(\frac{1}{n}\right)\right)+O\left(\frac{1}{n}\right) = e^{i(A+B)t}. \quad (4.102)$$

Modifications of the Trotter formula provide the methods by which higher order approximations can be derived for performing quantum simulations. For example, using similar reasoning to the proof above, it can be shown that

$$e^{i(A+B)\Delta t} = e^{iA\Delta t}e^{iB\Delta t} + O\left(\Delta t^2\right) \quad (4.103)$$

Similarly,

$$e^{i(A+B)\Delta t} = e^{iA\Delta t/2}e^{iB\Delta t}e^{iA\Delta t/2} + O\left(\Delta t^3\right) \quad (4.104)$$

An overview of the quantum simulation algorithm is given below, and an explicit example of simulating the one-dimensional non-relativistic Schrödinger equation is shown in Box 4.2.

Algorithm: Quantum simulation

Inputs: (1) A Hamiltonian $H = \sum_k H_k$ acting on an N-dimensional system, where each H_k acts on a small subsystem of size independent of N, (2) an initial state $|\psi_0\rangle$, of the system at $t = 0$, (3) a positive, non-zero accuracy δ, and (3) a time t_f at which the evolved state is desired.

Outputs: A state $\left|\tilde{\psi}\left(t_f\right)\right\rangle$ such that $\left|\left\langle\tilde{\psi}\left(t_f\right)\right| e^{-iHt_f}\left|\psi_0\right\rangle\right|^2 \geq 1-\delta$.

Runtime: $O(\text{poly}(1/\delta))$ operations.

Procedure: Choose a representation such that the state $|\tilde{\psi}\rangle$ of $n = \text{poly}(\log N)$ qubits approximates the system and the operators $e^{-iH_k\Delta t}$ have efficient quantum circuit approximations. Select an approximation method (see for example Equations (4.103)-(4.105)) and Δt such that the expected error is acceptable (and $j\Delta t = t_f$ for an integer j), construct the corresponding quantum circuit $U_{\Delta t}$ for the iterative step, and do:

1.	$\left\|\tilde{\psi}_0\right\rangle \leftarrow \left\|\psi_0\right\rangle; j = 0$	initialize state
2.	$\rightarrow \left\|\tilde{\psi}_{j+1}\right\rangle = U_{\Delta t}\left\|\tilde{\psi}_j\right\rangle$	iterative update
3.	$\rightarrow j = j+1$; goto 2 until $j\Delta t \geq t_f$	loop
4.	$\rightarrow \left\|\tilde{\psi}\left(t_f\right)\right\rangle = \left\|\tilde{\psi}_j\right\rangle$	final result

Exercise 4.49: (Baker-Campbell-Hausdorf formula) Prove that

$$e^{(A+B)\Delta t} = e^{A\Delta t}e^{B\Delta t}e^{-\frac{1}{2}[A,B]\Delta t^2} + O\left(\Delta t^3\right) \quad (4.105)$$

and also prove Equations (4.103) and (4.104).

Exercise 4.50: Let $H = \sum_k^L H_k$, and define

$$U_{\Delta t} = \left[e^{-iH_1\Delta t}e^{-iH_2\Delta t}\ldots e^{-iH_L\Delta t}\right]\left[e^{-iH_L\Delta t}e^{-iH_{L-1}\Delta t}\ldots e^{-iH_1\Delta t}\right] \quad (4.106)$$

(a) Prove that $U_{\Delta t} = e^{-2iH\Delta t} + O\left(\Delta t^3\right)$.

(b) Use the results in Box 4.1 to prove that for a positive integer m,

$$E\left(U_{\Delta t}^m, e^{-2miH\Delta t}\right) \leq m\alpha\Delta t^3, \quad (4.107)$$

for some constant α.

Box 4.2: Quantum simulation of Schrödinger's equation

The methods and limitations of quantum simulation may be illustrated by the following example, drawn from the conventional models studied by physicists, rather than the abstract qubit model. Consider a single particle living on a line, in a onedimensional potential $V(x)$, governed by the Hamiltonian

$$H = \frac{p^2}{2m} + V(x), \tag{4.108}$$

where p is the momentum operator and x is the position operator. The eigenvalues of x are continuous, and the system state $|\psi\rangle$ resides in an infinite dimensional Hilbert space; in the x basis, it can be written as

$$|\psi\rangle = \int_{-\infty}^{\infty} |x\rangle\langle x \mid \psi\rangle dx \tag{4.109}$$

In practice, only some finite region is of interest, which we may take to be the range $-d \leq x \leq d$. Furthermore, it is possible to choose a differential step size Δx sufficiently small compared to the shortest wavelength in the system such that

$$|\tilde{\psi}\rangle = \sum_{k=-d/\Delta x}^{d/\Delta x} a_k |k\Delta x\rangle \tag{4.110}$$

provides a good physical approximation of $|\psi\rangle$. This state can be represented using $n = \lceil \log(2d/\Delta x + 1) \rceil$ qubits; we simply replace the basis $|k\Delta x\rangle$ (an eigenstate of the x operator) with $|k\rangle$, a computational basis state of n qubits. Note that only n qubits are required for this simulation, whereas classically 2^n complex numbers would have to be kept track of, thus leading to an exponential resource saving when performing the simulation on a quantum computer. Computation of $|\tilde{\psi}(t)\rangle = e^{-iHt}|\tilde{\psi}(0)\rangle$ must utilize one of the approximations of Equations (4.103)-(4.105) because in general $H_1 = V(x)$ does not commute with $H_0 = p^2/2m$. Thus, we must be able to compute $e^{-iH_1\Delta t}$ and $e^{-iH_0\Delta t}$. Because $|\tilde{\psi}\rangle$ is expressed in the eigenbasis of H_1, $e^{-iH_1\Delta t}$ is a diagonal transformation of the form

$$|k\rangle \rightarrow e^{-iV(k\Delta x)\Delta t}|k\rangle. \tag{4.111}$$

It is straightforward to compute this, since we can compute $V(k\Delta x)\Delta t$. (See also Problem 4.1.) The second term is also simple, because x and p are conjugate variables related by a quantum Fourier transform $U_{\text{FFT}} x U_{\text{FFT}}^\dagger = p$, and thus $e^{-iH_0\Delta t} = U_{\text{FFT}} e^{-ix^2\Delta t/2m} U_{\text{FFT}}^\dagger$; to compute $e^{-iH_0\Delta t}$, do

$$|k\rangle \rightarrow U_{\text{FFT}} e^{-ix^2/2m} U_{\text{FFT}}^\dagger |k\rangle. \tag{4.112}$$

The construction of U_{FFT} is discussed in Chapter 5.

8.1.15 4.7.3 An illustrative example

The procedure we have described for quantum simulations has concentrated on simulating Hamiltonians which are sums of local interations. However, this is not a fundamental requirement! As the following example illustrates, efficient quantum simulations are possible even for Hamiltonians which act non-trivially on all or nearly all parts of a large system.

Suppose we have the Hamiltonian

$$H = Z_1 \otimes Z_2 \otimes \cdots \otimes Z_n, \tag{4.113}$$

which acts on an n qubit system. Despite this being an interaction involving all of the system, indeed, it can be simulated efficiently. What we desire is a simple quantum circuit which implements $e^{-iH\Delta t}$, for arbitrary values of Δt. A circuit doing precisely this, for $n = 3$, is shown in Figure 4.19. The main insight is that although the Hamiltonian involves all the qubits in the system, it does so in a classical manner: the phase shift applied to the system is $e^{-i\Delta t}$ if the parity of the n qubits in the computational basis is even; otherwise, the phase shift should be $e^{i\Delta t}$. Thus, simple simulation of H is possible by first classically computing the parity (storing the result in an ancilla qubit), then applying the appropriate phase shift conditioned on the parity, then uncomputing the parity (to erase the ancilla). This strategy clearly works not only for $n = 3$, but also for arbitrary values of n.

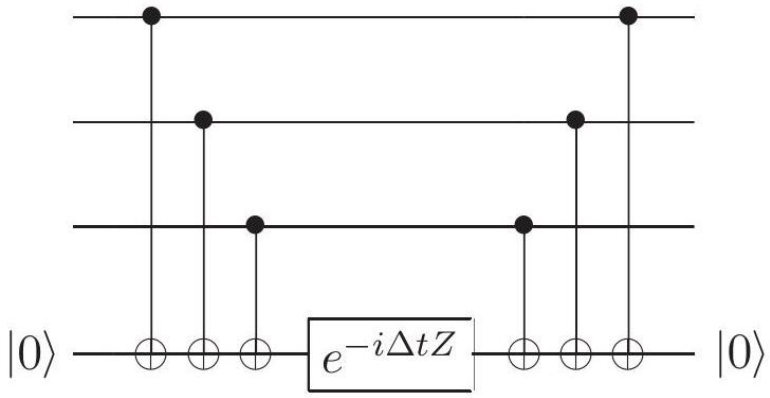


Figure 4.19. Quantum circuit for simulating the Hamiltonian $H=Z_{1 \otimes Z_{2} \otimes Z_{3}$ for time Δt.}

Furthermore, extending the same procedure allows us to simulate more complicated extended Hamiltonians. Specifically, we can efficiently simulate any Hamiltonian of the form

$$H = \bigotimes_{k=1}^{n} \sigma_{c(k)}^{k} \tag{4.114}$$

where $\sigma_{c(k)}^{k}$ is a Pauli matrix (or the identity) acting on the k th qubit, with $c(k) \in \{0, 1, 2, 3\}$ specifying one of $\{I, X, Y, Z\}$. The qubits upon which the identity operation is performed can be disregarded, and X or Y terms can be transformed by single qubit gates to Z operations. This leaves us with a Hamiltonian of the form of (4.113), which is simulated as described above.

Exercise 4.51: Construct a quantum circuit to simulate the Hamiltonian

$$H = X_1 \otimes Y_2 \otimes Z_3, \tag{4.115}$$

performing the unitary transform $e^{-i\Delta t H}$ for any Δt.

Using this procedure allows us to simulate a wide class of Hamiltonians containing terms which are not local. In particular, it is possible to simulate a Hamiltonian of the form $H = \sum_{k=1}^{L} H_k$ where the only restriction is that the individual H_k have a tensor product structure, and that L is polynomial in the total number of particles n. More generally, all that is required is that there be an efficient circuit to simulate each H_k separately. As an example, the Hamiltonian $H = \sum_{k=1}^{n} X_k + Z^{\otimes n}$ can easily be simulated using the above techniques. Such Hamiltonians typically do not arise in Nature. However, they provide a new and possibly valuable vista on the world of quantum algorithms.

8.1.16 4.7.4 Perspectives on quantum simulation

The quantum simulation algorithm is very similar to classical methods, but also differs in a fundamental way. Each iteration of the quantum algorithm must completely replace the old state with the new one; there is no way to obtain (non-trivial) information from an intermediate step without significantly changing the algorithm, because the state is a quantum one. Furthermore, the final measurement must be chosen cleverly to provide the desired result, because it disturbs the quantum state. Of course, the quantum simulation can be repeated to obtain statistics, but it is desirable to repeat the algorithm only at most a polynomial number of times. It may be that even though the simulation can be performed efficiently, there is no way to efficiently perform a desired measurement.

Also, there are Hamiltonians which simply can't be simulated efficiently. In Section 4.5.4, we saw that there exist unitary transformations which quantum computers cannot efficiently approximate. As a corollary, not all Hamiltonian evolutions can be efficiently simulated on a quantum computer, for if this were possible, then all unitary transformations could be efficiently approximated!

Another difficult problem - one which is very interesting - is the simulation of equilibration processes. A system with Hamiltonian H in contact with an environment at temperature T will generally come to thermal equilibrium in a state known as the Gibbs state, $\rho_{\text{therm}} = e^{-H/k_{\text{B}}T}/\mathcal{Z}$, where k_{B} is Boltzmann's constant, and $\mathcal{Z} = \operatorname{tr} e^{-H/k_{\text{B}}T}$ is the usual partition function normalization, which ensures that $\operatorname{tr}(\rho) = 1$. The process by which this equilibration occurs is not very well understood, although certain requirements are known: the environment must be large, it must have non-zero population in states with energies matching the eigenstates of H, and its coupling with the system should be weak. Obtaining ρ_{therm} for arbitrary H and T is generally an exponentially difficult problem for a classical computer. Might a quantum computer be able to solve this efficiently? We do not yet know.

On the other hand, as we discussed above many interesting quantum problems can indeed be simulated efficiently with a quantum computer, even when they have extra constraints beyond the simple algorithms presented here. A particular class of these involve global symmetries originating from particle statistics. In the everyday world, we are used to being able to identify different particles; tennis balls can be followed around a tennis court, keeping track of which is which. This ability to keep track of which object is which is a general feature of classical objects - by continuously measuring the position of a classical particle it can be tracked at all times, and thus uniquely distinguished from other particles. However, this breaks down in quantum mechanics, which prevents us from following the motion of individual particles exactly. If the two particles are inherently different, say a proton and an electron, then we can distinguish them by measuring the sign of the charge to tell which particle is which. But in the case of identical particles, like two electrons, it is found that they are truly indistinguishable.

Indistinguishability of particles places a constraint on the state vector of a system which manifests itself in two ways. Experimentally, particles in Nature are found to come in two distinct flavors, known as bosons and fermions. The state vector of a system of bosons remains unchanged under permutation of any two constituents, reflecting their fundamental indistinguishability. Systems of fermions, in contrast, experience a sign change in their state vector under interchange of any two constituents. Both kinds of systems can be simulated efficiently on a quantum computer. The detailed description of how this is done is outside the scope of this book; suffice it to say the procedure is fairly straightforward. Given an initial state of the wrong symmetry, it can be properly symmetrized before the simulation begins. And the operators used in the simulation can be constructed to respect the desired symmetry, even allowing for the effects of higher order error terms. The reader who is interested in pursuing this and other topics further will find pointers to the literature in 'History and further reading,' at the end of the chapter.

Problem 4.1: (Computable phase shifts) Let m and n be positive integers. Suppose $f : \{0, \ldots, 2^m - 1\} \rightarrow \{0, \ldots, 2^n - 1\}$ is a classical function from m to n bits which may be computed reversibly using T Toffoli gates, as described in Section 3.2.5. That is, the function $(x, y) \rightarrow (x, y \oplus f(x))$ may be implemented using T Toffoli gates. Give a quantum circuit using $2T + n$ (or fewer) one, two, and three qubit gates to implement the unitary operation defined by

$$|x\rangle \rightarrow \exp\left(\frac{-2i\pi f(x)}{2^n}\right)|x\rangle. \tag{4.116}$$

Problem 4.2: Find a depth $O(\log n)$ construction for the $C^n(X)$ gate. (Comment: The depth of a circuit is the number of distinct timesteps at which gates are applied; the point of this problem is that it is possible to parallelize the $C^n(X)$ construction by applying many gates in parallel during the same timestep.)

Problem 4.3: (Alternate universality construction) Suppose U is a unitary matrix on n qubits. Define $H \equiv i \ln(U)$. Show that
(1) H is Hermitian, with eigenvalues in the range 0 to 2π.
(2) H can be written

$$H = \sum_g h_g g \tag{4.117}$$

where h_g are real numbers and the sum is over all n-fold tensor products g of the Pauli matrices $\{I, X, Y, Z\}$.
(3) Let $\Delta = 1/k$, for some positive integer k. Explain how the unitary operation $\exp(-ih_g g\Delta)$ may be implemented using $O(n)$ one and two qubit operations.
(4) Show that

$$\exp(-iH\Delta) = \prod_g \exp(-ih_g g\Delta) + O\left(4^n \Delta^2\right) \tag{4.118}$$

where the product is taken with respect to any fixed ordering of the n-fold tensor products of Pauli matrices, g.
(5) Show that

$$U = \left[\prod_g \exp(-ih_g g\Delta)\right]^k + O\left(4^n \Delta\right). \tag{4.119}$$

(6) Explain how to approximate U to within a distance $\epsilon > 0$ using $O\left(n16^n/\epsilon\right)$ one and two qubit unitary operations.

Problem 4.4: (Minimal Toffoli construction) (Research)

(1) What is the smallest number of two qubit gates that can be used to implement the Toffoli gate?
(2) What is the smallest number of one qubit gates and cNOT gates that can be used to implement the Toffoli gate?
(3) What is the smallest number of one qubit gates and controlled- Z gates that can be used to implement the Toffoli gate?

Problem 4.5: (Research) Construct a family of Hamiltonians, $\{H_n\}$, on n qubits, such that simulating H_n requires a number of operations super-polynomial in n.
(Comment: This problem seems to be quite difficult.)
Problem 4.6: (Universality with prior entanglement) Controlled-NOT gates and single qubit

gates form a universal set of quantum logic gates. Show that an alternative universal set of resources is comprised of single qubit unitaries, the ability to perform measurements of pairs of qubits in the Bell basis, and the ability to prepare arbitrary four qubit entangled states.

8.1.17 Summary of Chapter 4: Quantum circuits

- Universality: Any unitary operation on n qubits may be implemented exactly by composing single qubit and controlled-not gates.
- Universality with a discrete set: The Hadamard gate, phase gate, controllednot gate, and $\pi/8$ gate are universal for quantum computation, in the sense that an arbitrary unitary operation on n qubits can be approximated to an arbitrary accuracy $\epsilon > 0$ using a circuit composed of only these gates. Replacing the $\pi/8$ gate in this list with the Toffoli gate also gives a universal family.
- Not all unitary operations can be efficiently implemented: There are unitary operations on n qubits which require $\Omega\left(2^n \log(1/\epsilon)/\log(n)\right)$ gates to approximate to within a distance ϵ using any finite set of gates.
- Simulation: For a Hamiltonian $H = \sum_k H_k$ which is a sum of polynomially many terms H_k such that efficient quantum circuits for H_k can be constructed, a quantum computer can efficiently simulate the evolution e^{-iHt} and approximate $|\psi(t)\rangle = e^{-iHt}|\psi(0)\rangle$, given $|\psi(0)\rangle$.

History and further reading

The gate constructions in this chapter are drawn from a wide variety of sources. The paper by Barenco, Bennett, Cleve, DiVincenzo, Margolus, Shor, Sleator, Smolin, and Weinfurter [BBC+95] was the source of many of the circuit constructions in this chapter, and for the universality proof for single qubit and controlled-not gates. Another useful source of insights about quantum circuits is the paper by Beckman, Chari, Devabhaktuni, and Preskill[BCDP96]. A gentle and accessible introduction has been provided by DiVincenzo [DiV98]. The fact that measurements commute with control qubit terminals was pointed out by Griffiths and Niu [GN96] .

The universality proof for two-level unitaries is due to Reck, Zeilinger, Bernstein, and Bertani [RZBB94]. The universality of the controlled-not and single qubit gates was proved by DiVincenzo [DiV5 b]. The universal gate G in Exercise 4.44 is sometimes known as the Deutsch gate [Deu89]. Deutsch, Barenco, and Ekert [DBE95] and Lloyd [Llo95] independently proved that almost any two qubit quantum logic gate is universal. That errors caused by sequences of gates is at most the sum of the errors of the individual gates was proven by Bernstein and Vazirani [BV97] . The specific universal set of gates we have focused on - the Hadamard, phase, controllednot and $\pi/8$ gates, was proved universal in Boykin, Mor, Pulver, Roychowdhury, and Vatan [BMP +99, which also contains a proof that θ defined by $\cos(\theta/2) \equiv \cos^2(\pi/8)$ is an irrational multiple of π. The bound in Section 4.5.4 is based on a paper by Knill [Kni95], which does a much more detailed investigation of the hardness of approximating arbitrary unitary operations using quantum circuits. In particular, Knill obtains tighter and more general bounds than we do, and his analysis applies also to cases where the universal set is a continuum of gates, not just a finite set, as we have considered.

The quantum circuit model of computation is due to Deutsch [Deu89], and was further developed by Yao[Yao93]. The latter paper showed that the quantum circuit model of computation is equivalent to the quantum Turing machine model. Quantum Turing machines were introduced in 1980 by Benioff[Ben80], further developed by Deutsch[Deu85] and Yao[Yao93], and their modern definition given by Bernstein and Vazirani [BV97]. The latter two papers also take

first steps towards setting up a theory of quantum computational complexity, analogous to classical computational complexity theory. In particular, the inclusion BQP $\subseteq$ PSPACE and some slightly stronger results was proved by Bernstein and Vazirani. Knill and Laflamme[KL99] develop some fascinating connections between quantum and classical computational complexity. Other interesting work on quantum computational complexity includes the paper by Adleman, Demarrais and Huang [ADH97] , and the paper by Watrous [Wat99]. The latter paper gives intriguing evidence to suggest that quantum computers are more powerful than classical computers in the setting of 'interactive proof systems'.

The suggestion that non-computational basis starting states may be used to obtain computational power beyond the quantum circuits model was made by Daniel Gottesman and Michael Nielson.

That quantum computers might simulate quantum systems more efficiently than classical computers was intimated by Manin [Man80] in 1980, and independently developed in more detail by Feynman [Fey82] in 1982. Much more detailed investigations were subsequently carried out by Abrams and Lloyd[AL97], Boghosian and Taylor [BT97], Sornborger and Stewart [SS99], Wiesner [Wie96], and Zalka[Zal98]. The Trotter formula is attributed to Trotter [Tro59], and was also proven by Chernoff [Che68], although the simpler form for
unitary operators is much older, and goes back to the time of Sophus Lie. The third order version of the Baker-Campbell-Hausdorff formula, Equation (4.104), was given by Sornborger and Stewart [SS99]. Abrams and Lloyd [AL97] give a procedure for simulating many-body Fermi systems on a quantum computer. Terhal and DiVincenzo address the problem of simulating the equilibration of quantum systems to the Gibbs state [TD98]. The method used to simulate the Schrödinger equation in Box 4.2 is due to Zalka [Zal98] and Wiesner [Wie96].

Exercise 4.25 is due to Vandersypen, and is related to work by Chau and Wilczek [$CW95$]. Exercise 4.45 is due to Boykin, Mor, Pulver, Roychowdhury, and Vatan [$BMP^{+}99$]. Problem 4.2 is due to Gottesman. Problem 4.6 is due to Gottesman and Chuang [GC99].

8.2 5 The quantum Fourier transform and its applications

The most spectacular discovery in quantum computing to date is that quantum computers can efficiently perform some tasks which are not feasible on a classical computer. For example, finding the prime factorization of an n-bit integer is thought to require $\exp\left(\Theta\left(n^{1/3}\log^{2/3} n\right)\right)$ operations using the best classical algorithm known at the time of writing, the so-called number field sieve. This is exponential in the size of the number being factored, so factoring is generally considered to be an intractable problem on a classical computer: it quickly becomes impossible to factor even modest numbers. In contrast, a quantum algorithm can accomplish the same task using $O\left(n^2 \log n \log\log n\right)$ operations. That is, a quantum computer can factor a number exponentially faster than the best known classical algorithms. This result is important in its own right, but perhaps the most exciting aspect is the question it raises: what other problems can be done efficiently on a quantum computer which are infeasible on a classical computer?

In this chapter we develop the quantum Fourier transform, which is the key ingredient for quantum factoring and many other interesting quantum algorithms. The quantum Fourier transform, with which we begin in Section 5.1, is an efficient quantum algorithm for performing a Fourier transform of quantum mechanical amplitudes. It does not speed up the classical task of computing Fourier transforms of classical data. But one important task which it does enable is phase estimation, the approximation of the eigenvalues of a unitary operator under certain circumstances, as described in Section 5.2. This allows us to solve several other interesting problems, including the order-finding problem and the factoring problem, which are covered in Section 5.3. Phase estimation can also be combined with the quantum search algorithm to solve the problem of counting solutions to a search problem, as described in the next chapter.

Section 5.4 concludes the chapter with a discussion of how the quantum Fourier transform may be used to solve the hidden
subgroup problem, a generalization of the phase estimation and order-finding problems that has among its special cases an efficient quantum algorithm for the discrete logarithm problem, another problem thought to be intractable on a classical computer.

8.2.1 5.1 The quantum Fourier transform

> A good idea has a way of becoming simpler and solving problems other than that for which it was intended.
>
> - Robert Tarjan

One of the most useful ways of solving a problem in mathematics or computer science is to transform it into some other problem for which a solution is known. There are a few transformations of this type which appear so often and in so many different contexts that the transformations are studied for their own sake. A great discovery of quantum computation has been that some such transformations can be computed much faster on a quantum computer than on a classical computer, a discovery which has enabled the construction of fast algorithms for quantum computers.

One such transformation is the discrete Fourier transform. In the usual mathematical notation, the discrete Fourier transform takes as input a vector of complex numbers, $x_0, \ldots, x_{N-1}$ where the length N of the vector is a fixed parameter. It outputs the transformed data, a vector of complex numbers $y_0, \ldots, y_{N-1}$, defined by

$$y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi i j k/N} \tag{5.1}$$

The quantum Fourier transform is exactly the same transformation, although the conventional notation for the quantum Fourier transform is somewhat different. The quantum Fourier transform on an orthonormal basis $|0\rangle, \ldots, |N-1\rangle$ is defined to be a linear operator with the following action on the basis states,

$$|j\rangle \longrightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i j k/N} |k\rangle \tag{5.2}$$

Equivalently, the action on an arbitrary state may be written

$$\sum_{j=0}^{N-1} x_j |j\rangle \longrightarrow \sum_{k=0}^{N-1} y_k |k\rangle \tag{5.3}$$

where the amplitudes y_k are the discrete Fourier transform of the amplitudes x_j. It is not obvious from the definition, but this transformation is a unitary transformation, and thus can be implemented as the dynamics for a quantum computer. We shall demonstrate the unitarity of the Fourier transform by constructing a manifestly unitary quantum circuit computing the Fourier transform. It is also easy to prove directly that the Fourier transform is unitary:

Exercise 5.1: Give a direct proof that the linear transformation defined by Equation (5.2) is unitary.

Exercise 5.2: Explicitly compute the Fourier transform of the n qubit state $|00\ldots0\rangle$.

In the following, we take $N = 2^n$, where n is some integer, and the basis $|0\rangle, \ldots, |\,2^n - 1\rangle$ is the computational basis for an n qubit quantum computer. It is helpful to write the state

$|j\rangle$ using the binary representation $j = j_1 j_2 \ldots j_n$. More formally, $j = j_1 2^{n-1} + j_2 2^{n-2} + \ldots + j_n 2^0$. It is also convenient to adopt the notation $0.j_l j_{l+1} \ldots j_m$ to represent the binary fraction $j_l/2 + j_{l+1}/4 + \cdots + j_m/2^{m-l+1}$.

With a little algebra the quantum Fourier transform can be given the following useful product representation:

$$|j_1, \ldots, j_n\rangle \rightarrow \frac{\left(|0\rangle + e^{2\pi i 0.j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle\right)\cdots\left(|0\rangle + e^{2\pi i 0.j_1 j_2 \cdots j_n}|1\rangle\right)}{2^{n/2}} \tag{5.4}$$

This product representation is so useful that you may even wish to consider this to be the definition of the quantum Fourier transform. As we explain shortly this representation allows us to construct an efficient quantum circuit computing the Fourier transform, a proof that the quantum Fourier transform is unitary, and provides insight into algorithms based upon the quantum Fourier transform. As an incidental bonus we obtain the classical fast Fourier transform, in the exercises!

The equivalence of the product representation (5.4) and the definition (5.2) follows from some elementary algebra:

$$|j\rangle \rightarrow \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{2\pi i j k/2^n} |k\rangle \tag{5.5}$$

$$= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} e^{2\pi i j \left(\sum_{l=1}^{n} k_l 2^{-l}\right)} |k_1 \ldots k_n\rangle \tag{5.6}$$

$$= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} \bigotimes_{l=1}^{n} e^{2\pi i j k_l 2^{-l}} |k_l\rangle \tag{5.7}$$

$$= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left[\sum_{k_l=0}^{1} e^{2\pi i j k_l 2^{-l}} |k_l\rangle\right] \tag{5.8}$$

$$= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left[|0\rangle + e^{2\pi i j 2^{-l}}|1\rangle\right] \tag{5.9}$$

$$= \frac{\left(|0\rangle + e^{2\pi i 0.j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle\right)\cdots\left(|0\rangle + e^{2\pi i 0.j_1 j_2 \cdots j_n}|1\rangle\right)}{2^{n/2}}. \tag{5.10}$$

The product representation (5.4) makes it easy to derive an efficient circuit for the quantum Fourier transform. Such a circuit is shown in Figure 5.1. The gate R_k denotes the unitary transformation

$$R_k \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix} \tag{5.11}$$

To see that the pictured circuit computes the quantum Fourier transform, consider what happens when the state $|j_1 \ldots j_n\rangle$ is input. Applying the Hadamard gate to the first bit produces the state

$$\frac{1}{2^{1/2}}\left(|0\rangle + e^{2\pi i 0.j_1}|1\rangle\right)|j_2 \ldots j_n\rangle \tag{5.12}$$

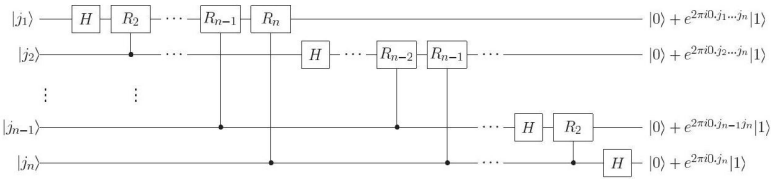


Figure 5.1. Efficient circuit for the quantum Fourier transform. This circuit is easily derived from the product representation (5.4) for the quantum Fourier transform. Not shown are swap gates at the end of the circuit which reverse the order of the qubits, or normalization factors of \$1 / \sqrt{2

\$ in the output.}

since $e^{2\pi i 0.j_1} = -1$ when $j_1 = 1$, and is $+1$ otherwise. Applying the controlled- R_2 gate produces the state

$$\frac{1}{2^{1/2}} \left(|0\rangle + e^{2\pi i 0.j_1 j_2}|1\rangle\right) |j_2 \ldots j_n\rangle \,. \tag{5.13}$$

We continue applying the controlled- R_3, R_4 through R_n gates, each of which adds an extra bit to the phase of the co-efficient of the first $|1\rangle$. At the end of this procedure we have the state

$$\frac{1}{2^{1/2}} \left(|0\rangle + e^{2\pi i 0.j_1 j_2 \ldots j_n}|1\rangle\right) |j_2 \ldots j_n\rangle \,. \tag{5.14}$$

Next, we perform a similar procedure on the second qubit. The Hadamard gate puts us in the state

$$\frac{1}{2^{2/2}} \left(|0\rangle + e^{2\pi i 0.j_1 j_2 \ldots j_n}|1\rangle\right) \left(|0\rangle + e^{2\pi i 0.j_2}|1\rangle\right) |j_3 \ldots j_n\rangle \,, \tag{5.15}$$

and the controlled- R_2 through R_{n-1} gates yield the state

$$\frac{1}{2^{2/2}} \left(|0\rangle + e^{2\pi i 0.j_1 j_2 \ldots j_n}|1\rangle\right) \left(|0\rangle + e^{2\pi i 0.j_2 \ldots j_n}|1\rangle\right) |j_3 \ldots j_n\rangle \,. \tag{5.16}$$

We continue in this fashion for each qubit, giving a final state

$$\frac{1}{2^{n/2}} \left(|0\rangle + e^{2\pi i 0.j_1 j_2 \ldots j_n}|1\rangle\right) \left(|0\rangle + e^{2\pi i 0.j_2 \ldots j_n}|1\rangle\right) \ldots \left(|0\rangle + e^{2\pi i 0.j_n}|1\rangle\right) . \tag{5.17}$$

Swap operations (see Section 1.3.4 for a description of the circuit), omitted from Figure 5.1 for clarity, are then used to reverse the order of the qubits. After the swap operations, the state of the qubits is

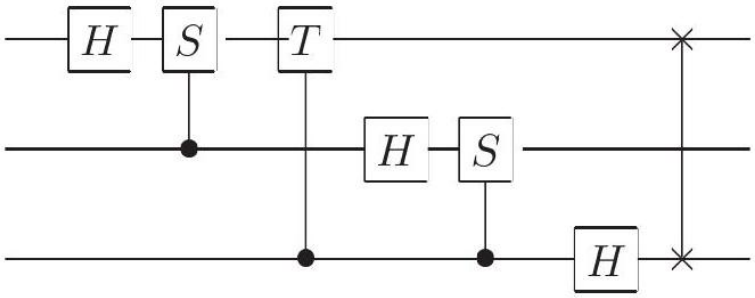
$$\frac{1}{2^{n/2}} \left(|0\rangle + e^{2\pi i 0.j_n}|1\rangle\right) \left(|0\rangle + e^{2\pi i 0.j_{n-1} j_n}|1\rangle\right) \ldots \left(|0\rangle + e^{2\pi i 0.j_1 j_2 \cdots j_n}|1\rangle\right) . \tag{5.18}$$

Comparing with Equation (5.4) we see that this is the desired output from the quantum Fourier transform. This construction also proves that the quantum Fourier transform is unitary, since each gate in the circuit is unitary. An explicit example showing a circuit for the quantum Fourier transform on three qubits is given in Box 5.1.

How many gates does this circuit use? We start by doing a Hadamard gate and $n-1$ conditional rotations on the first qubit - a total of n gates. This is followed by a Hadamard gate and $n-2$ conditional rotations on the second qubit, for a total of $n + (n-1)$ gates. Continuing in this way, we see that $n + (n-1) + \cdots + 1 = n(n+1)/2$ gates are required,

Box 5.1: Three qubit quantum Fourier transform

For concreteness it may help to look at the explicit circuit for the three qubit quantum Fourier transform:



Recall that S and T are the phase and $\pi/8$ gates (see page xxiii). As a matrix the quantum Fourier transform in this instance may be written out explicitly, using $\omega = e^{2\pi i/8} = \sqrt{i}$, as

$$\frac{1}{\sqrt{8}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^1 & \omega^4 & \omega^7 & \omega^2 & \omega^5 \\ 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 \\ 1 & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega^1 & \omega^6 & \omega^3 \\ 1 & \omega^6 & \omega^4 & \omega^2 & 1 & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega^1 \end{bmatrix}. \tag{5.19}$$

plus the gates involved in the swaps. At most $n/2$ swaps are required, and each swap can be accomplished using three controlled-not gates. Therefore, this circuit provides a $\Theta(n^2)$ algorithm for performing the quantum Fourier transform.

In contrast, the best classical algorithms for computing the discrete Fourier transform on 2^n elements are algorithms such as the Fast Fourier Transform (FFT), which compute the discrete Fourier transform using $\Theta(n2^n)$ gates. That is, it requires exponentially more operations to compute the Fourier transform on a classical computer than it does to implement the quantum Fourier transform on a quantum computer.

At face value this sounds terrific, since the Fourier transform is a crucial step in so many real-world data processing applications. For example, in computer speech recognition, the first step in phoneme recognition is to Fourier transform the digitized sound. Can we use the quantum Fourier transform to speed up the computation of these Fourier transforms? Unfortunately, the answer is that there is no known way to do this. The problem is that the amplitudes in a quantum computer cannot be directly accessed by measurement. Thus, there is no way of determining the Fourier transformed amplitudes of the original state. Worse still, there is in general no way to efficiently prepare the original state to be Fourier transformed. Thus, finding uses for the quantum Fourier transform is more subtle than we might have hoped. In this and the next chapter we develop several algorithms based upon a more subtle application of the quantum Fourier transform.

Exercise 5.3: (Classical fast Fourier transform) Suppose we wish to perform a Fourier transform of a vector containing 2^n complex numbers on a classical computer. Verify that the straightforward method for performing the Fourier transform, based upon direct evaluation of Equation (5.1) requires $\Theta(2^{2n})$ elementary arithmetic operations. Find a method for reducing this to $\Theta(n2^n)$ operations, based upon Equation (5.4).

Exercise 5.4: Give a decomposition of the controlled- R_k gate into single qubit and cNOT gates.

Exercise 5.5: Give a quantum circuit to perform the inverse quantum Fourier transform.

Exercise 5.6: (Approximate quantum Fourier transform) The quantum circuit construction of the quantum Fourier transform apparently requires gates of exponential precision in the number of qubits used. However, such precision is never required in any quantum circuit of polynomial size. For example, let U be the ideal quantum Fourier transform on n qubits, and V be the transform which results if the controlled- R_k gates are performed to a precision $\Delta = 1/p(n)$ for some polynomial $p(n)$. Show that the error $E(U,V) \equiv \max_{|\psi\rangle} \|(U-V)|\psi\rangle\|$ scales as $\Theta\left(n^2/p(n)\right)$, and thus polynomial precision in each gate is sufficient to guarantee polynomial accuracy in the output state.

8.2.2 5.2 Phase estimation

The Fourier transform is the key to a general procedure known as phase estimation, which in turn is the key for many quantum algorithms. Suppose a unitary operator U has an eigenvector $|u\rangle$ with eigenvalue $e^{2\pi i\varphi}$, where the value of φ is unknown. The goal of the phase estimation algorithm is to estimate φ. To perform the estimation we assume that we have available black boxes (sometimes known as oracles) capable of preparing the state $|u\rangle$ and performing the controlled- U^{2^j} operation, for suitable non-negative integers j. The use of black boxes indicates that the phase estimation procedure is not a complete quantum algorithm in its own right. Rather, you should think of phase estimation as a kind of 'subroutine' or 'module' that, when combined with other subroutines, can be used to perform interesting computational tasks. In specific applications of the phase estimation procedure we shall do exactly this, describing how these black box operations are to be performed, and combining them with the phase estimation procedure to do genuinely useful tasks. For the moment, though, we will continue to imagine them as black boxes.

The quantum phase estimation procedure uses two registers. The first register contains t qubits initially in the state $|0\rangle$. How we choose t depends on two things: the number of digits of accuracy we wish to have in our estimate for φ, and with what probability we wish the phase estimation procedure to be successful. The dependence of t on these quantities emerges naturally from the following analysis.

The second register begins in the state $|u\rangle$, and contains as many qubits as is necessary to store $|u\rangle$. Phase estimation is performed in two stages. First, we apply the circuit shown in Figure 5.2. The circuit begins by applying a Hadamard transform to the first register, followed by application of controlled- U operations on the second register, with U raised to successive powers of two. The final state of the first register is easily seen to be:

$$\frac{1}{2^{t/2}}\left(|0\rangle + e^{2\pi i 2^{t-1}\varphi}|1\rangle\right)\left(|0\rangle + e^{2\pi i 2^{t-2}\varphi}|1\rangle\right)\ldots\left(|0\rangle + e^{2\pi i 2^{0}\varphi}|1\rangle\right) = \frac{1}{2^{t/2}}\sum_{k=0}^{2^t-1} e^{2\pi i\varphi k}|k\rangle \tag{5.20}$$

We omit the second register from this description, since it stays in the state $|u\rangle$ throughout the computation.

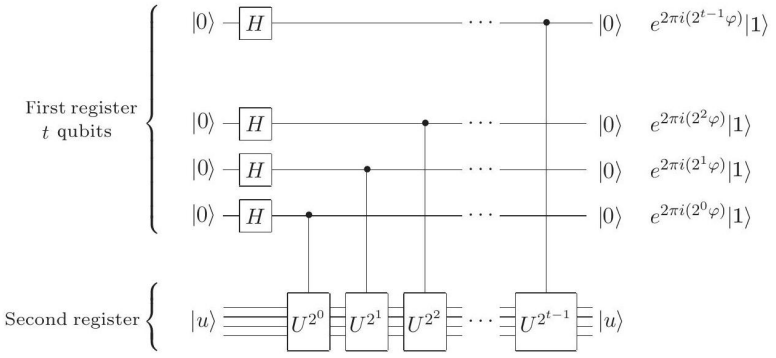


Figure 5.2. The first stage of the phase estimation procedure. Normalization factors of \$1 / \sqrt{2
\$ have been omitted, on the right.}

Exercise 5.7: Additional insight into the circuit in Figure 5.2 may be obtained by showing, as you should now do, that the effect of the sequence of controlled- U operations like that in Figure 5.2 is to take the state $|j\rangle|u\rangle$ to $|j\rangle U^j|u\rangle$. (Note that this does not depend on $|u\rangle$ being an eigenstate of U.)

The second stage of phase estimation is to apply the inverse quantum Fourier transform on the first register. This is obtained by reversing the circuit for the quantum Fourier transform in the previous section (Exercise 5.5), and can be done in $\Theta(t^2)$ steps. The third and final stage of phase estimation is to read out the state of the first register by doing a measurement in the computational basis. We will show that this provides a pretty good estimate of φ. An overall schematic of the algorithm is shown in Figure 5.3.

To sharpen our intuition as to why phase estimation works, suppose φ may be expressed exactly in t bits, as $\varphi = 0.\varphi_1 \ldots \varphi_t$. Then the state (5.20) resulting from the first stage of phase estimation may be rewritten

$$\frac{1}{2^{t/2}} \left(|0\rangle + e^{2\pi i 0.\varphi_t}|1\rangle\right) \left(|0\rangle + e^{2\pi i 0.\varphi_{t-1}\varphi_t}|1\rangle\right) \ldots \left(|0\rangle + e^{2\pi i 0.\varphi_1\varphi_2\cdots\varphi_t}|1\rangle\right). \tag{5.21}$$

The second stage of phase estimation is to apply the inverse quantum Fourier transform. But comparing the previous equation with the product form for the Fourier transform, Equation (5.4), we see that the output state from the second stage is the product state $|\varphi_1 \ldots \varphi_t\rangle$. A measurement in the computational basis therefore gives us φ exactly!

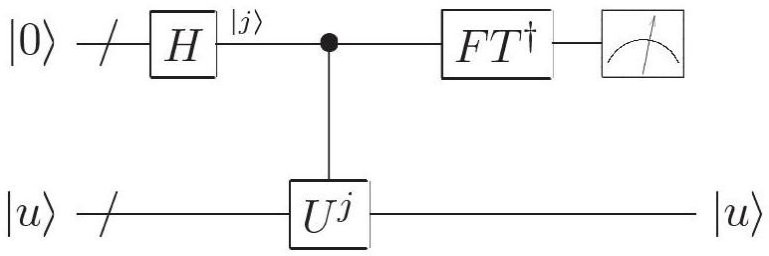


Figure 5.3. Schematic of the overall phase estimation procedure. The top t qubits (the '/' denotes a bundle of wires, as usual) are the first register, and the bottom qubits are the second register, numbering as many as required to perform U.$|u\rangle$ is an eigenstate of U with eigenvalue \$e^{2 \pi i \varphi
\$. The output of the measurement is an approximation to φ accurate to $t - \left\lceil \log\left(2 + \frac{1}{2\epsilon}\right)\right\rceil$ bits, with probability of success at least $1 - \epsilon$.}

Summarizing, the phase estimation algorithm allows one to estimate the phase φ of an eigenvalue of a unitary operator U, given the corresponding eigenvector $|u\rangle$. An essential feature at the heart of this procedure is the ability of the inverse Fourier transform to perform the transformation

$$\frac{1}{2^{t/2}} \sum_{j=0}^{2^t-1} e^{2\pi i \varphi j} |j\rangle |u\rangle \rightarrow |\tilde{\varphi}\rangle |u\rangle, \tag{5.22}$$

where $|\tilde{\varphi}\rangle$ denotes a state which is a good estimator for φ when measured.

8.2.3 5.2.1 Performance and requirements

The above analysis applies to the ideal case, where φ can be written exactly with a t bit binary expansion. What happens when this is not the case? It turns out that the procedure we have described will produce a pretty good approximation to φ with high probability, as foreshadowed by the notation used in (5.22). Showing this requires some careful manipulations.

Let b be the integer in the range 0 to $2^t - 1$ such that $b/2^t = 0.b_1 \ldots b_t$ is the best t bit approximation to φ which is less than φ. That is, the difference $\delta \equiv \varphi - b/2^t$ between φ and $b/2^t$ satisfies $0 \leq \delta \leq 2^{-t}$. We aim to show that the observation at the end of the phase estimation procedure produces a result which is close to b, and thus enables us to estimate φ accurately, with high probability. Applying the inverse quantum Fourier transform to the state (5.20) produces the state

$$\frac{1}{2^t} \sum_{k,l=0}^{2^t-1} e^{\frac{-2\pi i k l}{2^t}} e^{2\pi i \varphi k} |l\rangle. \tag{5.23}$$

Let α_l be the amplitude of $|(b+l) \, (\mathrm{mod} 2^t)\rangle$,

$$\alpha_l \equiv \frac{1}{2^t} \sum_{k=0}^{2^t-1} \left(e^{2\pi i \left(\varphi - (b+l)/2^t\right)} \right)^k. \tag{5.24}$$

This is the sum of a geometric series, so

$$\alpha_l = \frac{1}{2^t} \left(\frac{1 - e^{2\pi i \left(2^t \varphi - (b+l)\right)}}{1 - e^{2\pi i (\varphi - (b+l)/2^t)}} \right) \tag{5.25}$$

$$= \frac{1}{2^t} \left(\frac{1 - e^{2\pi i \left(2^t \delta - l\right)}}{1 - e^{2\pi i (\delta - l/2^t)}} \right) \tag{5.26}$$

Suppose the outcome of the final measurement is m. We aim to bound the probability of obtaining a value of m such that $|m - b| > e$, where e is a positive integer characterizing our desired tolerance to error. The probability of observing such an m is given by

$$p(|m - b| > e) = \sum_{-2^{t-1} < l \leq -(e+1)} |\alpha_l|^2 + \sum_{e+1 \leq l \leq 2^{t-1}} |\alpha_l|^2 . \tag{5.27}$$

But for any real $\theta, |1 - \exp(i\theta)| \leq 2$, so

$$|\alpha_l| \leq \frac{2}{2^t \left|1 - e^{2\pi i (\delta - l/2^t)}\right|} \tag{5.28}$$

By elementary geometry or calculus $|1 - \exp(i\theta)| \geq 2|\theta|/\pi$ whenever $-\pi \leq \theta \leq \pi$. But when $-2^{t-1} < l \leq 2^{t-1}$ we have $-\pi \leq 2\pi \left(\delta - l/2^t\right) \leq \pi$. Thus

$$|\alpha_l| \leq \frac{1}{2^{t+1}\left(\delta - l/2^t\right)} \tag{5.29}$$

Combining (5.27) and (5.29) gives

$$p(|m-b|>e) \leq \frac{1}{4}\left[\sum_{l=-2^{t-1}+1}^{-(e+1)} \frac{1}{\left(l-2^t\delta\right)^2} + \sum_{l=e+1}^{2^{t-1}} \frac{1}{\left(l-2^t\delta\right)^2}\right] \tag{5.30}$$

Recalling that $0 \leq 2^t\delta \leq 1$, we obtain

$$p(|m-b|>e) \leq \frac{1}{4}\left[\sum_{l=-2^{t-1+1}}^{-(e+1)} \frac{1}{l^2} + \sum_{l=e+1}^{2^{t-1}} \frac{1}{(l-1)^2}\right] \tag{5.31}$$

$$\leq \frac{1}{2}\sum_{l=e}^{2^{t-1}-1} \frac{1}{l^2} \tag{5.32}$$

$$\leq \frac{1}{2}\int_{e-1}^{2^{t-1}-1} dl \frac{1}{l^2} \tag{5.33}$$

$$= \frac{1}{2(e-1)} \tag{5.34}$$

Suppose we wish to approximate φ to an accuracy 2^{-n}, that is, we choose $e = 2^{t-n} - 1$. By making use of $t = n + p$ qubits in the phase estimation algorithm we see from (5.34) that the probability of obtaining an approximation correct to this accuracy is at least $1 - 1/2\left(2^p - 2\right)$. Thus to successfully obtain φ accurate to n bits with probability of success at least $1 - \epsilon$ we choose

$$t = n + \left\lceil \log\left(2 + \frac{1}{2\epsilon}\right)\right\rceil \tag{5.35}$$

In order to make use of the phase estimation algorithm, we need to be able to prepare an eigenstate $|u\rangle$ of U. What if we do not know how to prepare such an eigenstate? Suppose that we prepare some other state $|\psi\rangle$ in place of $|u\rangle$. Expanding this state in terms of eigenstates $|u\rangle$ of U gives $|\psi\rangle = \sum_u c_u|u\rangle$. Suppose the eigenstate $|u\rangle$ has eigenvalue $e^{2\pi i\varphi_u}$. Intuitively, the result of running the phase estimation algorithm will be to give
as output a state close to $\sum_u c_u \left|\widetilde{\varphi_u}\right\rangle |u\rangle$, where $\widetilde{\varphi_u}$ is a pretty good approximation to the phase φ_u. Therefore, we expect that reading out the first register will give us a good approximation to φ_u, where u is chosen at random with probability $|c_u|^2$. Making this argument rigorous is left for Exercise 5.8. This procedure allows us to avoid preparing a (possibly unknown) eigenstate, at the cost of introducing some additional randomness into the algorithm.

Exercise 5.8: Suppose the phase estimation algorithm takes the state $|0\rangle|u\rangle$ to the state $\left|\widetilde{\varphi_u}\right\rangle|u\rangle$, so that given the input $|0\rangle\left(\sum_u c_u|u\rangle\right)$, the algorithm outputs $\sum_u c_u \left|\widetilde{\varphi_u}\right\rangle|u\rangle$. Show that if t is chosen according to (5.35), then the probability for measuring φ_u accurate to n bits at the conclusion of the phase estimation algorithm is at least $|c_u|^2(1-\epsilon)$.

Why is phase estimation interesting? For its own sake, phase estimation solves a problem which is both non-trivial and interesting from a physical point of view: how to estimate the eigenvalue associated to a given eigenvector of a unitary operator. Its real use, though, comes from the observation that other interesting problems can be reduced to phase estimation, as will be shown in subsequent sections. The phase estimation algorithm is summarized below.

Algorithm: Quantum phase estimation

Inputs: (1) A black box wich performs a controlled- U^j operation, for integer j, (2) an eigenstate $|u\rangle$ of U with eigenvalue $e^{2\pi i\varphi_u}$, and (3) $t = n + \left\lceil \log\left(2 + \frac{1}{2\epsilon}\right)\right\rceil$ qubits initialized to $|0\rangle$.

Outputs: An n-bit approximation $\widetilde{\varphi_u}$ to φ_u.

Runtime: $O(t^2)$ operations and one call to controlled- U^j black box. Succeeds with probability at least $1 - \epsilon$.

Procedure:

1. $|0\rangle|u\rangle$ initial state
2. $\rightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle|u\rangle$ create superposition
3. $\rightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle U^j|u\rangle$ apply black box

$$= \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} e^{2\pi ij\varphi_u}|j\rangle|u\rangle$$

result of black box

4. $\rightarrow |\widetilde{\varphi_u}\rangle\,|u\rangle$

apply inverse Fourier transform

5. $\rightarrow \widetilde{\varphi_u}$

measure first register

Exercise 5.9: Let U be a unitary transform with eigenvalues ± 1, which acts on a state $|\psi\rangle$. Using the phase estimation procedure, construct a quantum circuit to collapse $|\psi\rangle$ into one or the other of the two eigenspaces of U, giving also a
classical indicator as to which space the final state is in. Compare your result with Exercise 4.34.

8.2.4 5.3 Applications: order-finding and factoring

The phase estimation procedure can be used to solve a variety of interesting problems. We now describe two of the most interesting of these problems: the order-finding problem, and the factoring problem. These two problems are, in fact, equivalent to one another, so in Section 5.3.1 we explain a quantum algorithm for solving the order-finding problem, and in Section 5.3.2 we explain how the order-finding problem implies the ability to factor as well.

To understand the quantum algorithms for factoring and order-finding requires a little background in number theory. All the required materials are collected together in Appendix 4. The description we give over the next two sections focuses on the quantum aspects of the problem, and requires only a little familiarity with modular arithmetic to be readable. Detailed proofs of the number-theoretic results we quote here may be found in Appendix 4.

The fast quantum algorithms for order-finding and factoring are interesting for at least three reasons. First, and most important in our opinion, they provide evidence for the idea that quantum computers may be inherently more powerful than classical computers, and provide a credible challenge to the strong Church-Turing thesis. Second, both problems are of sufficient intrinsic worth to justify interest in any novel algorithm, be it classical or quantum. Third, and most important from a practical standpoint, efficient algorithms for order-finding and factoring can be used to break the RSA public-key cryptosystem (Appendix 5).

8.2.5 5.3.1 Application: order-finding

For positive integers x and $N, x < N$, with no common factors, the order of x modulo N is defined to be the least positive integer, r, such that $x^r = 1(\bmod N)$. The order-finding problem is to determine the order for some specified x and N. Order-finding is believed to be a hard problem on a classical computer, in the sense that no algorithm is known to solve the problem using resources polynomial in the $O(L)$ bits needed to specify the problem, where $L \equiv \lceil \log(N) \rceil$ is the number of bits needed to specify N. In this section we explain how phase estimation may be used to obtain an efficient quantum algorithm for order-finding.

Exercise 5.10: Show that the order of $x = 5$ modulo $N = 21$ is 6 .
Exercise 5.11: Show that the order of x satisfies $r \leq N$.
The quantum algorithm for order-finding is just the phase estimation algorithm applied to the unitary operator

$$U|y\rangle \equiv |xy(\bmod N)\rangle \tag{5.36}$$

with $y \in \{0,1\}^L$. (Note that here and below, when $N \leq y \leq 2^L - 1$, we use the convention that $xy(\bmod N)$ is just y again. That is, U only acts non-trivially when $0 \leq y \leq N-1$.) A simple calculation shows that the states defined by

$$|u_s\rangle \equiv \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left[\frac{-2\pi i s k}{r}\right] \left|x^k \bmod N\right\rangle \tag{5.37}$$

for integer $0 \leq s \leq r-1$ are eigenstates of U, since

$$U\,|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left[\frac{-2\pi i s k}{r}\right] \left|x^{k+1} \bmod N\right\rangle \tag{5.38}$$

$$= \exp\left[\frac{2\pi i s}{r}\right] |u_s\rangle \tag{5.39}$$

Using the phase estimation procedure allows us to obtain, with high accuracy, the corresponding eigenvalues $\exp(2\pi i s/r)$, from which we can obtain the order r with a little bit more work.

Exercise 5.12: Show that U is unitary (Hint: x is co-prime to N, and therefore has an inverse modulo N).

There are two important requirements for us to be able to use the phase estimation procedure: we must have efficient procedures to implement a controlled- U^{2^j} operation for any integer j, and we must be able to efficiently prepare an eigenstate $|u_s\rangle$ with a nontrivial eigenvalue, or at least a superposition of such eigenstates. The first requirement is satisfied by using a procedure known as modular exponentiation, with which we can implement the entire sequence of controlled- U^{2^j} operations applied by the phase estimation procedure using $O\left(L^3\right)$ gates, as described in Box 5.2.

The second requirement is a little tricker: preparing $|u_s\rangle$ requires that we know r, so this is out of the question. Fortunately, there is a clever observation which allows us to circumvent the problem of preparing $|u_s\rangle$, which is that

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = |1\rangle. \tag{5.44}$$

In performing the phase estimation procedure, if we use $t = 2L + 1 + \left\lceil \log\left(2 + \frac{1}{2\epsilon}\right) \right\rceil$ qubits in the first register (referring to Figure 5.3), and prepare the second register in the state $|1\rangle$ -

which is trivial to construct - it follows that for each s in the range 0 through $r-1$, we will obtain an estimate of the phase $\varphi \approx s/r$ accurate to $2L+1$ bits, with probability at least $(1-\epsilon)/r$. The order-finding algorithm is schematically depicted in Figure 5.4.

Exercise 5.13: Prove (5.44). (Hint: $\sum_{s=0}^{r-1} \exp(-2\pi isk/r) = r\delta_{k0}$.) In fact, prove that

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{2\pi isk/r} |u_s\rangle = \left|x^k \bmod N\right\rangle. \tag{5.45}$$

Exercise 5.14: The quantum state produced in the order-finding algorithm, before the inverse Fourier transform, is

$$|\psi\rangle = \sum_{j=0}^{2^t-1} |j\rangle U^j |1\rangle = \sum_{j=0}^{2^t-1} |j\rangle \left|x^j \bmod N\right\rangle, \tag{5.46}$$

Box 5.2: Modular exponentiation

How can we compute the sequence of controlled- U^{2^j} operations used by the phase estimation procedure as part of the order-finding algorithm? That is, we wish to compute the transformation

$$|z\rangle|y\rangle \rightarrow |z\rangle U^{z_t t^{t-1}} \ldots U^{z_1 2^0} |y\rangle \tag{5.40}$$

$$= |z\rangle \left|x^{z_t 2^{t-1}} \times \cdots \times x^{z_1 2^0} y (\mathrm{mod} N)\right\rangle \tag{5.41}$$

$$= |z\rangle \left|x^z y (\mathrm{mod} N)\right\rangle. \tag{5.42}$$

Thus the sequence of controlled- U^{2^j} operations used in phase estimation is equivalent to multiplying the contents of the second register by the modular exponential $x^z (\mathrm{mod} N)$, where z is the contents of the first register. This operation may be accomplished easily using the techniques of reversible computation. The basic idea is to reversibly compute the function $x^z (\mathrm{mod} N)$ of z in a third register, and then to reversibly multiply the contents of the second register by $x^z (\mathrm{mod}\, N)$, using the trick of uncomputation to erase the contents of the third register upon completion. The algorithm for computing the modular exponential has two stages. The first stage uses modular multiplication to compute $x^2 (\mathrm{mod} N)$, by squaring x modulo N, then computes $x^4 (\mathrm{mod} N)$ by squaring $x^2 (\mathrm{mod} N)$, and continues in this way, computing $x^{2^j} (\mathrm{mod} N)$ for all j up to $t-1$. We use $t = 2L + 1 + \lceil \log(2 + 1/(2\epsilon)) \rceil = O(L)$, so a total of $t - 1 = O(L)$ squaring operations is performed at a cost of $O(L^2)$ each (this cost assumes the circuit used to do the squaring implements the familiar algorithm we all learn as children for multiplication), for a total cost of $O(L^3)$ for the first stage. The second stage of the algorithm is based upon the observation we've already noted,

$$x^z (\mathrm{mod} N) = \left(x^{z_t 2^{t-1}} (\mathrm{mod} N)\right) \left(x^{z_{t-1} 2^{t-2}} (\mathrm{mod} N)\right) \ldots \left(x^{z_1 2^0} (\mathrm{mod} N)\right). \tag{5.43}$$

Performing $t-1$ modular multiplications with a cost $O(L^2)$ each, we see that this product can be computed using $O(L^3)$ gates. This is sufficiently efficient for our purposes, but more efficient algorithms are possible based on more efficient algorithms for multiplication (see 'History and further reading'). Using the techniques of Section 3.2.5, it is now straightforward to construct a reversible circuit with a t bit register and an L bit register which, when started in the state $(\ z, y\ )$ outputs $(z, x^z y (\mathrm{mod} N))$, using $O(L^3)$ gates, which can be translated into a quantum circuit using $O(L^3)$ gates computing the transformation $|z\rangle|y\rangle \rightarrow |z\rangle |x^z y (\mathrm{mod} N)\rangle$.

if we initialize the second register as $|1\rangle$. Show that the same state is obtained if we replace U^j with a different unitary transform V, which computes

$$V|j\rangle|k\rangle = |j\rangle \left|k + x^j \bmod N\right\rangle \tag{5.47}$$

and start the second register in the state $|0\rangle$. Also show how to construct V using $O(L^3)$ gates.

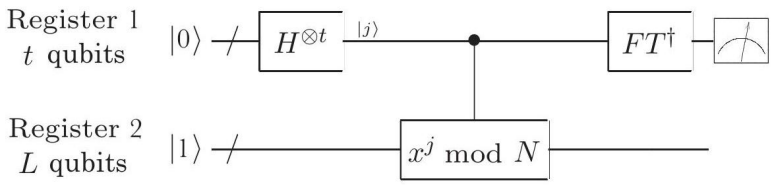


Figure 5.4. Quantum circuit for the order-finding algorithm. The second register is shown as being initialized to the $|1\rangle$ state, but if the method of Exercise 5.14 is used, it can be initialized to $|0\rangle$ instead. This circuit can also be used for factoring, using the reduction given in Section 5.3.2.

8.2.6 The continued fraction expansion

The reduction of order-finding to phase estimation is completed by describing how to obtain the desired answer, r, from the result of the phase estimation algorithm, $\varphi \approx s/r$. We only know φ to $2L+1$ bits, but we also know a priori that it is a rational number - the ratio of two bounded integers - and if we could compute the nearest such fraction to φ we might obtain r.

Remarkably, there is an algorithm which accomplishes this task efficiently, known as the continued fractions algorithm. An example of how this works is described in Box 5.3. The reason this algorithm satisfies our needs is the following theorem, which is proved in Appendix 4:

Theorem 5.1: Suppose s/r is a rational number such that

$$\left|\frac{s}{r} - \varphi\right| \leq \frac{1}{2r^2} \tag{5.48}$$

Then s/r is a convergent of the continued fraction for φ, and thus can be computed in $O(L^3)$ operations using the continued fractions algorithm.

Since φ is an approximation of s/r accurate to $2L+1$ bits, it follows that $|s/r - \varphi| \leq 2^{-2L-1} \leq 1/2r^2$, since $r \leq N \leq 2^L$. Thus, the theorem applies.

Summarizing, given φ the continued fractions algorithm efficiently produces numbers s' and r' with no common factor, such that $s'/r' = s/r$. The number r' is our candidate for the order. We can check to see whether it is the order by calculating $x^{r'} \bmod N$, and seeing if the result is 1 . If so, then r' is the order of x modulo N, and we are done!

Performance

How can the order-finding algorithm fail? There are two possibilities. First, the phase estimation procedure might produce a bad estimate to s/r. This occurs with probability at most ϵ, and can be made small with a negligible increase in the size of the circuit. More seriously, it might be that s and r have a common factor, in which case the number r' returned by the continued fractions algorithm be a factor of r, and not r itself. Fortunately, there are at least three ways around this problem.

Perhaps the most straightforward way is to note that for randomly chosen s in the range 0 through $r-1$, it's actually pretty likely that s and r are co-prime, in which case the continued fractions algorithm must return r. To see that this is the case, note that by Problem 4.1 on page 638 the number of prime numbers less than r is at least

Box 5.3: The continued fractions algorithm

The idea of the continued fractions algorithm is to describe real numbers in terms of integers alone, using expressions of the form

$$[a_0, \ldots, a_M] \equiv a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{a_M}}}} \tag{5.49}$$

where $a_0, \ldots, a_M$ are positive integers. (For applications to quantum computing it is convenient to allow $a_0 = 0$ as well.) We define the m th convergent ($0 \leq m \leq M$) to this continued fraction to be $[a_0, \ldots, a_m]$. The continued fractions algorithm is a method for determining the continued fraction expansion of an arbitrary real number. It is easily understood by example. Suppose we are trying to decompose 31/13 as a continued fraction. The first step of the continued fractions algorithm is to split 31/13 into its integer and fractional part,

$$\frac{31}{13} = 2 + \frac{5}{13} \tag{5.50}$$

Next we invert the fractional part, obtaining

$$\frac{31}{13} = 2 + \frac{1}{\frac{13}{5}} \tag{5.51}$$

These steps - split then invert - are now applied to 13/5, giving

$$\frac{31}{13} = 2 + \frac{1}{2 + \frac{3}{5}} = 2 + \frac{1}{2 + \frac{1}{\frac{5}{3}}} \tag{5.52}$$

Next we split and invert 5/3:

$$\frac{31}{13} = 2 + \frac{1}{2 + \frac{1}{1 + \frac{2}{3}}} = 2 + \frac{1}{2 + \frac{1}{1 + \frac{1}{\frac{3}{2}}}} \tag{5.53}$$

The decomposition into a continued fraction now terminates, since

$$\frac{3}{2} = 1 + \frac{1}{2} \tag{5.54}$$

may be written with a 1 in the numerator without any need to invert, giving a final continued fraction representation of 31/13 as

$$\frac{31}{13} = 2 + \frac{1}{2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2}}}} \tag{5.55}$$

It's clear that the continued fractions algorithm terminates after a finite number of 'split and invert' steps for any rational number, since the numerators which appear ($31, 5, 3, 2, 1$ in the example) are strictly decreasing. How quickly does this termination occur? It turns out that if $\varphi = s/r$ is a rational number, and s and r are L bit integers, then the continued fraction expansion for φ can be computed using $O(L^3)$ operations $-O(L)$ 'split and invert' steps, each using $O(L^2)$ gates for elementary arithmetic.

$r/2\log r$, and thus the chance that s is prime (and therefore, co-prime to r) is at least $1/2\log(r) > 1/2\log(N)$. Thus, repeating the algorithm $2\log(N)$ times we will, with high probability, observe a phase s/r such that s and r are co-prime, and therefore the continued fractions algorithm produces r, as desired.

A second method is to note that if $r' \neq r$, then r' is guaranteed to be a factor of r, unless $s = 0$, which possibility occurs with probability $1/r \leq 1/2$, and which can be discounted further by a few repetitions. Suppose we replace a by $a' \equiv a^{r'} (\mathrm{mod} N)$. Then the order of a' is r/r'. We can now repeat the algorithm, and try to compute the order of a', which, if we succeed, allows us to compute the order of a, since $r = r' \times r/r'$. If we fail, then we obtain r'' which is a factor of r/r', and we now try to compute the order of $a'' \equiv (a')^{r''} (\mathrm{mod} N)$. We iterate this procedure until we determine the order of a. At most $\log(r) = O(L)$ iterations are required, since each repetition reduces the order of the current candidate $a'' \cdots$ by a factor of at least two.

The third method is better than the first two methods, in that it requires only a constant number of trials, rather than $O(L)$ repetitions. The idea is to repeat the phase estimation-continued fractions procedure twice, obtaining r'_1, s'_1 the first time, and r'_2, s'_2 the second time. Provided s'_1 and s'_2 have no common factors, r may be extracted by taking the least common multiple of r_1 and r_2. The probability that s'_1 and s'_2 have no common factors is given by

$$1 - \sum_q p\left(q \mid s'_1\right) p\left(q \mid s'_2\right) \tag{5.56}$$

where the sum is over all prime numbers q, and $p(x \mid y)$ here means the probability of x dividing y. If q divides s'_1 then it must also divide the true value of s, s_1, on the first iteration, so to upper bound $p\left(q \mid s'_1\right)$ it suffices to upper bound $p\left(q \mid s_1\right)$, where s_1 is chosen uniformly at random from 0 through $r-1$. It is easy to see that $p\left(q \mid s_1\right) \leq 1/q$, and thus $p\left(q \mid s'_1\right) \leq 1/q$. Similarly, $p\left(q \mid s'_2\right) \leq 1/q$, and thus the probability that s'_1 and s'_2 have no common factors satisfies

$$1 - \sum_q p\left(q \mid s'_1\right) p\left(q \mid s'_2\right) \geq 1 - \sum_q \frac{1}{q^2}. \tag{5.57}$$

The right hand side can be upper bounded in a number of ways; a simple technique is provided in Exercise 5.16, which gives

$$1 - \sum_q p\left(q \mid s'_1\right) p\left(q \mid s'_2\right) \geq \frac{1}{4} \tag{5.58}$$

and thus the probability of obtaining the correct r is at least $1/4$.

Exercise 5.15: Show that the least common multiple of positive integers x and y is $xy/\gcd(x, y)$, and thus may be computed in $O\left(L^2\right)$ operations if x and y are L bit numbers.

Exercise 5.16: For all $x \geq 2$ prove that $\int_x^{x+1} 1/y^2 dy \geq 2/3x^2$. Show that

$$\sum_q \frac{1}{q^2} \leq \frac{3}{2} \int_2^\infty \frac{1}{y^2} dy = \frac{3}{4} \tag{5.59}$$

and thus that (5.58) holds.

What resource requirements does this algorithm consume? The Hadamard transform requires $O(L)$ gates, and the inverse Fourier transform requires $O\left(L^2\right)$ gates. The major cost in the quantum circuit proper actually comes from the modular exponentiation, which uses $O\left(L^3\right)$ gates, for a total of $O\left(L^3\right)$ gates in the quantum circuit proper. The continued fractions algorithm adds $O\left(L^3\right)$ more gates, for a total of $O\left(L^3\right)$ gates to obtain r'. Using the third

method for obtaining r from r' we need only repeat this procedure a constant number of times to obtain the order, r, for a total cost of $O(L^3)$. The algorithm is summarized below.

Algorithm: Quantum order-finding

Inputs: (1) A black box $U_{x,N}$ which performs the transformation $|j\rangle|k\rangle \rightarrow |j\rangle |x^j k \bmod N\rangle$, for x co-prime to the L-bit number N, (2) $t = 2L + 1 + \left\lceil \log\left(2 + \frac{1}{2\epsilon}\right)\right\rceil$ qubits initialized to $|0\rangle$, and (3) L qubits initialized to the state $|1\rangle$.

Outputs: The least integer $r > 0$ such that $x^r = 1(\mathrm{mod} N)$.

Runtime: $O(L^3)$ operations. Succeeds with probability $O(1)$.

Procedure:

1. $|0\rangle|1\rangle$ initial state
2. $\rightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle|1\rangle$ create superposition
3. $\rightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle |x^j \bmod N\rangle$ apply $U_{x,N}$

$$\approx \frac{1}{\sqrt{r2^t}} \sum_{s=0}^{r-1} \sum_{j=0}^{2^t-1} e^{2\pi i s j/r} |j\rangle |u_s\rangle$$

4. $\rightarrow \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |\widetilde{s/r}\rangle |u_s\rangle$
   apply inverse Fourier transform to first register
5. $\rightarrow \widetilde{s/r}$
   measure first register
6. $\rightarrow r$
   apply continued fractions algorithm

8.2.7 5.3.2 Application: factoring

The problem of distinguishing prime numbers from composites, and of resolving composite numbers into their prime factors, is one of the most important and useful in all of arithmetic. [...] The dignity of science seems to demand that every aid to the solution of such an elegant and celebrated problem be zealously cultivated.

- Carl Friedrich Gauss, as quoted by Donald Knuth

Given a positive composite integer N, what prime numbers when multiplied together equal it? This factoring problem turns out to be equivalent to the order-finding problem we just studied, in the sense that a fast algorithm for order-finding can easily be turned into a fast algorithm for factoring. In this section we explain the method used to reduce factoring to order-finding, and give a simple example of this reduction.

The reduction of factoring to order-finding proceeds in two basic steps. The first step is to show that we can compute a factor of N if we can find a non-trivial solution $x \neq \pm 1(\bmod N)$ to the equation $x^2 = 1(\bmod N)$. The second step is to show that a randomly chosen y co-prime to N is quite likely to have an order r which is even, and such that $y^{r/2} \neq \pm 1(\mathrm{mod} N)$, and thus $x \equiv y^{r/2}(\mathrm{mod} N)$ is a non-trivial solution to $x^2 = 1(\mathrm{mod} N)$. These two steps are embodied in the following theorems, whose proofs may be found in Section A4.3 of Appendix 4.

Theorem 5.2: Suppose N is an L bit composite number, and x is a non-trivial solution to the equation $x^2 = 1(\mathrm{mod}N)$ in the range $1 \leq x \leq N$, that is, neither $x = 1(\mathrm{mod}N)$ nor $x = N-1 = -1(\mathrm{mod}\, N)$. Then at least one of $\gcd(x-1, N)$ and $\gcd(x+1, N)$ is a non-trivial factor of N that can be computed using $O\left(L^3\right)$ operations.

Theorem 5.3: Suppose $N = p_1^{\alpha_1} \ldots p_m^{\alpha_m}$ is the prime factorization of an odd composite positive integer. Let x be an integer chosen uniformly at random, subject to the requirements that $1 \leq x \leq N-1$ and x is co-prime to N. Let r be the order of x modulo N. Then

$$p\left(r \text{ is even and } x^{r/2} \neq -1(\mathrm{mod}N)\right) \geq 1 - \frac{1}{2^m} \tag{5.60}$$

Theorems 5.2 and 5.3 can be combined to give an algorithm which, with high probability, returns a non-trivial factor of any composite N. All the steps in the algorithm can be performed efficiently on a classical computer except (so far as is known today) an order-finding 'subroutine' which is used by the algorithm. By repeating the procedure we may find a complete prime factorization of N. The algorithm is summarized below.

Algorithm: Reduction of factoring to order-finding

Inputs: A composite number N
Outputs: A non-trivial factor of N.
Runtime: $O\left((\log N)^3\right)$ operations. Succeeds with probability $O(1)$.

Procedure:

1. If N is even, return the factor 2 .

2. Determine whether $N = a^b$ for integers $a \geq 1$ and $b \geq 2$, and if so return the factor a (uses the classical algorithm of Exercise 5.17).

3. Randomly choose x in the range 1 to $N-1$. If $\gcd(x, N) > 1$ then return the factor $\gcd(x, N)$.

4. Use the order-finding subroutine to find the order r of x modulo N.

5. If r is even and $x^{r/2} \neq -1(\mathrm{\ mod}\ N)$ then compute $\gcd\left(x^{r/2}-1, N\right)$ and $\gcd\left(x^{r/2}+1, N\right)$, and test to see if one of these is a non-trivial factor, returning that factor if so. Otherwise, the algorithm fails.
   Steps 1 and 2 of the algorithm either return a factor, or else ensure that N is an odd integer with more than one prime factor. These steps may be performed using $O(1)$ and $O\left(L^3\right)$ operations, respectively. Step 3 either returns a factor, or produces a randomly chosen element x of $\{0, 1, 2, \ldots, N-1\}$. Step 4 calls the order-finding subroutine, computing the order r of x modulo N. Step 5 completes the algorithm, since Theorem 5.3 guarantees that with probability at least one-half r will be even and $x^{r/2} \neq -1(\mathrm{mod}N)$, and then Theorem 5.2 guarantees that either $\gcd\left(x^{r/2}-1, N\right)$ or $\gcd\left(x^{r/2}+1, N\right)$ is a non-trivial factor of N. An example illustrating the use of this algorithm with the quantum order-finding subroutine is shown in Box 5.4.

Exercise 5.17: Suppose N is L bits long. The aim of this exercise is to find an efficient classical algorithm to determine whether $N = a^b$ for some integers $a \geq 1$ and $b \geq 2$. This may be done as follows:
(1) Show that b, if it exists, satisfies $b \leq L$.
(2) Show that it takes at most $O\left(L^2\right)$ operations to compute $\log_2 N$, $x = y/b$ for $b \leq L$, and the two integers u_1 and u_2 nearest to 2^x.

(3) Show that it takes at most $O(L^2)$ operations to compute u_1^b and u_2^b (use repeated squaring) and check to see if either is equal to N.
(4) Combine the previous results to give an $O(L^3)$ operation algorithm to determine whether $N = a^b$ for integers a and b.

Exercise 5.18: (Factoring 91) Suppose we wish to factor $N = 91$. Confirm that steps 1 and 2 are passed. For step 3, suppose we choose $x = 4$, which is co-prime to 91 . Compute the order r of x with respect to N, and show that $x^{r/2} \bmod 91 = 64 \neq -1(\text{mod}91)$, so the algorithm succeeds, giving $\gcd(64 - 1, 19) = 7$.
It is unlikely that this is the most efficient method you've seen for factoring 91. Indeed, if all computations had to be carried out on a classical computer, this reduction would not result in an efficient factoring algorithm, as no efficient method is known for solving the order-finding problem on a classical computer.

Exercise 5.19: Show that $N = 15$ is the smallest number for which the order-finding subroutine is required, that is, it is the smallest composite number that is not even or a power of some smaller integer.

8.2.8 5.4 General applications of the quantum Fourier transform

The main applications of the quantum Fourier transform we have described so far in this chapter are phase estimation and order-finding. What other problems can be solved with these techniques? In this section, we define a very general problem known as the hidden subgroup problem, and describe an efficient quantum algorithm for solving it. This problem, which encompasses all known 'exponentially fast' applications of the quantum Fourier transform, can be thought of as a generalization of the task of finding the unknown period of a periodic function, in a context where the structure of the domain and range

Box 5.4: Factoring 15 quantum-mechanically

The use of order-finding, phase estimation, and continued fraction expansions in the quantum factoring algorithm is illustrated by applying it to factor $N = 15$. First, we choose a random number which has no common factors with N; suppose we choose $x = 7$. Next, we compute the order r of x with respect to N, using the quantum order-finding algorithm: begin with the state $|0\rangle|0\rangle$ and create the state

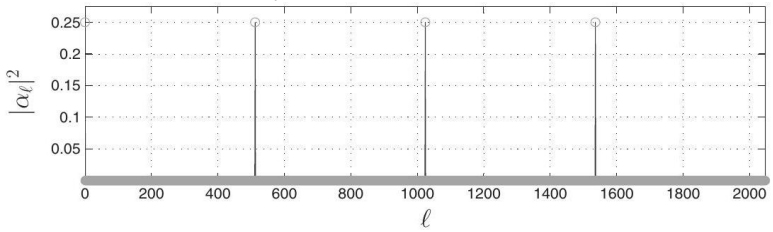
$$\frac{1}{\sqrt{2^t}} \sum_{k=0}^{2^t-1} |k\rangle|0\rangle = \frac{1}{\sqrt{2^t}} \left[|0\rangle + |1\rangle + |2\rangle + \cdots + \left|2^t - 1\right\rangle\right] |0\rangle \tag{5.61}$$

by applying $t = 11$ Hadamard transforms to the first register. Choosing this value of t ensures an error probability ϵ of at most $1/4$. Next, compute $f(k) = x^k \bmod N$, leaving the result in the second register,

$$\begin{aligned} &\frac{1}{\sqrt{2^t}} \sum_{k=0}^{2^t-1} |k\rangle \left|x^k \bmod N\right\rangle \\ &= \frac{1}{\sqrt{2^t}} [|0\rangle|1\rangle + |1\rangle|7\rangle + |2\rangle|4\rangle + |3\rangle|13\rangle + |4\rangle|1\rangle + |5\rangle|7\rangle + |6\rangle|4\rangle + \ldots] \end{aligned} \tag{5.62}$$

We now apply the inverse Fourier transform $FT^\dagger$ to the first register and measure it. One way of analyzing the distribution of outcomes obtained is to calculate the reduced density matrix for the first register, and apply $FT^\dagger$ to it, and calculate the measurement statistics. However, since no further operation is applied to the second register, we can instead apply the

principle of implicit measurement (Section 4.4) and assume that the second register is measured, obtaining a random result from 1 , 7,4 , or 13 . Suppose we get 4 (any of the results works); this means the state input to $FT^\dagger$ would have been $\sqrt{\frac{4}{2^t}}[|2\rangle + |6\rangle + |10\rangle + |14\rangle + \ldots]$. After applying $FT^\dagger$ we obtain some state $\sum_\ell \alpha_\ell |\ell\rangle$, with the probability distribution



shown for $2^t = 2048$. The final measurement therefore gives either $0, 512, 1024$, or 1536 , each with probability almost exactly $1/4$. Suppose we obtain $\ell = 1536$ from the measurement; computing the continued fraction expansion thus gives $1536/2048 = 1/(1 + (1/3))$, so that $3/4$ occurs as a convergent in the expansion, giving $r = 4$ as the order of $x = 7$. By chance, r is even, and moreover, $x^{r/2} \bmod N = 7^2 \bmod 15 = 4 \neq -1 \bmod 15$, so the algorithm works: computing the greatest common divisor $\gcd(x^2 - 1, 15) = 3$ and $\gcd(x^2 + 1, 15) = 5$ tells us that $15 = 3 \times 5$.
of the function may be very intricate. In order to present this problem in the most approachable manner, we begin with two more specific applications: period-finding (of a one-dimensional function), and discrete logarithms. We then return to the general hidden subgroup problem. Note that the presentation in this section is rather more schematic and conceptual than earlier sections in this chapter; of necessity, this means that the reader interested in understanding all the details will have to work much harder!

8.2.9 5.4.1 Period-finding

Consider the following problem. Suppose f is a periodic function producing a single bit as output and such that $f(x+r) = f(x)$, for some unknown $0 < r < 2^L$, where $x, r \in \{0, 1, 2, \ldots\}$. Given a quantum black box U which performs the unitary transform $U|x\rangle|y\rangle \to |x\rangle|y \oplus f(x)\rangle$ (where $\oplus$ denotes addition modulo 2) how many black box queries and other operations are required to determine r ? Note that in practice U operates on a finite domain, whose size is determined by the desired accuracy for r. Here is a quantum algorithm which solves this problem using one query, and $O(L^2)$ other operations:

Algorithm: Period-finding

Inputs: (1) A black box which performs the operation $U|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$, (2) a state to store the function evaluation, initialized to $|0\rangle$, and (3) $t = O(L + \log(1/\epsilon))$ qubits initialized to $|0\rangle$.

Outputs: The least integer $r > 0$ such that $f(x + r) = f(x)$.
Runtime: One use of U, and $O(L^2)$ operations. Succeeds with probability $O(1)$.

Procedure:

1. $|0\rangle|0\rangle$
2. $\to \frac{1}{\sqrt{2^t}} \sum_{x=0}^{2^t-1} |x\rangle|0\rangle$
3. $\to \frac{1}{\sqrt{2^t}} \sum_{x=0}^{2^t-1} |x\rangle|f(x)\rangle$

$$\approx \frac{1}{\sqrt{r2^t}} \sum_{\ell=0}^{r-1} \sum_{x=0}^{2^t-1} e^{2\pi i \ell x/r} |x\rangle |\hat{f}(\ell)\rangle$$

4. $\rightarrow \frac{1}{\sqrt{r}} \sum_{\ell=0}^{r-1} \widetilde{|\ell/r\rangle} |\hat{f}(\ell)\rangle$

5. $\rightarrow \widetilde{\ell/r}$

6. $\rightarrow r$

initial state
create superposition
apply U
apply inverse Fourier transform to first register
measure first register
apply continued fractions algorithm

The key to understanding this algorithm, which is based on phase estimation, and is nearly identical to the algorithm for quantum order-finding, is step 3, in which we introduce the state

$$|\hat{f}(\ell)\rangle \equiv \frac{1}{\sqrt{r}} \sum_{x=0}^{r-1} e^{-2\pi i \ell x/r} |f(x)\rangle \tag{5.63}$$

the Fourier transform of $|f(x)\rangle$. The identity used in step 3 is based on

$$|f(x)\rangle = \frac{1}{\sqrt{r}} \sum_{\ell=0}^{r-1} e^{2\pi i \ell x/r} |\hat{f}(\ell)\rangle \tag{5.64}$$

which is easy to verify by noting that $\sum_{\ell=0}^{r-1} e^{2\pi i \ell x/r} = r$ for x an integer multiple of r, and zero otherwise. The approximate equality in step 3 is required because 2^t may not be an integer multiple of r in general (it need not be: this is taken account of by the phase estimation bounds). By Equation (5.22), applying the inverse Fourier transform to the first register, in step 4, gives an estimate of the phase ℓ/r, where ℓ is chosen randomly. r can be efficiently obtained in the final step using a continued fraction expansion.

Box 5.5: The shift-invariance property of the Fourier transform

The Fourier transform, Equation (5.1), has an interesting and very useful property, known as shift invariance. Using notation which is useful in describing the general application of this property, let us describe the quantum Fourier transform as

$$\sum_{h \in H} \alpha_h |h\rangle \rightarrow \sum_{g \in G} \tilde{\alpha}_g |g\rangle, \tag{5.65}$$

where $\tilde{\alpha}_g = \sum_{h \in H} \alpha_h \exp(2\pi i g h/|G|)$, H is some subset of G, and G indexes the states in an orthonormal basis of the Hilbert space. For example, G may be the set of numbers from 0 to $2^n - 1$ for an n qubit system. $|G|$ denotes the number of elements in G. Suppose we apply to the initial state an operator U_k which performs the unitary transform

$$U_k |g\rangle = |g + k\rangle \tag{5.66}$$

then apply the Fourier transform. The result,

$$U_k \sum_{h\in H} \alpha_h |h\rangle = \sum_{h\in H} \alpha_h |h+k\rangle \rightarrow \sum_{g\in G} e^{2\pi igk/|G|} \tilde{\alpha}_g |g\rangle \tag{5.67}$$

has the property that the magnitude of the amplitude for $|g\rangle$ does not change, no matter what k is, that is: $|\exp(2\pi igk/|G|)\tilde{\alpha}_g| = |\tilde{\alpha}_g|$.
In the language of group theory, G is a group, H a subgroup of G, and we say that if a function f on G is constant on cosets of H, then the Fourier transform of f is invariant over cosets of H.

Why does this work? One way to understand this is to realize that (5.63) is approximately the Fourier transform over $\{0, 1, \ldots, 2^L - 1\}$ of $|f(x)\rangle$ (see Exercise 5.20), and the Fourier transform has an interesting and very useful property, known as shift invariance, described in Box 5.5. Another is to realize that what the order-finding algorithm does is just to find the period of the function $f(k) = x^k \bmod N$, so the ability to find the period of a general periodic function is not unexpected. Yet another way is to realize that the implementation of the black box U is naturally done using a certain unitary operator whose eigenvectors are precisely $|\hat{f}(\ell)\rangle$, as described in Exercise 5.21 below, so that the phase estimation procedure of Section 5.2 can be applied.

Exercise 5.20: Suppose $f(x+r) = f(x)$, and $0 \leq x < N$, for N an integer multiple of r. Compute

$$\hat{f}(\ell) \equiv \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{-2\pi i\ell x/N} f(x) \tag{5.68}$$

and relate the result to (5.63). You will need to use the fact that

$$\sum_{k\in\{0,r,2r,\ldots,N-r\}} e^{2\pi ik\ell/N} = \begin{cases} \sqrt{N/r} & \text{if } \ell \text{ is an integer multiple of } N/r \\ 0 & \text{otherwise.} \end{cases} \tag{5.69}$$

Exercise 5.21: (Period-finding and phase estimation) Suppose you are given a unitary operator U_y which performs the transformation $U_y|f(x)\rangle = |f(x+y)\rangle$, for the periodic function described above.
(1) Show that the eigenvectors of U_y are $|\hat{f}(\ell)\rangle$, and calculate their eigenvalues.
(2) Show that given $|f(x_0)\rangle$ for some x_0, U_y can be used to realize a black box which is as useful as U in solving the period-finding problem.

8.2.10 5.4.2 Discrete logarithms

The period finding problem we just considered is a simple one, in that the domain and range of the periodic function were integers. What happens when the function is more complex? Consider the function $f(x_1, x_2) = a^{sx_1+x_2} \bmod N$, where all the variables are integers, and r is the smallest positive integer for which $a^r \bmod N = 1$. This function is periodic, since $f(x_1 + \ell, x_2 - \ell s) = f(x_1, x_2)$, but now the period is a 2 -tuple, $(\ell, -\ell s)$, for integer ℓ. This may seem to be a strange function, but it is very useful in cryptography, since determining s allows one to solve what is known as the discrete logarithm problem: given a and $b = a^s$, what is s ? Here is a quantum algorithm which solves this problem using one query of a quantum black box U which performs the unitary transform $U|x_1\rangle|x_2\rangle|y\rangle \rightarrow |x_1\rangle|x_2\rangle|y \oplus f(x)\rangle$ (where $\oplus$ denotes bitwise addition modulo 2), and $O(\lceil \log r \rceil^2)$ other operations. We assume knowledge of the minimum $r > 0$ such that $a^r \bmod N = 1$, which can be obtained using the order-finding algorithm described previously.

Algorithm: Discrete logarithm

Inputs: (1) A black box which performs the operation $U|x_1\rangle|x_2\rangle|y\rangle = |x_1\rangle|x_2\rangle|y \oplus f(x_1,x_2)\rangle$, for $f(x_1,x_2) = b^{x_1}a^{x_2}$, (2) a state to store the function evaluation, initialized to $|0\rangle$, and (3) two $t = O(\lceil \log r \rceil + \log(1/\epsilon))$ qubit registers initialized to $|0\rangle$.

Outputs: The least positive integer s such that $a^s = b$.

Runtime: One use of U, and $O(\lceil \log r \rceil^2)$ operations. Succeeds with probability $O(1)$.

Procedure:

1. $|0\rangle|0\rangle|0\rangle$
2. $\rightarrow \frac{1}{2^t}\sum_{x_1=0}^{2^t-1}\sum_{x_2=0}^{2^t-1}|x_1\rangle|x_2\rangle|0\rangle$ create superposition
3. $\rightarrow \frac{1}{2^t}\sum_{x_1=0}^{2^t-1}\sum_{x_2=0}^{2^t-1}|x_1\rangle|x_2\rangle|f(x_1,x_2)\rangle$ apply U

$$\approx \frac{1}{2^t\sqrt{r}}\sum_{\ell_2=0}^{r-1}\sum_{x_1=0}^{2^t-1}\sum_{x_2=0}^{2^t-1} e^{2\pi i(s\ell_2 x_1 + \ell_2 x_2)/r}|x_1\rangle|x_2\rangle\left|\hat{f}(s\ell_2,\ell_2)\right\rangle$$

$$= \frac{1}{2^t\sqrt{r}}\sum_{\ell_2=0}^{r-1}\left[\sum_{x_1=0}^{2^t-1} e^{2\pi i(s\ell_2 x_1)/r}|x_1\rangle\right]\left[\sum_{x_2=0}^{2^t-1} e^{2\pi i(\ell_2 x_2)/r}|x_2\rangle\right]\left|\hat{f}(s\ell_2,\ell_2)\right\rangle$$

4. $\rightarrow \frac{1}{\sqrt{r}}\sum_{\ell_2=0}^{r-1}\left|\widetilde{s\ell_2/r}\right\rangle\left|\widetilde{\ell_2/r}\right\rangle\left|\hat{f}(s\ell_2,\ell_2)\right\rangle$ apply inverse Fourier transform to first two registers
5. $\rightarrow \left(\widetilde{s\ell_2/r}, \widetilde{\ell_2/r}\right)$ measure first two registers
6. $\rightarrow s$ apply generalized continued fractions algorithm

apply generalized co
fractions algorithm

Again, the key to understanding this algorithm is step 3, in which we introduce the state

$$\left|\hat{f}(\ell_1,\ell_2)\right\rangle = \frac{1}{\sqrt{r}}\sum_{j=0}^{r-1} e^{-2\pi i\ell_2 j/r}|f(0,j)\rangle \tag{5.70}$$

the Fourier transform of $|f(x_1,x_2)\rangle$ (see Exercise 5.22). In this equation, the values of ℓ_1 and ℓ_2 must satisfy

$$\sum_{k=0}^{r-1} e^{2\pi ik(\ell_1/s - \ell_2)/r} = r \tag{5.71}$$

Otherwise, the amplitude of $\left|\hat{f}(\ell_1,\ell_2)\right\rangle$ is nearly zero. The generalized continued fraction expansion used in the final step to determine s is analogous to the procedures used in Section 5.3.1, and is left as a simple exercise for you to construct.

Exercise 5.22: Show that

$$\left|\hat{f}\left(\ell_1,\ell_2\right)\right\rangle = \sum_{x_1=0}^{r-1}\sum_{x_2=0}^{r-1} e^{-2\pi i(\ell_1 x_1+\ell_2 x_2)/r}\left|f\left(x_1,x_2\right)\right\rangle = \frac{1}{\sqrt{r}}\sum_{j=0}^{r-1} e^{-2\pi i \ell_2 j/r}|f(0,j)\rangle, \tag{5.72}$$

and we are constrained to have $\ell_1/s - \ell_2$ be an integer multiple of r for this expression to be non-zero.

Exercise 5.23: Compute

$$\frac{1}{r}\sum_{\ell_1=0}^{r-1}\sum_{\ell_2=0}^{r-1} e^{-2\pi i(\ell_1 x_1+\ell_2 x_2)/r}\left|\hat{f}\left(\ell_1,\ell_2\right)\right\rangle \tag{5.73}$$

using (5.70), and show that the result is $f\left(x_1,x_2\right)$.

Exercise 5.24: Construct the generalized continued fractions algorithm needed in step 6 of the discrete logarithm algorithm to determine s from estimates of $s\ell_2/r$ and ℓ_2/r.

Exercise 5.25: Construct a quantum circuit for the black box U used in the quantum discrete logarithm algorithm, which takes a and b as parameters, and performs the unitary transform $|x_1\rangle|x_2\rangle|y\rangle \rightarrow |x_1\rangle|x_2\rangle|y \oplus b^{x_1}a^{x_2}\rangle$. How many elementary operations are required?

8.2.11 5.4.3 The hidden subgroup problem

By now, a pattern should be coming clear: if we are given a periodic function, even when the structure of the periodicity is quite complicated, we can often use a quantum algorithm to determine the period efficiently. Importantly, however, not all periods of periodic functions can be determined. The general problem which defines a broad framework for these questions can be succinctly expressed in the language of group theory (see Appendix 2 for a quick review) as follows:

> Let f be a function from a finitely generated group G to a finite set X such that f is constant on the cosets of a subgroup K, and distinct on each coset. Given a quantum black box for performing the unitary transform $U|g\rangle|h\rangle = |g\rangle|h \oplus f(g)\rangle$, for $g \in G, h \in X$, and $\oplus$ an appropriately chosen binary operation on X, find a generating set for K.

Order-finding, period-finding, discrete logarithms, and many other problems are instances of this hidden subgroup problem; some interesting ones are listed in Figure 5.5.

For G a finite *Abelian* group, a quantum computer can solve the hidden subgroup problem using a number of operations polynomial in $\log|G|$, and one use of the black box function evaluation, using an algorithm very similar to the others in this section. (In fact, solution for a finitely generated Abelian group is also possible, along similar lines, but we'll stick to the finite case here.) We shall leave detailed specification of the algorithm to you as an exercise, which should be simple after we explain the basic idea. Many things remain essentially the same, because finite Abelian groups are isomorphic to products of additive groups over the integers in modular arithmetic. This means that the quantum Fourier transform of f over G is well defined (see Section A2.3), and can still be done efficiently. The first non-trivial step of the algorithm is to use a Fourier transform (generalizing the Hadamard operation) to create a superposition over group elements, which is then transformed by applying the quantum black box for f in the next step, to give

$$\frac{1}{\sqrt{|G|}}\sum_{g\in G}|g\rangle|f(g)\rangle. \tag{5.74}$$

As before, we would now like to rewrite $|f(g)\rangle$ in the Fourier basis. We start with

$$|f(g)\rangle = \frac{1}{\sqrt{|G|}} \sum_{\ell=0}^{|G|-1} e^{2\pi i \ell g/|G|} |\hat{f}(\ell)\rangle, \tag{5.75}$$

where we have chosen $\exp[-2\pi i \ell g/|G|]$ as a representation (see Exercise A2.13) of $g \in G$ indexed by ℓ (the Fourier transform maps between group elements and representations: see Exercise A2.23). The key is to recognize that this expression can be simplified because

Name	G	X	K	Function
Deutsch	$\{0,1\}, \oplus$	{0,1}	$\{0\}$ or $\{0,1\}$	$K = \{0,1\} : \begin{cases} f(x) = \\ f(x) = \end{cases}$ $K = \{0\} : \begin{cases} f(x) = x \\ f(x) = 1 \end{cases}$
Simon	$\{0,1\}^n, \oplus$	any finite set	$\{0, s\}$ $s \in \{0,1\}^n$	$f(x \oplus s) = f(x)$
Periodfinding	Z, +	any finite set	$\{0, r, 2r, \ldots\}$ $r \in G$	$f(x + r) = f(x)$
Orderfinding	Z, +	$\{a^j\}$ $j \in Z_r$ $a^r = 1$	$\{0, r, 2r, \ldots\}$ $r \in G$	$f(x) = a^x$ $f(x + r) = f(x)$
Discrete logarithm	$\mathbf{Z}_r \times \mathbf{Z}_r$ $+(\mathrm{mod} r)$	$\{a^j\}$ $j \in Z_r a^r = 1$	$(\ell, -\ell s)$ $\ell, s \in \mathbf{Z}_r$	$f(x_1, x_2) = a^{kx_1 + x_2}$ $f(x_1 + \ell, x_2 - \ell s) = f$
Order of a permutation	$\mathbf{Z}_{2^m} \times \mathbf{Z}_{2^n}$ $+ (\mathrm{mod} 2^m)$	$\mathbf{Z}_{2^n}$	$\{0, r, 2r, \ldots\}$ $r \in X$	$f(x, y) = \pi^x(y)$ $f(x + r, y) = f(x, y)$ $\pi =$ permutation on X
Hidden linear function	$\mathbf{Z} \times \mathbf{Z}, +$	Z_N	$(\ell, -\ell s)$ $\ell, s \in X$	$f(x_1, x_2) =$ $\pi(sx_1 + x_2 \bmod N)$ $\pi =$ permutation on X
Abelian stabilizer	(H, N) $H =$ any Abelian group	any finite set	$\{s \in H$ $f(s, x) = x,$ $\forall x \in X\}$	$f(gh, x) = f(g, f(h, x))$ $f(gs, x) = f(g, x)$

Figure 5.5. Hidden subgroup problems. The function f maps from the group G to the finite set X, and is promised to be constant on cosets of the hidden subgroup \$K \subseteq G . \mathbf{Z _{N}\$ represents the set $\{0, 1, \ldots, N-1\}$ in this table, and $\mathbf{Z}$ is the integers. The problem is to find K (or a generating set for it), given a black box for f.}

f is constant and distinct on cosets of the subgroup K, so that

$$|\hat{f}(\ell)\rangle = \frac{1}{\sqrt{|G|}} \sum_{g \in G} e^{-2\pi i \ell g/|G|} |f(g)\rangle \tag{5.76}$$

has nearly zero amplitude for all values of ℓ except those which satisfy

$$\sum_{h \in K} e^{-2\pi i \ell h/|G|} = |K|. \tag{5.77}$$

If we can determine ℓ, then using the linear constraints given by this expression allows us to determine elements of K, and since K is Abelian, this allows us to eventually determine a generating set for the whole hidden subgroup, solving the problem.

However, life is not so simple. An important reason why the period-finding and discrete logarithm algorithms work is because of the success of the continued fraction expansion in obtaining ℓ from $\ell/|G|$. In those problems, ℓ and $|G|$ are arranged to not have any common factors, with high probability. In the general case, however, this may not be true, since $|G|$ is free to be a composite number with many factors, and we have no useful prior information about ℓ.

Fortunately, this problem can be solved: as mentioned above, any finite Abelian group G is isomorphic to a product of cyclic groups of prime power order, that is, $G = \mathbf{Z}_{p_1} \times \mathbf{Z}_{p_2} \times \cdots \times \mathbf{Z}_{p_M}$, where p_i are primes, and $\mathbf{Z}_{p_i}$ is the group over integers $\{0, 1, \ldots, p_i - 1\}$ with addition modulo p_i being the group operation. We can thus re-express the phase which appears in (5.75) as

$$e^{2\pi i \ell g/|G|} = \prod_{i=1}^{M} e^{2\pi i \ell'_i g_i/p_i} \tag{5.78}$$

for $g_i \in \mathbf{Z}_{p_i}$. The phase estimation procedure now gives us ℓ'_i, from which we determine ℓ, and thus, sample K as described above, to solve the hidden subgroup problem.

Exercise 5.26: Since K is a subgroup of G, when we decompose G into a product of cyclic groups of prime power order, this also decomposes K. Re-express (5.77) to show that determining ℓ'_i allows one to sample from the corresponding cyclic subgroup K_{p_i} of K.

Exercise 5.27: Of course, the decomposition of a general finite Abelian group G into a product of cyclic groups of prime power order is usually a difficult problem (at least as hard as factoring integers, for example). Here, quantum algorithms come to the rescue again: explain how the algorithms in this chapter can be used to efficiently decompose G as desired.

Exercise 5.28: Write out a detailed specification of the quantum algorithm to solve the hidden subgroup problem, complete with runtime and success probability estimates, for finite Abelian groups.

Exercise 5.29: Give quantum algorithms to solve the Deutsch and Simon problems listed in Figure 5.5, using the framework of the hidden subgroup problem.

8.2.12 5.4.4 Other quantum algorithms?

One of the most intriguing aspects of this framework for describing quantum algorithms in terms of the hidden subgroup problem is the suggestion that more difficult problems might be solvable by considering various groups G and functions f. We have only described the solution of this problem for Abelian groups. What about non-Abelian groups? They are quite interesting (see Appendix 2 for a discussion of general Fourier transforms over non-Abelian groups): for example, the problem of graph isomorphism is to determine if two given graphs are the same under some permutation of the labels of the n vertices (Section 3.2.3). These permutations can be described as transformations under the symmetric group S_n, and algorithms for performing fast Fourier transforms
over these groups exists. However, a quantum algorithm for efficiently solving the graph isomporphism problem remains unknown.

Even if more general cases of the hidden subgroup problem remain unsolvable by quantum computers, having this unifying framework is useful, because it allows us to ask questions about how one might be able to step outside its limitations. It is difficult to believe that all fast quantum algorithms that will ever be discovered will be just ways to solve the hidden subgroup problem. If one thinks of these problems as being based on the coset invariance property of the Fourier transform, in searching for new algorithms, perhaps the thing to do then is to

investigate other transforms with different invariances. Going in another direction, one might ask: what difficult hidden subgroup problems might be efficiently solved given an arbitrary (but specified independently of the problem) quantum state as a helper? After all, as discussed in Chapter 4, most quantum states are actually exponentially hard to construct. Such a state might be a useful resource (a real 'quantum oracle'), if quantum algorithms existed to utilize them to solve hard problems!

The hidden subgroup problem also captures an important constraint underlying the class of quantum algorithms which are exponentially faster than their (known) classical counterparts: this is a promise problem, meaning that it is of the form ' $F(X)$ is promised to have such and such property: characterize that property.' Rather disappointingly, perhaps, we shall show at the end of the next chapter that, in solving problems without some sort of promise, quantum computers cannot achieve an exponential speedup over classical computers; the best speedup is polynomial. On the other hand, this gives us an important clue as to what kinds of problems quantum computers might be good at: in retrospect, the hidden subgroup problem might be thought of as a natural candidate for quantum computation. What other natural problems are there? Think about it!

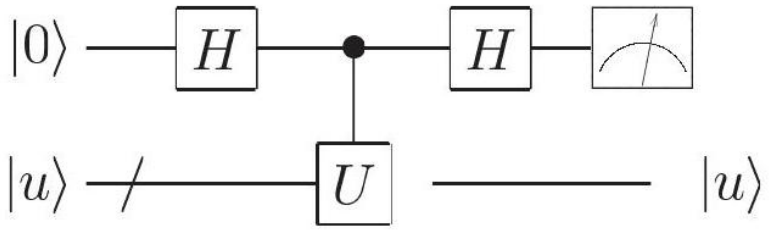
Problem 5.1: Construct a quantum circuit to perform the quantum Fourier transform

$$|j\rangle \longrightarrow \frac{1}{\sqrt{p}} \sum_{k=0}^{p-1} e^{2\pi i j k/p} |k\rangle \tag{5.79}$$

where p is prime.

Problem 5.2: (Measured quantum Fourier transform) Suppose the quantum Fourier transform is performed as the last step of a quantum computation, followed by a measurement in the computational basis. Show that the combination of quantum Fourier transform and measurement is equivalent to a circuit consisting entirely of one qubit gates and measurement, with classical control, and no two qubit gates. You may find the discussion of Section 4.4 useful.

Problem 5.3: (Kitaev's algorithm) Consider the quantum circuit



where $|u\rangle$ is an eigenstate of U with eigenvalue $e^{2\pi i\varphi}$. Show that the top qubit is measured to be 0 with probability $p \equiv \cos^2(\pi\varphi)$. Since the state $|u\rangle$ is unaffected by the circuit it may be reused; if U can be replaced by U^k, where k is an arbitrary integer under your control, show that by repeating this circuit and increasing k appropriately, you can efficiently obtain as many bits of p as desired, and thus, of φ. This is an alternative to the phase estimation algorithm.

Problem 5.4: The runtime bound $O(L^3)$ we have given for the factoring algorithm is not tight. Show that a better upper bound of $O(L^2 \log L \log\log L)$ operations can be achieved.

Problem 5.5: (Non-Abelian hidden subgroups - Research) Let f be a function on a finite group G to an arbitrary finite range X, which is promised to be constant and distinct on distinct left cosets of a subgroup K. Start with the state

$$\frac{1}{\sqrt{|G|^m}} \sum_{g_1,\ldots,g_m} |g_1,\ldots,g_m\rangle\, |f(g_1),\ldots,f(g_m)\rangle \tag{5.80}$$

and prove that picking $m = 4\log|G| + 2$ allows K to be identified with probability at least $1 - 1/|G|$. Note that G does not necessarily have to be Abelian, and being able to perform

a Fourier transform over G is not required. This result shows that one can produce (using only $O(\log|G|)$ oracle calls) a final result in which the pure state outcomes corresponding to different possible hidden subgroups are nearly orthogonal. However, it is unknown whether a POVM exists or not which allows the hidden subgroup to be identified efficiently (i.e. using poly($\log|G|$) operations) from this final state.

Problem 5.6: (Addition by Fourier transforms) Consider the task of constructing a quantum circuit to compute $|x\rangle \rightarrow |x+y \bmod 2^n\rangle$, where y is a fixed constant, and $0 \leq x < 2^n$. Show that one efficient way to do this, for values of y such as 1, is to first perform a quantum Fourier transform, then to apply single qubit phase shifts, then an inverse Fourier transform. What values of y can be added easily this way, and how many operations are required?

8.2.13 Summary of Chapter 5: The quantum Fourier transform and its applications

- When $N = 2^n$ the quantum Fourier transform

$$|j\rangle = |j_1, \ldots, j_n\rangle \longrightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i \frac{jk}{N}} |k\rangle \tag{5.81}$$

may be written in the form

$$|j\rangle \rightarrow \frac{1}{2^{n/2}} \left(|0\rangle + e^{2\pi i 0.j_n}|1\rangle\right) \left(|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle\right) \ldots \left(|0\rangle + e^{2\pi i 0.j_1 j_2 \ldots j_n}|1\rangle\right), \tag{5.82}$$

and may be implemented using $\Theta(n^2)$ gates.

- Phase estimation: Let $|u\rangle$ be an eigenstate of the operator U with eigenvalue $e^{2\pi i\varphi}$. Starting from the initial state $|0\rangle^{\otimes t}|u\rangle$, and given the ability to efficiently perform U^{2^k} for integer k, this algorithm (shown in Figure 5.3) can be used to efficiently obtain the state $|\tilde{\varphi}\rangle|u\rangle$, where $\tilde{\varphi}$ accurately approximates φ to $t - \left\lceil \log\left(2 + \frac{1}{2\epsilon}\right)\right\rceil$ bits with probability at least $1 - \epsilon$.

- Order-finding: The order of x modulo N is the least positive integer r such that $x^r \bmod N = 1$. This number can be computed in $O(L^3)$ operations using the quantum phase estimation algorithm, for L-bit integers x and N.

- Factoring: The prime factors of an L-bit integer N can be determined in $O(L^3)$ operations by reducing this problem to finding the order of a random number x co-prime with N.

- Hidden subgroup problem: All the known fast quantum algorithms can be described as solving the following problem: Let f be a function from a finitely generated group G to a finite set X such that f is constant on the cosets of a subgroup K, and distinct on each coset. Given a quantum black box for performing the unitary transform $U|g\rangle|h\rangle = |g\rangle|h \oplus f(g)\rangle$, for $g \in G$ and $h \in X$, find a generating set for K.

History and further reading

The definition of the Fourier transform may be generalized beyond what we have considered in this chapter. In the general scenario a Fourier transform is defined on a set of complex numbers α_g, where the index g is chosen from some group, G. In this chapter we have chosen G to be the additive group of integers modulo 2^n, often denoted $\mathbf{Z}_{2^n}$. Deutsch [Deu85] showed that

the Fourier transform over the group $\mathbf{Z}_2^n$ could be implemented efficiently on a quantum computer - this is the Hadamard transform of earlier chapters. Shor [*Sho*94] realized to spectacular effect that quantum computers could efficiently implement the quantum Fourier transform over groups $\mathbf{Z}_m$ for certain special values of m. Inspired by this result Coppersmith [Cop94] , Deutsch (unpublished), and Cleve (unpublished) gave the simple quantum circuits for computing the quantum Fourier transform over $\mathbf{Z}_{2^n}$ which we have used in this chapter. Cleve, Ekert, Macchiavello and Mosca [CEMM98] and Griffiths and Niu [GN96] independently discovered the product formula (5.4); in fact, this result had been realized much earlier by Danielson and Lanczos. The simplified proof starting in Equation (5.5) was suggested by Zhou. Griffiths and Niu [GN96] are responsible for the measured quantum Fourier transform found in Problem 5.2.

The Fourier transform over $\mathbf{Z}_{2^n}$ was generalized to obtain a Fourier transform over an arbitrary finite Abelian group by Kitaev [Kit95], who also introduced the phase estimation procedure in the form given in Problem 5.3. Cleve, Ekert, Macchiavello and Mosca[CEMM98] also integrated several of the techniques of Shor and Kitaev into one nice picture, upon which Section 5.2 is based. A good description of the phase estimation algorithm can be found in Mosca's Ph.D. thesis [Mos99].

Shor announced the quantum order-finding algorithm in a seminal paper in 1994[Sho94], and noted that the problems of performing discrete logarithms and factoring could be reduced to order-finding. The final paper, including extended discussion and references, was published in 1997[Sho97]. This paper also contains a discussion of clever multiplication methods that may be used to speed up the algorithm even further than in our description, which uses relatively naive multiplication techniques. With these faster multiplication methods the resources required to factor a composite integer n scale as $O\left(n^2 \log n \log\log n\right)$, as claimed in the introduction to the chapter. In 1995 Kitaev[Kit95] announced an algorithm for finding the stabilizer of a general Abelian group, which he showed could be used to solve discrete logarithm and factoring as special cases. In addition, this algorithm contained several elements not present in Shor's algorithm. A good review of the factoring algorithm was written by Ekert and Jozsa [EJ96] ; also see DiVincenzo [DiV95a]. The discussion of continued fractions is based upon Chapter 10 of Hardy and Wright [HW60]. At the time of writing, the most efficient classical algorithm for factoring on a classical computer is the number field sieve. This is described in a collection edited by A. K. Lenstra and H. W. Lenstra, Jr. [LL93].

The generalization of quantum algorithms to solving the hidden subgroup problem has been considered by many authors. Historically, Simon was first to note that a quantum computer could find a hidden period of a function satisfying $f(x \oplus s) = f(x)$[Sim 94,Sim 97]. In fact, Shor found his result by generalizing Simon's result, and by applying a Fourier transform over $\mathbf{Z}_N$ instead of Simon's Hadamard transforms (a Fourier transform over $\mathbf{Z}_2^k$). Boneh and Lipton then noted the connection to the hidden subgroup problem, and described a quantum algorithm for solving the hidden linear function problem [BL95]. Jozsa was the first to explicitly provide a uniform description of the Deutsch-Jozsa, Simon, and Shor algorithms in terms of the hidden subgroup problem[Joz97]. Ekert and Jozsa's work in studying the role of the Abelian and non-Abelian Fast Fourier Transform algorithms in speedup of quantum algorithms [EJ98] has also been insightful. Our description of the hidden subgroup problem in Section 5.4 follows the framework of Mosca and Ekert[ME99, Mos99]. Cleve has proven that the problem of finding an order of a permutation requires an exponential number of queries for a bounded-error probabilistic classical computer [Cle99] . Generalizations of this method to beyond Abelian groups have been attempted by Ettinger and Høyer [EH99], by Roetteler and Beth [RB98] and Pueschel, Roetteler, and Beth [PRB98], by Beals, who also described constructions of quantum Fourier transforms over the symmetric group [BBC+98], and by Ettinger, Høyer, and Knill [EHK99]. These results have shown, so far, that there exists a quantum algorithm to solve the hidden subgroup problem for non-Abelian groups using only $O(\log |G|)$ oracle calls, but whether

this can be realized in polynomial time is unknown (Problem 5.5).

8.3 6 Quantum search algorithms

Suppose you are given a map containing many cities, and wish to determine the shortest route passing through all cities on the map. A simple algorithm to find this route is to search all possible routes through the cities, keeping a running record of which route has the shortest length. On a classical computer, if there are N possible routes, it obviously takes $O(N)$ operations to determine the shortest route using this method. Remarkably, there is a quantum search algorithm, sometimes known as Grover's algorithm, which enables this search method to be sped up substantially, requiring only $O(\sqrt{N})$ operations. Moreover, the quantum search algorithm is general in the sense that it can be applied far beyond the route-finding example just described to speed up many (though not all) classical algorithms that use search heuristics.

In this chapter we explain the fast quantum search algorithm. The basic algorithm is described in Section 6.1. In Section 6.2 we derive the algorithm from another point of view, based on the quantum simulation algorithm of Section 4.7. Three important applications of this algorithm are also described: quantum counting in Section 6.3, speedup of solution of NP-complete problems in Section 6.4, and search of unstructured databases in Section 6.5. One might hope to improve upon the search algorithm to do even better than a square root speedup but, as we show in Section 6.6, it turns out this is not possible. We conclude in Section 6.7 by showing that this speed limit applies to most unstructured problems.

8.3.1 6.1 The quantum search algorithm

Let us begin by setting the stage for the search algorithm in terms of an oracle, similar to that encountered in Section 3.1.1. This allows us to present a very general description of the search procedure, and a geometric way to visualize its action and see how it performs.

8.3.2 6.1.1 The oracle

Suppose we wish to search through a search space of N elements. Rather than search the elements directly, we concentrate on the index to those elements, which is just a number in the range 0 to $N-1$. For convenience we assume $N = 2^n$, so the index can be stored in n bits, and that the search problem has exactly M solutions, with $1 \leq M \leq N$. A particular instance of the search problem can conveniently be represented by a function f, which takes as input an integer x, in the range 0 to $N-1$. By definition, $f(x) = 1$ if x is a solution to the search problem, and $f(x) = 0$ if x is not a solution to the search problem.

Suppose we are supplied with a quantum oracle - a black box whose internal workings we discuss later, but which are not important at this stage - with the ability to recognize solutions to the search problem. This recognition is signalled by making use of an oracle
qubit. More precisely, the oracle is a unitary operator, O, defined by its action on the computational basis:

$$|x\rangle|q\rangle \xrightarrow{O} |x\rangle|q \oplus f(x)\rangle, \tag{6.1}$$

where $|x\rangle$ is the index register, $\oplus$ denotes addition modulo 2 , and the oracle qubit $|q\rangle$ is a single qubit which is flipped if $f(x) = 1$, and is unchanged otherwise. We can check whether x is a solution to our search problem by preparing $|x\rangle|0\rangle$, applying the oracle, and checking to see if the oracle qubit has been flipped to $|1\rangle$.

In the quantum search algorithm it is useful to apply the oracle with the oracle qubit initially in the state $(|0\rangle - |1\rangle)/\sqrt{2}$, just as was done in the Deutsch-Jozsa algorithm of Section 1.4.4.

If x is not a solution to the search problem, applying the oracle to the state $|x\rangle(|0\rangle - |1\rangle)/\sqrt{2}$ does not change the state. On the other hand, if x is a solution to the search problem, then $|0\rangle$ and $|1\rangle$ are interchanged by the action of the oracle, giving a final state $-|x\rangle(|0\rangle - |1\rangle)/\sqrt{2}$. The action of the oracle is thus:

$$|x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \stackrel{O}{\rightarrow} (-1)^{f(x)} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \tag{6.2}$$

Notice that the state of the oracle qubit is not changed. It turns out that this remains $(|0\rangle - |1\rangle)/\sqrt{2}$ throughout the quantum search algorithm, and can therefore be omitted from further discussion of the algorithm, simplifying our description.

With this convention, the action of the oracle may be written:

$$|x\rangle \stackrel{O}{\rightarrow} (-1)^{f(x)} |x\rangle. \tag{6.3}$$

We say that the oracle marks the solutions to the search problem, by shifting the phase of the solution. For an N item search problem with M solutions, it turns out that we need only apply the search oracle $O(\sqrt{N/M})$ times in order to obtain a solution, on a quantum computer.

This discussion of the oracle without describing how it works in practice is rather abstract, and perhaps even puzzling. It seems as though the oracle already knows the answer to the search problem; what possible use could it be to have a quantum search algorithm based upon such oracle consultations?! The answer is that there is a distinction between knowing the solution to a search problem, and being able to recognize the solution; the crucial point is that it is possible to do the latter without necessarily being able to do the former.

A simple example to illustrate this is the problem of factoring. Suppose we have been given a large number, m, and told that it is a product of two primes, p and q - the same sort of situation as arises in trying to break the RSA public key cryptosystem (Appendix 5). To determine p and q, the obvious method on a classical computer is to search all numbers from 2 through $m^{1/2}$ for the smaller of the two prime factors. That is, we successively do a trial division of m by each number in the range 2 to $m^{1/2}$, until we find the smaller prime factor. The other prime factor can then be found by dividing m by the smaller prime. Obviously, this search-based method requires roughly $m^{1/2}$ trial divisions to find a factor on a classical computer.

The quantum search algorithm can be used to speed up this process. By definition, the action of the oracle upon input of the state $|x\rangle$ is to divide m by x, and check to see if the division is exact, flipping the oracle qubit if this is so. Applying the quantum search algorithm with this oracle yields the smaller of the two prime factors with high probability.

But to make the algorithm work, we need to construct an efficient circuit implementing the oracle. How to do this is an exercise in the techniques of reversible computation. We begin by defining the function $f(x) \equiv 1$ if x divides m, and $f(x) = 0$ otherwise; $f(x)$ tells us whether the trial division is successful or not. Using the techniques of reversible computation discussed in Section 3.2.5, construct a classical reversible circuit which takes (x, q) - representing an input register initially set to x and a one bit output register initially set to $q-$ to $(x, q \oplus f(x))$, by modifying the usual (irreversible) classical circuit for doing trial division. The resource cost of this reversible circuit is the same to within a factor two as the irreversible classical circuit used for trial division, and therefore we regard the two circuits as consuming essentially the same resources. Furthermore, the classical reversible circuit can be immediately translated into a quantum circuit that takes $|x\rangle|q\rangle$ to $|x\rangle|q \oplus f(x)\rangle$, as required of the oracle. The key point is that even without knowing the prime factors of m, we can explicitly construct an oracle which recognizes a solution to the search problem when it sees one. Using this oracle and the quantum search algorithm we can search the range 2 to $m^{1/2}$ using $O\left(m^{1/4}\right)$ oracle consultations. That

is, we need only perform the trial division roughly $m^{1/4}$ times, instead of $m^{1/2}$ times, as with the classical algorithm!

The factoring example is conceptually interesting but not practical: there are classical algorithms for factoring which work much faster than searching through all possible divisors. However, it illustrates the general way in which the quantum search algorithm may be applied: classical algorithms which rely on search-based techniques may be sped up using the quantum search algorithm. Later in this chapter we examine scenarios where the quantum search algorithm offers a genuinely useful aid in speeding up the solution of NP-complete problems.

8.3.3 6.1.2 The procedure

Schematically, the search algorithm operates as shown in Figure 6.1. The algorithm proper makes use of a single n qubit register. The internal workings of the oracle, including the possibility of it needing extra work qubits, are not important to the description of the quantum search algorithm proper. The goal of the algorithm is to find a solution to the search problem, using the smallest possible number of applications of the oracle.

The algorithm begins with the computer in the state $|0\rangle^{\otimes n}$. The Hadamard transform is used to put the computer in the equal superposition state,

$$|\psi\rangle = \frac{1}{N^{1/2}} \sum_{x=0}^{N-1} |x\rangle \tag{6.4}$$

The quantum search algorithm then consists of repeated application of a quantum subroutine, know as the Grover iteration or Grover operator, which we denote G. The Grover iteration, whose quantum circuit is illustrated in Figure 6.2, may be broken up into four steps:
(1) Apply the oracle O.
(2) Apply the Hadamard transform $H^{\otimes n}$.
(3) Perform a conditional phase shift on the computer, with every computational basis state except $|0\rangle$ receiving a phase shift of -1 ,

$$|x\rangle \rightarrow -(-1)^{\delta_{x0}}|x\rangle \tag{6.5}$$

(4) Apply the Hadamard transform $H^{\otimes n}$.

Exercise 6.1: Show that the unitary operator corresponding to the phase shift in the Grover iteration is $2|0\rangle\langle 0| - I$.

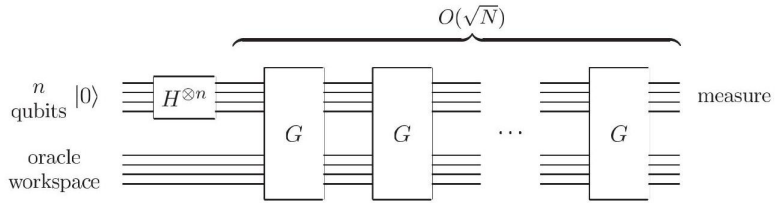


Figure 6.1. Schematic circuit for the quantum search algorithm. The oracle may employ work qubits for its implementation, but the analysis of the quantum search algorithm involves only the n qubit register.

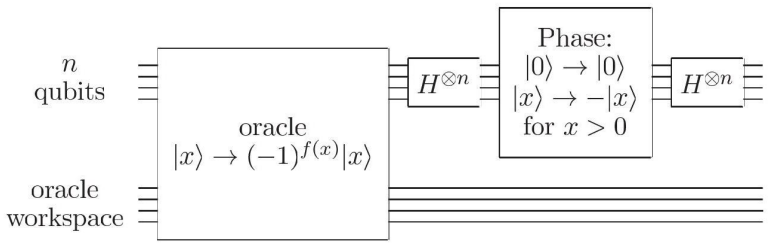


Figure 6.2. Circuit for the Grover iteration, G.

Each of the operations in the Grover iteration may be efficiently implemented on a quantum computer. Steps 2 and 4, the Hadamard transforms, require $n = \log(N)$ operations each. Step 3, the conditional phase shift, may be implemented using the techniques of Section 4.3, using $O(n)$ gates. The cost of the oracle call depends upon the specific application; for now, we merely need note that the Grover iteration requires only a single oracle call. It is useful to note that the combined effect of steps 2,3 , and 4 is

$$H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n} = 2|\psi\rangle\langle\psi| - I, \tag{6.6}$$

where $|\psi\rangle$ is the equally weighted superposition of states, (6.4). Thus the Grover iteration, G, may be written $G = (2|\psi\rangle\langle\psi| - I)O$.

Exercise 6.2: Show that the operation $(2|\psi\rangle\langle\psi| - I)$ applied to a general state $\sum_k \alpha_k|k\rangle$ produces

$$\sum_k \left[-\alpha_k + 2\langle\alpha\rangle\right]|k\rangle, \tag{6.7}$$

where $\langle\alpha\rangle \equiv \sum_k \alpha_k/N$ is the mean value of the α_k. For this reason, $(2|\psi\rangle\langle\psi| - I)$ is sometimes referred to as the inversion about mean operation.

8.3.4 6.1.3 Geometric visualization

What does the Grover iteration do? We have noted that $G = (2|\psi\rangle\langle\psi| - I)O$. In fact, we will show that the Grover iteration can be regarded as a rotation in the two-dimensional space spanned by the starting vector $|\psi\rangle$ and the state consisting of a uniform superposition of solutions to the search problem. To see this it is useful to adopt the convention that $\sum_x'$ indicates a sum over all x which are solutions to the search problem, and $\sum_x''$ indicates a sum over all x which are not solutions to the search problem. Define normalized states

$$|\alpha\rangle \equiv \frac{1}{\sqrt{N-M}} \sum_x'' |x\rangle \tag{6.8}$$

$$|\beta\rangle \equiv \frac{1}{\sqrt{M}} \sum_x' |x\rangle \tag{6.9}$$

Simple algebra shows that the initial state $|\psi\rangle$ may be re-expressed as

$$|\psi\rangle = \sqrt{\frac{N-M}{N}}|\alpha\rangle + \sqrt{\frac{M}{N}}|\beta\rangle, \tag{6.10}$$

so the initial state of the quantum computer is in the space spanned by $|\alpha\rangle$ and $|\beta\rangle$.
The effect of G can be understood in a beautiful way by realizing that the oracle operation

O performs a reflection about the vector $|\alpha\rangle$ in the plane defined by $|\alpha\rangle$ and $|\beta\rangle$. That is, $O(a|\alpha\rangle + b|\beta\rangle) = a|\alpha\rangle - b|\beta\rangle$. Similarly, $2|\psi\rangle\langle\psi| - I$ also performs a reflection in the plane defined by $|\alpha\rangle$ and $|\beta\rangle$, about the vector $|\psi\rangle$. And the product of two reflections is a rotation! This tells us that the state $G^k|\psi\rangle$ remains in the space spanned by $|\alpha\rangle$ and $|\beta\rangle$ for all k. It also gives us the rotation angle. Let $\cos\theta/2 = \sqrt{(N-M)/N}$, so that $|\psi\rangle = \cos\theta/2|\alpha\rangle + \sin\theta/2|\beta\rangle$. As Figure 6.3 shows, the two reflections which comprise G take $|\psi\rangle$ to

$$G|\psi\rangle = \cos\frac{3\theta}{2}|\alpha\rangle + \sin\frac{3\theta}{2}|\beta\rangle, \tag{6.11}$$

so the rotation angle is in fact θ. It follows that continued application of G takes the state to

$$G^k|\psi\rangle = \cos\left(\frac{2k+1}{2}\theta\right)|\alpha\rangle + \sin\left(\frac{2k+1}{2}\theta\right)|\beta\rangle. \tag{6.12}$$

Summarizing, G is a rotation in the two-dimensional space spanned by $|\alpha\rangle$ and $|\beta\rangle$, rotating the space by θ radians per application of G. Repeated application of the Grover iteration rotates the state vector close to $|\beta\rangle$. When this occurs, an observation in the computational basis produces with high probability one of the outcomes superposed in $|\beta\rangle$, that is, a solution to the search problem! An example illustrating the search algorithm with $N = 4$ is given in Box 6.1.

Exercise 6.3: Show that in the $|\alpha\rangle, |\beta\rangle$ basis, we may write the Grover iteration as

$$G = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \tag{6.13}$$

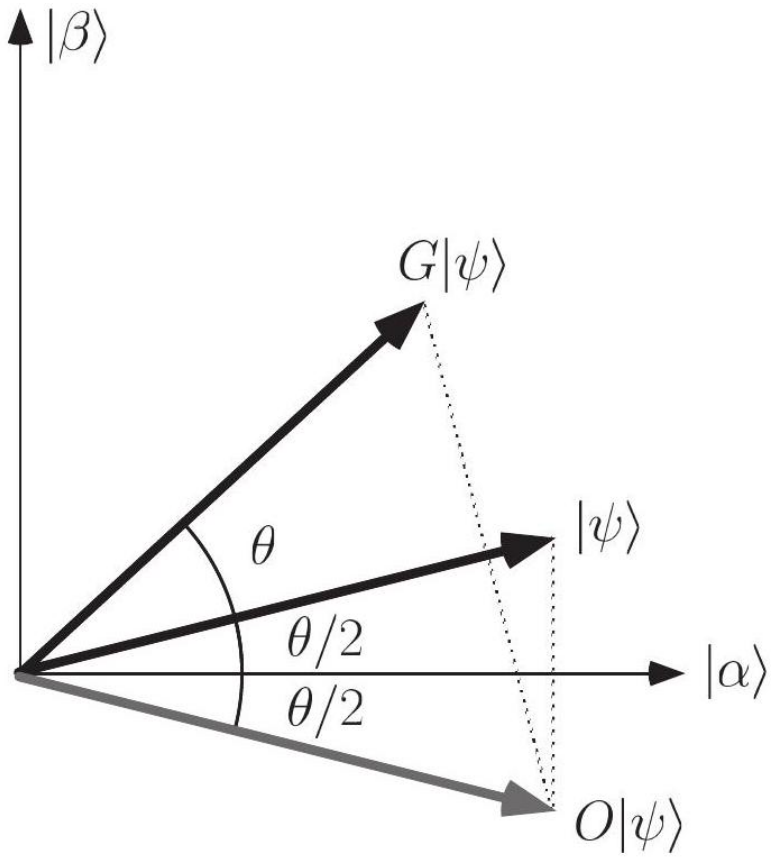


Figure 6.3. The action of a single Grover iteration, G : the state vector is rotated by θ towards the superposition $|\beta\rangle$ of all solutions to the search problem. Initially, it is inclined at angle $\theta/2$ from $|\alpha\rangle$, a state orthogonal to $|\beta\rangle$. An oracle operation O reflects the state about the state $|\alpha\rangle$, then the operation $2|\psi\rangle\langle\psi| - I$ reflects it about $|\psi\rangle$. In the figure $|\alpha\rangle$ and $|\beta\rangle$ are lengthened slightly to reduce clutter (all states should be unit vectors). After repeated Grover iterations, the state vector gets close to $|\beta\rangle$, at which point an observation in the computational basis outputs a solution to the search problem with high probability. The remarkable efficiency of the algorithm occurs because θ behaves like $\Omega(\sqrt{M / N})$, so only $O(\sqrt{N/M})$ applications of G are required to rotate the state vector close to $|\beta\rangle$.}

where θ is a real number in the range 0 to $\pi/2$ (assuming for simplicity that $M \leq N/2$; this limitation will be lifted shortly), chosen so that

$$\sin\theta = \frac{2\sqrt{M(N-M)}}{N}. \tag{6.14}$$

8.3.5 6.1.4 Performance

How many times must the Grover iteration be repeated in order to rotate $|\psi\rangle$ near $|\beta\rangle$? The initial state of the system is $|\psi\rangle = \sqrt{(N-M)/N}|\alpha\rangle + \sqrt{M/N}|\beta\rangle$, so rotating through $\arccos\sqrt{M/N}$ radians takes the system to $|\beta\rangle$. Let $\mathrm{CI}(x)$ denote the integer closest to the real number x, where by convention we round halves down, $\mathrm{CI}(3.5) = 3$, for example. Then repeating the Grover iteration

$$R = \mathrm{CI}\left(\frac{\arccos\sqrt{M/N}}{\theta}\right) \tag{6.15}$$

times rotates $|\psi\rangle$ to within an angle $\theta/2 \leq \pi/4$ of $|\beta\rangle$. Observation of the state in the computational basis then yields a solution to the search problem with probability at least one-half. Indeed, for specific values of M and N it is possible to achieve a much higher probability of success. For example, when $M \ll N$ we have $\theta \approx \sin\theta \approx 2\sqrt{M/N}$, and thus the angular error in the final state is at most $\theta/2 \approx \sqrt{M/N}$, giving a probability of error of at most M/N. Note that R depends on the number of solutions M, but not
on the identity of those solutions, so provided we know M we can apply the quantum search algorithm as described. In Section 6.3 we will explain how to remove even the need for a knowledge of M in applying the search algorithm.

The form (6.15) is useful as an exact expression for the number of oracle calls used to perform the quantum search algorithm, but it would be useful to have a simpler expression summarizing the essential behavior of R. To achieve this, note from (6.15) that $R \leq \lceil \pi/2\theta \rceil$, so a lower bound on θ will give an upper bound on R. Assuming for the moment that $M \leq N/2$, we have

$$\frac{\theta}{2} \geq \sin\frac{\theta}{2} = \sqrt{\frac{M}{N}}, \tag{6.16}$$

from which we obtain an elegant upper bound on the number of iterations required,

$$R \leq \left\lceil \frac{\pi}{4}\sqrt{\frac{N}{M}} \right\rceil \tag{6.17}$$

That is, $R = O(\sqrt{N/M})$ Grover iterations (and thus oracle calls) must be performed in order to obtain a solution to the search problem with high probability, a quadratic improvement over the $O(N/M)$ oracle calls required classically. The quantum search algorithm is summarized below, for the case $M = 1$.

Algorithm: Quantum search

Inputs: (1) a black box oracle O which performs the transformation $O|x\rangle|q\rangle = |x\rangle|q \oplus f(x)\rangle$, where $f(x) = 0$ for all $0 \leq x < 2^n$ except x_0, for which $f(x_0) = 1$; (2) $n+1$ qubits in the state $|0\rangle$.

Outputs: x_0.

Runtime: $O\left(\sqrt{2^n}\right)$ operations. Succeeds with probability $O(1)$.

Procedure:

1. $|0\rangle^{\otimes n}|0\rangle$ initial state
2. $\rightarrow \frac{1}{\sqrt{2^n}} \sum^{2^n-1} |x\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$ apply $H^{\otimes n}$ to the first n qubits, and HX to the last qubit
3. $\rightarrow [(2|\psi\rangle\langle\psi| - I)O]^R \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$ apply the Grover iteration $R \approx \left\lceil \pi\sqrt{2^n}/4 \right\rceil$ times.

   $$\approx |x_0\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

4. $\rightarrow x_0$
   measure the first n qubits

Exercise 6.4: Give explicit steps for the quantum search algorithm, as above, but for the case of multiple solutions ($1 < M < N/2$).

What happens when more than half the items are solutions to the search problem, that is, $M \geq N/2$? From the expression $\theta = \arcsin\left(2\sqrt{M(N-M)}/N\right)$ (compare (6.14)) we see that the angle θ gets smaller as M varies from $N/2$ to N. As a result, the number of iterations needed by the search algorithm increases with M, for $M \geq N/2$. Intuitively,
this is a silly property for a search algorithm to have: we expect that it should become easier to find a solution to the problem as the number of solutions increases. There are at least two ways around this problem. If M is known in advance to be larger than $N/2$ then we can just randomly pick an item from the search space, and then check that it is a solution using the oracle. This approach has a success probability at least one-half, and only requires one consultation with the oracle. It has the disadvantage that we may not know the number of solutions M in advance.

In the case where it isn't known whether $M \geq N/2$, another approach can be used. This approach is interesting in its own right, and has a useful application to simplify the analysis of the quantum algorithm for counting the number of solutions to the search problem, as presented in Section 6.3. The idea is to double the number of elements in the search space by adding N extra items to the search space, none of which are solutions. As a consequence, less than half the items in the new search space are solutions. This is effected by adding a single qubit $|q\rangle$ to the search index, doubling the number of items to be searched to $2N$. A new augmented oracle O' is constructed which marks an item only if it is a solution to the search problem and the extra bit is set to zero. In Exercise 6.5 you will explain how the oracle O' may be constructed using one call to O. The new search problem has only M solutions out of $2N$ entries, so running the search algorithm with the new oracle O' we see that at most $R = \pi/4\sqrt{2N/M}$ calls to O' are required, and it follows that $O(\sqrt{N/M})$ calls to O are required to perform the search.

Exercise 6.5: Show that the augmented oracle O' may be constructed using one application of O, and elementary quantum gates, using the extra qubit $|q\rangle$.

The quantum search algorithm may be used in a wide variety of ways, some of which will be explored in subsequent sections. The great utility of the algorithm arises because we do not assume any particular structure to the search problems being performed. This is the great advantage of posing the problem in terms of a 'black box' oracle, and we adopt this point of view whenever convenient through the remainder of this chapter. In practical applications, of course, it is necessary to understand how the oracle is being implemented, and in each of the practical problems we concern ourselves with an explicit description of the oracle implementation is given.

Exercise 6.6: Verify that the gates in the dotted box in the second figure of Box 6.1 perform the conditional phase shift operation $2|00\rangle\langle 00| - I$, up to an unimportant global phase factor.

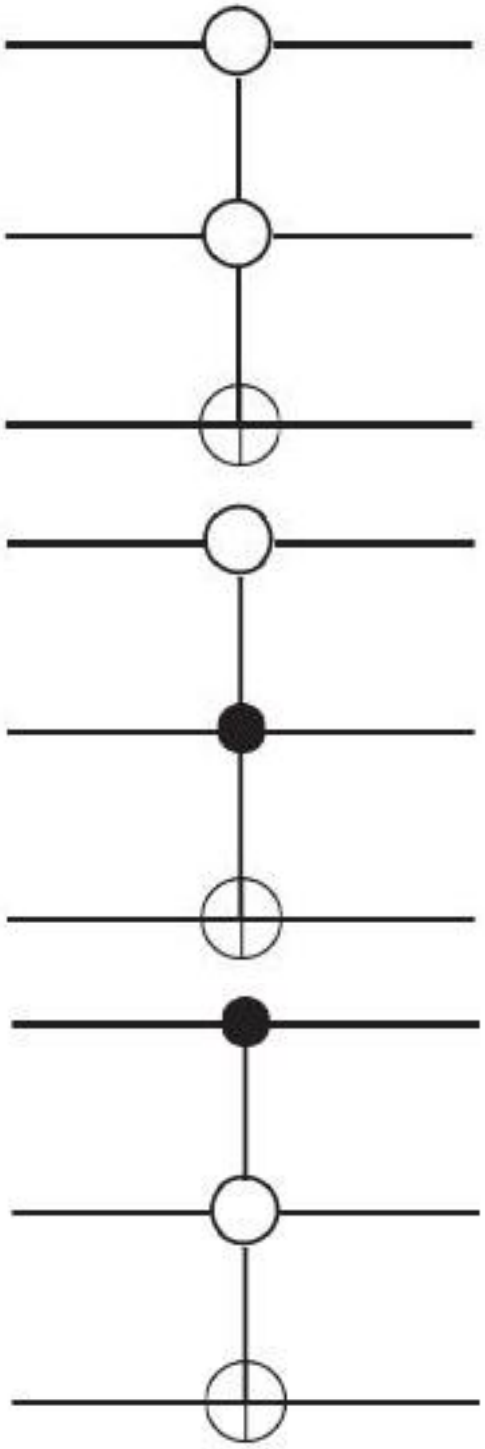
8.3.6 6.2 Quantum search as a quantum simulation

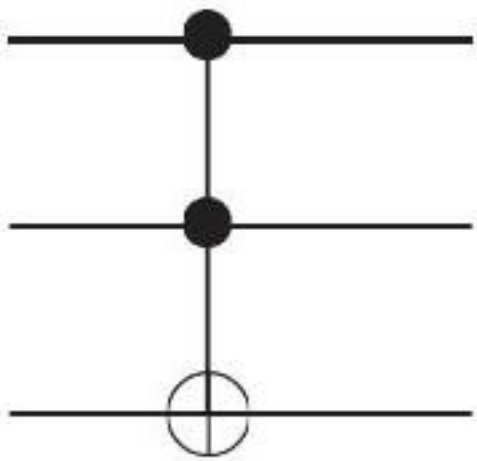
The correctness of the quantum search algorithm is easily verified, but it is by no means obvious how one would dream up such an algorithm from a state of ignorance. In this section we sketch a heuristic means by which one can 'derive' the quantum search algorithm, in the hope of lending some intuition as to the tricky task of quantum algorithm design. As a useful side effect we also obtain a deterministic quantum search algorithm. Because our goal is to obtain insight rather than generality, we assume for the sake of simplicity that the search problem has exactly one solution, which we label x.

Our method involves two steps. First, we make a guess as to a Hamiltonian which

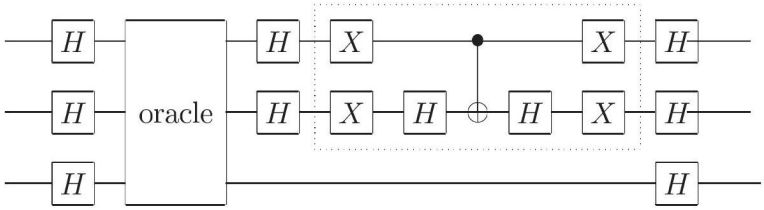
Box 6.1: Quantum search: a two-bit example

Here is an explicit example illustrating how the quantum search algorithm works on a search space of size $N = 4$. The oracle, for which $f(x) = 0$ for all x except $x = x_0$, in which case $f(x_0) = 1$, can be taken to be one of the four circuits





corresponding to $x_0 = 0, 1, 2$, or 3 from left to right, where the top two qubits carry the query x, and the bottom qubit carries the oracle's response. The quantum circuit which performs the initial Hadamard transforms and a single Grover iteration G is



Initially, the top two qubits are prepared in the state $|0\rangle$, and the bottom one as $|1\rangle$. The gates in the dotted box perform the conditional phase shift operation $2|00\rangle\langle 00| - I$. How many times must we repeat G to obtain x_0 ? From Equation (6.15), using $M = 1$, we find that less than one iteration is required. It turns out that because $\theta = \pi/3$ in (6.14), only exactly one iteration is required, to perfectly obtain x_0, in this special case. In the geometric picture of Figure 6.3, our initial state $|\psi\rangle = (|00\rangle + |01\rangle + |10\rangle + |11\rangle)/2$ is 30° from $|\alpha\rangle$, and a single rotation by $\theta = 60°$ moves $|\psi\rangle$ to $|\beta\rangle$. You can confirm for yourself directly, using the quantum circuits, that measurement of the top two qubits gives x_0, after using the oracle only once. In contrast, a classical computer - or classical circuit - trying to differentiate between the four oracles would require on average 2.25 oracle queries!
solves the search problem. More precisely, we write down a Hamiltonian H which depends on the solution x and an initial state $|\psi\rangle$ such that a quantum system evolving according to H will change from $|\psi\rangle$ to $|x\rangle$ after some prescribed time. Once we've found such a Hamiltonian and initial state, we can move on to the second step, which is to attempt to simulate the action of the Hamiltonian using a quantum circuit. Amazingly, following this procedure leads very quickly to the quantum search algorithm! We have already met this two-part procedure while studying universality in quantum circuits, in Problem 4.3, and it also serves well in the study of quantum searching.

We suppose that the algorithm starts with the quantum computer in a state $|\psi\rangle$. We'll tie down what $|\psi\rangle$ should be later on, but it is convenient to leave $|\psi\rangle$ undetermined until we understand the dynamics of the algorithm. The goal of quantum searching is to
change $|\psi\rangle$ into $|x\rangle$ or some approximation thereof. What Hamiltonians might we guess do a good job of causing such an evolution? Simplicity suggests that we should guess a Hamiltonian constructed entirely from the terms $|\psi\rangle$ and $|x\rangle$. Thus, the Hamiltonian must be a sum of terms like $|\psi\rangle\langle\psi|, |x\rangle\langle x|, |\psi\rangle\langle x|$ and $|x\rangle\langle\psi|$. Perhaps the simplest choices along these lines are the Hamiltonians:

$$H = |x\rangle\langle x| + |\psi\rangle\langle\psi| \tag{6.18}$$
$$H = |x\rangle\langle\psi| + |\psi\rangle\langle x|. \tag{6.19}$$

It turns out that both these Hamiltonians lead to the quantum search algorithm! For now, however, we restrict ourselves to analyzing the Hamiltonian in Equation (6.18). Recall from Section 2.2.2 that after a time t, the state of a quantum system evolving according to the Hamiltonian H and initially in the state $|\psi\rangle$ is given by

$$\exp(-iHt)|\psi\rangle \tag{6.20}$$

Intuitively it looks pretty good: for small t the effect of the evolution is to take $|\psi\rangle$ to $(I - itH)|\psi\rangle = (1 - it)|\psi\rangle - it\langle x \mid \psi\rangle|x\rangle$. That is, the $|\psi\rangle$ vector is rotated slightly, into the $|x\rangle$ direction. Let's actually do a full analysis, with the goal being to determine whether there is a t such that $\exp(-iHt)|\psi\rangle = |x\rangle$. Clearly we can restrict the analysis to the two-dimensional space spanned by $|x\rangle$ and $|\psi\rangle$. Performing the Gram-Schmidt procedure, we can find $|y\rangle$ such that $|x\rangle, |y\rangle$ forms an orthonormal basis for this space, and $|\psi\rangle = \alpha|x\rangle + \beta|y\rangle$, for some α, β such that $\alpha^2 + \beta^2 = 1$, and for convenience we have chosen the phases of $|x\rangle$ and $|y\rangle$ so that α and β are real and non-negative. In the $|x\rangle, |y\rangle$ basis we have

$$H = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} \alpha^2 & \alpha\beta \\ \alpha\beta & \beta^2 \end{bmatrix} = \begin{bmatrix} 1+\alpha^2 & \alpha\beta \\ \alpha\beta & 1-\alpha^2 \end{bmatrix} = I + \alpha(\beta X + \alpha Z) \tag{6.21}$$

Thus

$$\exp(-iHt)|\psi\rangle = \exp(-it)[\cos(\alpha t)|\psi\rangle - i\sin(\alpha t)(\beta X + \alpha Z)|\psi\rangle] \tag{6.22}$$

The global phase factor $\exp(-it)$ can be ignored, and simple algebra shows that $(\beta X + \alpha Z)|\psi\rangle = |x\rangle$, so the state of the system after a time t is

$$\cos(\alpha t)|\psi\rangle - i\sin(\alpha t)|x\rangle \tag{6.23}$$

Thus, observation of the system at time $t = \pi/2\alpha$ yields the result $|x\rangle$ with probability one: we have found a solution to the search problem! Unfortunately, the time of the observation depends on α, the component of $|\psi\rangle$ in the $|x\rangle$ direction, and thus on x, which is what we are trying to determine. The obvious solution is to attempt to arrange α to be the same for all $|x\rangle$, that is, to choose $|\psi\rangle$ to be the uniform superposition state

$$|\psi\rangle = \frac{\sum_x |x\rangle}{\sqrt{N}} \tag{6.24}$$

Making this choice gives $\alpha = 1/\sqrt{N}$ for all x, and thus the time of observation $t = \pi\sqrt{N}/2$ does not depend on knowing the value of x. Furthermore, the state (6.24) has the obvious advantage that we already know how to prepare such a state by doing a Hadamard transform.

We now know that the Hamiltonian (6.18) rotates the vector $|\psi\rangle$ to $|x\rangle$. Can we find a quantum circuit to simulate the Hamiltonian (6.18), and thus obtain a quantum search algorithm? Applying the method of Section 4.7, we see that a natural way of simulating H is to alternately simulate the Hamiltonians $H_1 \equiv |x\rangle\langle x|$ and $H_2 \equiv |\psi\rangle\langle\psi|$ for short time increments Δt. These Hamiltonians are easily simulated using the methods of Chapter 4, as illustrated in Figures 6.4 and 6.5.

Exercise 6.7: Verify that the circuits shown in Figures 6.4 and 6.5 implement the operations $\exp(-i|x\rangle\langle x|\Delta t)$ and $\exp(-i|\psi\rangle\langle\psi|\Delta t)$, respectively, with $|\psi\rangle$ as in (6.24).

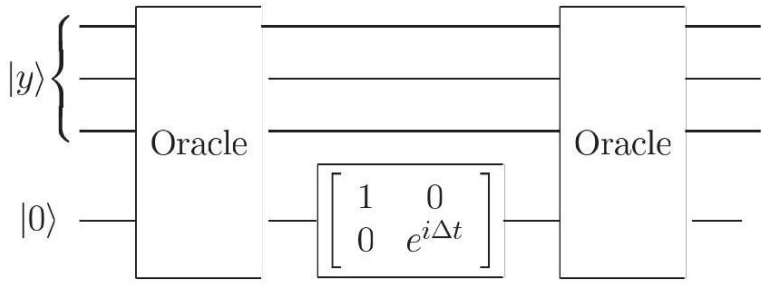


Figure 6.4. Circuit implementing the operation $\exp(-i|x\rangle\langle x|\Delta t)$ using two oracle calls.

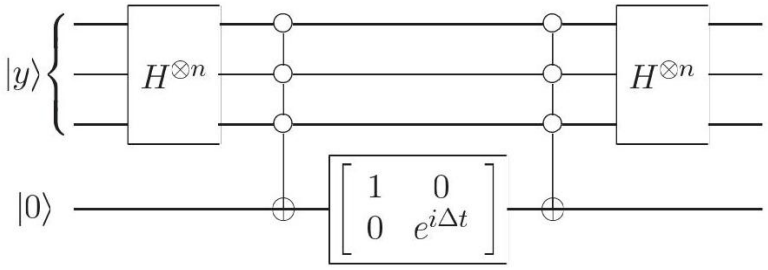


Figure 6.5. Circuit implementing the operation $\exp(-i|\psi\rangle\langle\psi|\Delta t)$, for $|\psi\rangle$ as in (6.24).

The number of oracle calls required by the quantum simulation is determined by how small a time-step is required to obtain reasonably accurate results. Suppose we use a simulation step of length Δt that is accurate to $O(\Delta t^2)$. The total number of steps required is $t/\Delta t = \Theta(\sqrt{N}/\Delta t)$, and thus the cumulative error is $O\left(\Delta t^2 \times \sqrt{N}/\Delta t\right) = O(\Delta t\sqrt{N})$. To obtain a reasonably high success probability we need the error to be $O(1)$, which means that we must choose $\Delta t = \Theta(1/\sqrt{N})$ which results in a number of oracle calls that scales like $O(N)$ - no better than the classical solution! What if we use a more accurate method of quantum simulation, say one that is accurate to $O(\Delta t^3)$? The cumulative error in this case is $O\left(\Delta t^2\sqrt{N}\right)$, and thus to achieve a reasonable success probability we need to choose $\Delta t = \Theta\left(N^{-1/4}\right)$, resulting in a total number of oracle calls $O\left(N^{3/4}\right)$, which is a distinct improvement over the classical situation, although still not as good as achieved by the quantum search algorithm of Section 6.1! In general going to a more accurate quantum simulation technique results in a reduction in the number of oracle calls required to perform the simulation:

Exercise 6.8: Suppose the simulation step is performed to an accuracy $O(\Delta t^r)$. Show that the number of oracle calls required to simulate H to reasonable accuracy is $O\left(N^{r/2(r-1)}\right)$. Note that as r becomes large the exponent of N approaches $1/2$.

We have been analyzing the accuracy of the quantum simulation of the Hamiltonian (6.18) using general results on quantum simulation from Section 4.7. Of course, in this instance we are dealing with a specific Hamiltonian, not the general case, which suggests that it might be interesting to calculate explicitly the effect of a simulation step of time Δt, rather than relying on the general analysis. We can do this for any specific choice of simulation method - it can be a little tedious to work out the effect of the simulation step, but it is essentially a straightforward calculation. The obvious starting point is to explicitly calculate the action of the lowest-order simulation techniques, that is, to calculate one or both of $\exp(-i|x\rangle\langle x|\Delta t)\exp(-i|\psi\rangle\langle\psi|\Delta t)$ or $\exp(-i|\psi\rangle\langle\psi|\Delta t)\exp(-i|x\rangle\langle x|\Delta t)$. The results are essentially the same in both instances; we will focus on the study of $U(\Delta t) \equiv \exp(-i|\psi\rangle\langle\psi|\Delta t)\exp(-i|x\rangle\langle x|\Delta t)$.$U(\Delta t)$ clearly acts non-trivially only in the space spanned by $|x\rangle\langle x|$ and $|\psi\rangle\langle\psi|$, so we restrict ourselves to that space,

working in the basis $|x\rangle, |y\rangle$, where $|y\rangle$ is defined as before. Note that in this representation $|x\rangle\langle x| = (I + Z)/2 = (I + \hat{z} \cdot \vec{\sigma})/2$, where $\hat{z} \equiv (0, 0, 1)$ is the unit vector in the z direction, and $|\psi\rangle\langle\psi| = (I + \vec{\psi} \cdot \vec{\sigma})/2$, where $\vec{\psi} = (2\alpha\beta, 0, (\alpha^2 - \beta^2)$ (recall that this is the Bloch vector representation; see Section 4.2). A simple calculation shows that up to an unimportant global phase factor,

$$\begin{aligned} U(\Delta t) = & \left(\cos^2 \left(\frac{\Delta t}{2} \right) - \sin^2 \left(\frac{\Delta t}{2} \right) \vec{\psi} \cdot \hat{z} \right) I \\ & - 2i \sin \left(\frac{\Delta t}{2} \right) \left(\cos \left(\frac{\Delta t}{2} \right) \frac{\vec{\psi} + \hat{z}}{2} + \sin \left(\frac{\Delta t}{2} \right) \frac{\vec{\psi} \times \hat{z}}{2} \right) \cdot \vec{\sigma} \end{aligned} \tag{6.25}$$

Exercise 6.9: Verify Equation (6.25). (Hint: see Exercise 4.15.)
Equation (6.25) implies that $U(\Delta t)$ is a rotation on the Bloch sphere about an axis of rotation $\vec{r}$ defined by

$$\vec{r} = \cos \left(\frac{\Delta t}{2} \right) \frac{\vec{\psi} + \hat{z}}{2} + \sin \left(\frac{\Delta t}{2} \right) \frac{\vec{\psi} \times \hat{z}}{2} \tag{6.26}$$

and through an angle θ defined by

$$\cos \left(\frac{\theta}{2} \right) = \cos^2 \left(\frac{\Delta t}{2} \right) - \sin^2 \left(\frac{\Delta t}{2} \right) \vec{\psi} \cdot \hat{z} \tag{6.27}$$

which simplifies upon substitution of $\vec{\psi} \cdot \hat{z} = \alpha^2 - \beta^2 = (2/N - 1)$ to

$$\cos \left(\frac{\theta}{2} \right) = 1 - \frac{2}{N} \sin^2 \left(\frac{\Delta t}{2} \right). \tag{6.28}$$

Note that $\vec{\psi} \cdot \vec{r} = \hat{z} \cdot \vec{r}$, so both $|\psi\rangle\langle\psi|$ and $|x\rangle\langle x|$ lie on the same circle of revolution about the $\vec{r}$ axis on the Bloch sphere. Summarizing, the action of $U(\Delta t)$ is to rotate $|\psi\rangle\langle\psi|$ about the $\vec{r}$ axis, through an angle θ for each application of $U(\Delta t)$, as illustrated in Figure 6.6. We terminate the procedure when enough rotations have been performed to rotate $|\psi\rangle\langle\psi|$ near to the solution $|x\rangle\langle x|$. Now initially we imagined that Δt was small, since we were considering the case of quantum simulation, but Equation (6.28) shows
that the smart thing to do is to choose $\Delta t = \pi$, in order to maximize the rotation angle θ. If we do this, then we obtain $\cos(\theta/2) = 1 - 2/N$, which for large N corresponds to $\theta \approx 4/\sqrt{N}$, and the number of oracle calls required to find the solution $|x\rangle$ is $O(\sqrt{N})$, just as for the original quantum search algorithm.

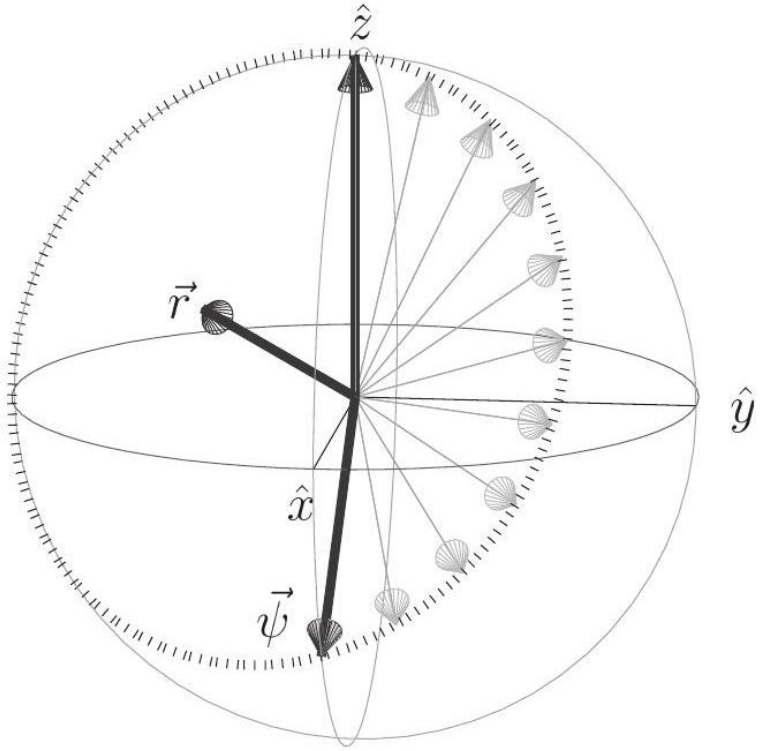


Figure 6.6. Bloch sphere diagram showing the initial state $\vec{\psi}$ rotating around the axis of rotation $\vec{r}$ going toward the final state $\hat{z}$.}

Indeed, if we make the choice $\Delta t = \pi$, then this 'quantum simulation' is in fact identical with the original quantum search algorithm, since the operators applied in the quantum simulation are $\exp(-i\pi|\psi\rangle\langle\psi|) = I - 2|\psi\rangle\langle\psi|$ and $\exp(-i\pi|x\rangle\langle x|) = I - 2|x\rangle\langle x|$, and up to a global phase shift these are identical to the steps making up the Grover iteration. Viewed this way, the circuits shown in Figures 6.2 and 6.3 for the quantum search algorithm are simplifications of the circuits shown in Figures 6.4 and 6.5 for the simulation, in the special case $\Delta t = \pi$!

Exercise 6.10: Show that by choosing Δt appropriately we can obtain a quantum search algorithm which uses $O(\sqrt{N})$ queries, and for which the final state is $|x\rangle$ exactly, that is, the algorithm works with probability 1, rather than with some smaller probability.

We have re-derived the quantum search algorithm from a different point of view, the point of view of quantum simulation. Why did this approach work? Might it be used to find other fast quantum algorithms? We can't answer these questions in any definitive way, but the following few thoughts may be of some interest. The basic procedure used is four-fold: (1) specify the problem to be solved, including a description of the desired input and output from the quantum algorithm; (2) guess a Hamiltonian to solve the problem, and verify that it does in fact work; (3) find a procedure to simulate the Hamiltonian; and (4) analyze the resource costs of the simulation. This is different from the more conventional approach in two respects: we guess a Hamiltonian, rather than a quantum circuit, and there is no analogue to the simulation step in the conventional approach. The more important of these two differences is the first. There is a great deal of freedom in specifying a quantum circuit to solve a problem. While that freedom is, in part, responsible
for the great power of quantum computation, it makes searching for good circuits rather difficult. By contrast, specifying a Hamiltonian is a much more constrained problem, and therefore affords less freedom in the solution of problems, but those same constraints may in fact make it much easier to find an efficient quantum algorithm to solve a problem. We've seen this happen for the quantum search algorithm, and perhaps other quantum algorithms will be discovered by

this method; we don't know. What seems certain is that this 'quantum algorithms as quantum simulations' point of view offers a useful alternative viewpoint to stimulate in the development of quantum algorithms.

Exercise 6.11: (Multiple solution continuous quantum search) Guess a

Hamiltonian with which one may solve the continuous time search problem in the case where the search problem has M solutions.

Exercise 6.12: (Alternative Hamiltonian for quantum search) Suppose

$$H = |x\rangle\langle\psi| + |\psi\rangle\langle x| \tag{6.29}$$

(1) Show that it takes time $O(1)$ to rotate from the state $|\psi\rangle$ to the state $|x\rangle$, given an evolution according to the Hamiltonian H.
(2) Explain how a quantum simulation of the Hamiltonian H may be performed, and determine the number of oracle calls your simulation technique requires to obtain the solution with high probability.

8.3.7 6.3 Quantum counting

How quickly can we determine the number of solutions, M, to an N item search problem, if M is not known in advance? Clearly, on a classical computer it takes $\Theta(N)$ consultations with an oracle to determine M. On a quantum computer it is possible to estimate the number of solutions much more quickly than is possible on a classical computer by combining the Grover iteration with the phase estimation technique based upon the quantum Fourier transform (Chapter 5). This has some important applications. First, if we can estimate the number of solutions quickly then it is also possible to find a solution quickly, even if the number of solutions is unknown, by first counting the number of solutions, and then applying the quantum search algorithm to find a solution. Second, quantum counting allows us to decide whether or not a solution even exists, depending on whether the number of solutions is zero, or non-zero. This has applications, for example, to the solution of NP-complete problems, which may be phrased in terms of the existence of a solution to a search problem.

Exercise 6.13: Consider a classical algorithm for the counting problem which samples uniformly and independently k times from the search space, and let $X_1, \ldots, X_k$ be the results of the oracle calls, that is, $X_j = 1$ if the j th oracle call revealed a solution to the problem, and $X_j = 0$ if the j th oracle call did not reveal a solution to the problem. This algorithm returns the estimate $S \equiv N \times \sum_j X_j/k$ for the number of solutions to the search problem. Show that the standard deviation in S is $\Delta S = \sqrt{M(N-M)/k}$. Prove that to obtain a probability at least $3/4$ of estimating M correctly to within an accuracy $\sqrt{M}$ for all values of M we must have $k = \Omega(N)$.

Exercise 6.14: Prove that any classical counting algorithm with a probability at least $3/4$ for estimating M correctly to within an accuracy $c\sqrt{M}$ for some constant c and for all values of M must make $\Omega(N)$ oracle calls.

Quantum counting is an application of the phase estimation procedure of Section 5.2 to estimate the eigenvalues of the Grover iteration G, which in turn enables us to determine the number of solutions M to the search problem. Suppose $|a\rangle$ and $|b\rangle$ are the two eigenvectors of the Grover iteration in the space spanned by $|\alpha\rangle$ and $|\beta\rangle$. Let θ be the angle of rotation determined by the Grover iteration. From Equation (6.13) we see that the corresponding eigenvalues are $e^{i\theta}$ and $e^{i(2\pi-\theta)}$. For ease of analysis it is convenient to assume that the oracle has been augmented, as described in Section 6.1, expanding the size of the search space to $2N$, and ensuring that $\sin^2(\theta/2) = M/2N$.

The phase estimation circuit used for quantum counting is shown in Figure 6.7. The function of the circuit is to estimate θ to m bits of accuracy, with a probability of success at least $1-\epsilon$. The first register contains $t \equiv m + \lceil \log(2 + 1/2\epsilon) \rceil$ qubits, as per the phase estimation algorithm, and the second register contains $n+1$ qubits, enough to implement the Grover iteration on the augmented search space. The state of the second register is initialized to an equal superposition of all possible inputs $\sum_x |x\rangle$ by a Hadamard transform. As we saw in Section 6.1 this state is a superposition of the eigenstates $|a\rangle$ and $|b\rangle$, so by the results of Section 5.2 the circuit in Figure 6.7 gives us an estimate of θ or $2\pi - \theta$ accurate to within $|\Delta\theta| \leq 2^{-m}$, with probability at least $1-\epsilon$. Furthermore, an estimate for $2\pi - \theta$ is clearly equivalent to an estimate of θ with the same level of accuracy, so effectively the phase estimation algorithm determines θ to an accuracy 2^{-m} with probability $1-\epsilon$.

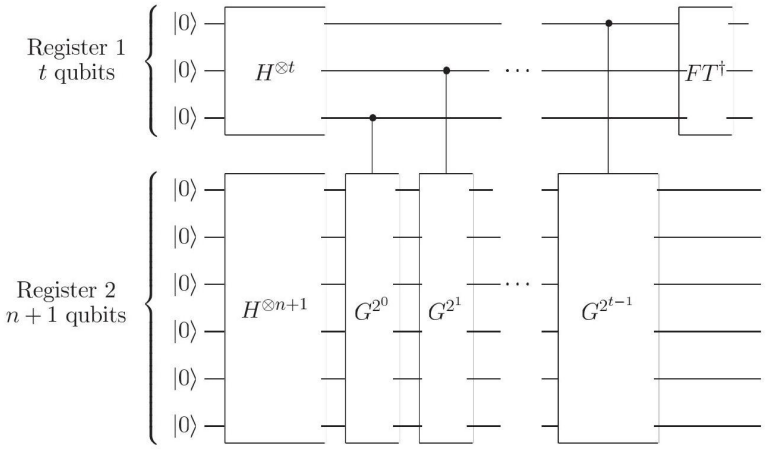


Figure 6.7. Circuit for performing approximate quantum counting on a quantum computer.

Using the equation $\sin^2(\theta/2) = M/2N$ and our estimate for θ we obtain an estimate of the number of solutions, M. How large an error, ΔM, is there in this estimate?

$$\frac{|\Delta M|}{2N} = \left| \sin^2\left(\frac{\theta+\Delta\theta}{2}\right) - \sin^2\left(\frac{\theta}{2}\right) \right| \tag{6.30}$$

$$= \left(\sin\left(\frac{\theta+\Delta\theta}{2}\right) + \sin\left(\frac{\theta}{2}\right) \right) \left| \sin\left(\frac{\theta+\Delta\theta}{2}\right) - \sin\left(\frac{\theta}{2}\right) \right|. \tag{6.31}$$

Calculus implies that $|\sin((\theta+\Delta\theta)/2) - \sin(\theta/2)| \leq |\Delta\theta|/2$, and elementary trigonometry that $|\sin((\theta+\Delta\theta)/2)| < \sin(\theta/2) + |\Delta\theta|/2$, so

$$\frac{|\Delta M|}{2N} < \left(2\sin\left(\frac{\theta}{2}\right) + \frac{|\Delta\theta|}{2} \right) \frac{|\Delta\theta|}{2}. \tag{6.32}$$

Substituting $\sin^2(\theta/2) = M/2N$ and $|\Delta\theta| \leq 2^{-m}$ gives our final estimate for the error in our estimate of M,

$$|\Delta M| < \left(\sqrt{2MN} + \frac{N}{2^{m+1}} \right) 2^{-m}. \tag{6.33}$$

As an example, suppose we choose $m = \lceil n/2 \rceil + 1$, and $\epsilon = 1/6$. Then we have $t = \lceil n/2 \rceil + 3$, so the algorithm requires $\Theta(\sqrt{N})$ Grover iterations, and thus $\Theta(\sqrt{N})$ oracle calls. By (6.33) our accuracy is $|\Delta M| < \sqrt{M/2} + 1/4 = O(\sqrt{M})$. Compare this with Exercise 6.14, according

to which it would have required $O(N)$ oracle calls to obtain a similar accuracy on a classical computer.

Indeed, the example just described serves double duty as an algorithm for determining whether a solution to the search problem exists at all, that is, whether $M = 0$ or $M \neq 0$. If $M = 0$ then we have $|\Delta M| < 1/4$, so the algorithm must produce the estimate zero with probability at least 5/6. Conversely, if $M \neq 0$ then it is easy to verify that the estimate for M is not equal to 0 with probability at least 5/6.

Another application of quantum counting is to find a solution to a search problem when the number M of solutions is unknown. The difficulty in applying the quantum search algorithm as described in Section 6.1 is that the number of times to repeat the Grover iteration, Equation (6.15), depends on knowing the number of solutions M. This problem can be alleviated by using the quantum counting algorithm to first estimate θ and M to high accuracy using phase estimation, and then to apply the quantum search algorithm as in Section 6.1, repeating the Grover iteration a number of times determined by (6.15), with the estimates for θ and M obtained by phase estimation substituted to determine R. The angular error in this case is at most $\pi/4(1 + |\Delta\theta|/\theta)$, so choosing $m = \lceil n/2 \rceil + 1$ as before gives an angular error at most $\pi/4 \times 3/2 = 3\pi/8$, which corresponds to a success probability of at least $\cos^2(3\pi/8) = 1/2 - 1/2\sqrt{2} \approx 0.15$ for the search algorithm. If the probability of obtaining an estimate of θ this accurate is 5/6, as in our earlier example, then the total probability of obtaining a solution to the search problem is $5/6 \times \cos^2(3\pi/8) \approx 0.12$, a probability which may quickly be boosted close to 1 by a few repetitions of the combined counting-search procedure.

8.3.8 6.4 Speeding up the solution of NP-complete problems

Quantum searching may be used to speed up the solution to problems in the complexity class NP (Section 3.2.2). We already saw, in Section 6.1.1, how factoring can be sped up; here, we illustrate how quantum search can be applied to assist the solution of the Hamiltonian cycle problem (HC). Recall that a Hamiltonian cycle of a graph is a simple cycle which visits every vertex of the graph. The HC problem is to determine whether a given graph has a Hamiltonian cycle or not. This problem belongs to the class of NPcomplete problems, widely believed (but not yet proved) to be intractable on a classical computer.

A simple algorithm to solve HC is to perform a search through all possible orderings of the vertices:
(1) Generate each possible ordering $(v_1, \ldots, v_n)$ of vertices for the graph. Repetitions will be allowed, as they ease the analysis without affecting the essential result.
(2) For each ordering check to see whether it is a Hamiltonian cycle for the graph. If not, continue checking the orderings.
Since there are $n^n = 2^{n \log n}$ possible orderings of the vertices which must be searched, this algorithm requires $2^{n \log n}$ checks for the Hamiltonian cycle property in the worst case. Indeed, any problem in NP may be solved in a similar way: if a problem of size n has witnesses which can be specified using $w(n)$ bits, where $w(n)$ is some polynomial in n, then searching through all $2^{w(n)}$ possible witnesses will reveal a solution to the problem, if one exists.

The quantum search algorithm may be used to speed up this algorithm by increasing the speed of the search. Specifically, we use the algorithm described in Section 6.3 to determine whether a solution to the search problem exists. Let $m \equiv \lceil \log n \rceil$. The search space for the algorithm will be represented by a string of mn qubits, each block of m qubits being used to store the index to a single vertex. Thus we can write the computational basis states as $|v_1, \ldots, v_n\rangle$, where each $|v_i\rangle$ is represented by the appropriate string of m qubits, for a total of nm qubits. The oracle for the search algorithm must apply the transformation:

$$O|v_1,\ldots,v_n\rangle = \begin{cases} |v_1,\ldots,v_n\rangle \text{ if } v_1,\ldots,v_n \text{ is not a Hamiltonian cycle} \\ -|v_1,\ldots,v_n\rangle \text{ if } v_1,\ldots,v_n \text{ is a Hamiltonian cycle} \end{cases} \quad (6.34)$$

Such an oracle is easy to design and implement when one has a description of the graph. One takes a polynomial size classical circuit recognizing Hamiltonian cycles in the graph, and converts it to a reversible circuit, also of polynomial size, computing the transformation $(v_1,\ldots,v_n,q) \rightarrow (v_1,\ldots,v_n,q \oplus f(v_1,\ldots,v_n))$, where $f(v_1,\ldots,v_n) = 1$ if $v_1,\ldots,v_n$ is a Hamiltonian cycle, and is 0 otherwise. Implementing the corresponding circuit on a quantum computer with the final qubit starting in the state $(|0\rangle - |1\rangle)/\sqrt{2}$ gives the desired transformation. We won't explicitly describe the details here, except to note the key point: the oracle requires a number of gates polynomial in n, as a direct consequence of the fact that Hamiltonian cycles can be recognized using polynomially many gates classically. Applying the variant of the search algorithm which determines whether a solution to the search problem exists (Section 6.3) we see that it takes $O\left(2^{mn/2}\right) = O\left(2^{n\lceil \log n \rceil/2}\right)$ applications of the oracle to determine whether a Hamiltonian cycle exists. When one does exist it is easy to apply the combined counting-search algorithm to find an example of such a cycle, which can then be exhibited as a witness for the problem.

To summarize:

- The classical algorithm requires $O\left(p(n)2^{n\lceil \log n \rceil}\right)$ operations to determine whether a

Hamiltonian cycle exists, where the polynomial factor $p(n)$ is overhead predominantly due to the implementation of the oracle, that is, the gates checking whether a candidate path is Hamiltonian or not. The dominant effect in determining the resources required is the exponent in $2^{n\lceil \log n \rceil}$. The classical algorithm is deterministic, that is, it succeeds with probability 1.

- The quantum algorithm requires $O\left(p(n)2^{n\lceil \log n \rceil/2}\right)$ operations to determine whether a Hamiltonian cycle exists. Once again, the polynomial $p(n)$ is overhead predominantly due to implementation of the oracle. The dominant effect in determining the resources required is the exponent in $2^{n\lceil \log n \rceil/2}$. There is a constant probability (say, 1/6) of error for the algorithm, which may be reduced to $1/6^r$ by r repetitions of the algorithm.

- Asymptotically the quantum algorithm requires the square root of the number of operations the classical algorithm requires.

8.3.9 6.5 Quantum search of an unstructured database

Suppose somebody gives you a list containing one thousand flower names, and asks you where 'Perth Rose' appears on the list. If the flower appears exactly once on the list, and the list is not ordered in any obvious way, then you will need to examine five hundred names, on average, before you find the 'Perth Rose'. Might it be possible to speed up this kind of database searching using the quantum search algorithm? Indeed, the quantum search algorithm is sometimes referred to as a database search algorithm, but its usefulness for that application is limited, and based on certain assumptions. In this section we take a look at how the quantum search algorithm can conceptually be used to search an unstructured database, in a setting rather like that found on a conventional computer. The picture we construct will clarify what resources are required to enable a quantum computer to search classical databases.

Suppose we have a database containing $N \equiv 2^n$ items, each of length l bits. We will label these items $d_1,\ldots,d_N$. We want to determine where a particular l bit string, s, is in the database. A classical computer, used to solve this problem, is typically split into two parts, illustrated in Figure 6.8. One is the central processing unit, or CPU, where data manipulation

takes place, using a small amount of temporary memory. The second part is a large memory which stores the database in a string of 2^n blocks of l bit cells. The memory is assumed to be passive, in the sense that it is not capable of processing data on its own. What is possible is to LOAD data from memory into the CPU, and STORE data from the CPU in memory, and to do manipulations of the data stored temporarily in the CPU. Of course, classical computers may be designed along different lines, but this CPU-memory split is a popular and common architecture.

To find out where a given string s is in the unstructured database, the most efficient classical algorithm is as follows. First, an n-bit index to the database elements is set up in the CPU. We assume that the CPU is large enough to store the $n \equiv \lceil \log N \rceil$ bit index. The index starts out at zero, and is incremented by one on each iteration of the algorithm. At each iteration, the database entry corresponding to the index is loaded into the CPU, and compared to the string which is being searched for. If they are the same, the algorithm outputs the value of the index and halts. If not, the algorithm continues incrementing the index. Obviously, this algorithm requires that items be loaded from

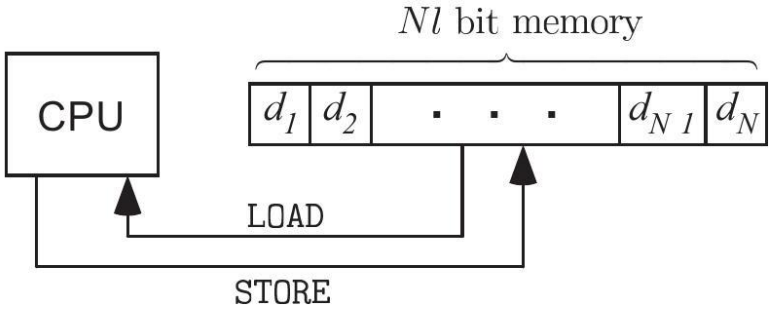


Figure 6.8. Classical database searching on a computer with distinct central processing unit (CPU) and memory. Only two operations may be directly performed on the memory - a memory element may be LOADed into the CPU, or an item from the CPU may be STOREd in memory.

memory 2^n times in the worst case. It is also clear that this is the most efficient possible algorithm for solving the problem in this model of computation.

How efficiently can an analogous algorithm be implemented on a quantum computer? And, even if a quantum speedup is possible, how useful is such an algorithm? We show first that a speedup is possible, and then return to the question of the utility of such an algorithm. Suppose our quantum computer consists of two units, just like the classical computer, a CPU and a memory. We assume that the CPU contains four registers: (1) an n qubit 'index' register initialized to $|0\rangle$; (2) an l qubit register initialized to $|s\rangle$ and remaining in that state for the entire computation; (3) an l qubit 'data' register initialized to $|0\rangle$; and (4) a 1 qubit register initialized to $(|0\rangle - |1\rangle)/\sqrt{2}$.

The memory unit can be implemented in one of two ways. The simplest is a quantum memory containing $N = 2^n$ cells of l qubits each, containing the database entries $|d_x\rangle$. The second implementation is to implement the memory as a classical memory with $N = 2^n$ cells of l bits each, containing the database entries d_x. Unlike a traditional classical memory, however, it can be addressed by an index x which can be in a superposition of multiple values. This quantum index allows a superposition of cell values to be LOADed from memory. Memory access works in the following way: if the CPU's index register is in the state $|x\rangle$ and the data register is in the state $|d\rangle$, then the contents d_x of the x th memory cell are added to the data register: $|d\rangle \rightarrow |d \oplus d_x\rangle$, where the addition is done bitwise, modulo 2 . First, let us see how this capability is used to perform quantum search, then we shall discuss how such a memory might be physically constructed.

The key part of implementing the quantum search algorithm is realization of the oracle, which must flip the phase of the index which locates s in the memory. Suppose the CPU is in the state

$$|x\rangle|s\rangle|0\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}}. \tag{6.35}$$

Applying the LOAD operation puts the computer in the state

$$|x\rangle|s\rangle\,|d_x\rangle\,\frac{|0\rangle-|1\rangle}{\sqrt{2}}. \tag{6.36}$$

Now the second and third registers are compared, and if they are the same, then a bit flip is applied to register 4; otherwise nothing is changed. The effect of this operation is

$$|x\rangle|s\rangle\,|d_x\rangle\,\frac{|0\rangle-|1\rangle}{\sqrt{2}}\rightarrow\begin{cases}-|x\rangle|s\rangle\,|d_x\rangle\,\dfrac{|0\rangle-|1\rangle}{\sqrt{2}} & \text{if } d_x=s\\ \;\;|x\rangle|s\rangle\,|d_x\rangle\,\dfrac{|0\rangle-|1\rangle}{\sqrt{2}} & \text{if } d_x\neq s\end{cases} \tag{6.37}$$

The data register is then restored to the state $|0\rangle$ by performing the LOAD operation again. The total action of the oracle thus leaves registers 2, 3 and 4 unaffected, and unentangled with register 1. Thus, the overall effect is to take the state of register 1 from $|x\rangle$ to $-|x\rangle$ if $d_x = s$, and to leave the register alone otherwise. Using the oracle implemented in this way, we may apply the quantum search algorithm to determine the location of s in the database, using $O(\sqrt{N})$ LOAD operations, compared to the N LOAD operations that were required classically.

In order for the oracle to function correctly on superpositions it seems at first glance as though the memory needs to be quantum mechanical. In fact, as we noted above, with some caveats the memory can actually be implemented classically, which likely makes it much more resistant to the effects of noise. But a quantum addressing scheme is still needed; a conceptual picture illustrating how this might be done is shown in Figure 6.9. The principle of operation is a means by which the binary encoded state of the quantum index (where 0 to $2^n - 1$ is represented by n qubits) is translated into a unary encoding (where 0 to $2^n - 1$ is represented by the position of a single probe within 2^n possible locations) which addresses the classical database. The database effects a change on a degree of freedom within the probe which is unrelated to its position. The binary to unary encoding is then reversed, leaving the data register with the desired contents.

Are there practical instances in which the quantum search algorithm could be useful for searching classical databases? Two distinct points may be made. First, databases are not ordinarily unstructured. Simple databases, like one containing flower names discussed in the introduction to this section, may be maintained in alphabetical order, such that a binary search can be used to locate an item in time which is $O(\log(N))$ for an N-element database. However, some databases may require a much more complex structure, and although sophisticated techniques exist to optimize classical searches, given queries of a sufficiently complex or unanticipated nature, a predetermined structure may not be of assistance, and the problem can be regarded as being essentially the unstructured database search problem we discussed.

Second, for a quantum computer to be able to search a classical database, a quantum addressing scheme is required. The scheme we depicted requires $O(N \log N)$ quantum switches - about the same amount of hardware as would be required to store the database itself. Presumably, these switches may someday be as simple and inexpensive as classical memory elements, but if that is not the case, then building a quantum computer to perform a quantum search may not be economically advantageous, compared with using classical computing hardware distributed over the memory elements.

Given these considerations, it appears that the principle use of quantum search algorithms will not be in searching classical databases. Rather, their use will probably be in searching for solutions to hard problems, as discussed in the last section, such as the Hamiltonian cycle, traveling salesman, and satisfiability problems.

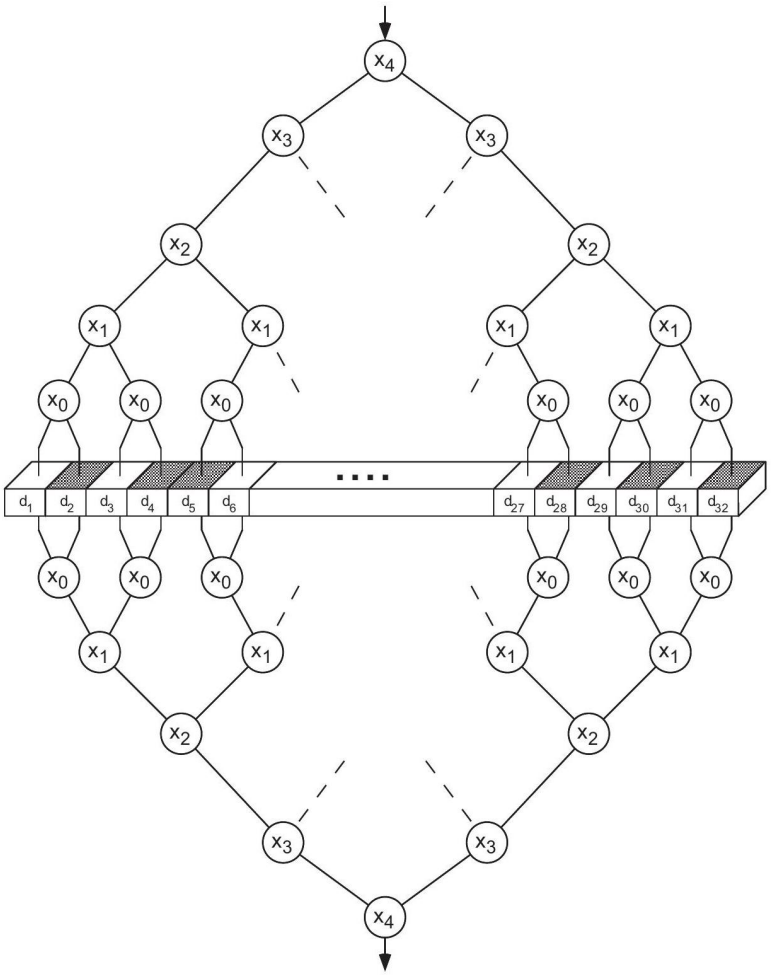


Figure 6.9. Conceptual diagram of a 32 cell classical memory with a five qubit quantum addressing scheme. Each circle represents a switch, addressed by the qubit inscribed within. For example, when $\left|x_{4}\right\rangle=|0\rangle$, the corresponding switch routes the input qubit towards the left; when $|x_4\rangle = |1\rangle$ the switch routes the input qubit to the right. If $|x_4\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, then an equal superposition of both routes is taken. The data register qubits enter at the top of the tree, and are routed down to the database, which changes their state according to the contents of the memory. The qubits are then routed back into a definite position, leaving them with the retrieved information. Physically, this could be realized using, for example, single photons for the data register qubits, which are steered using nonlinear interferometers (Chapter 7). The classical database could be just a simple sheet of plastic in which a 'zero' (illustrated as white squares) transmits light unchanged, and a 'one' (shaded squares) shifts the polarization of the incident light by 90°.}

8.3.10 6.6 Optimality of the search algorithm

We have shown that a quantum computer can search N items, consulting the search oracle only $O(\sqrt{N})$ times. We now prove that no quantum algorithm can perform this task using

fewer than $\Omega(\sqrt{N})$ accesses to the search oracle, and thus the algorithm we have demonstrated is optimal.

Suppose the algorithm starts in the state $|\psi\rangle$. For simplicity, we prove the lower bound for the case where the search problem has a single solution, x. To determine x we are allowed to apply an oracle O_x which gives a phase shift of -1 to the solution $|x\rangle$ and leaves all other states invariant, $O_x = I - 2|x\rangle\langle x|$. We suppose the algorithm starts in a state $|\psi\rangle$ and applies the oracle O_x exactly k times, with unitary operations $U_1, U_2, \ldots, U_k$ interleaved between the oracle operations. Define

$$|\psi_k^x\rangle \equiv U_k O_x U_{k-1} O_x \ldots U_1 O_x |\psi\rangle \tag{6.38}$$

$$|\psi_k\rangle \equiv U_k U_{k-1} \ldots U_1 |\psi\rangle. \tag{6.39}$$

That is, $|\psi_k\rangle$ is the state that results when the sequence of unitary operations $U_1, \ldots, U_k$ is carried out, without the oracle operations. Let $|\psi_0\rangle = |\psi\rangle$. Our goal will be to bound the quantity

$$D_k \equiv \sum_x \|\psi_k^x - \psi_k\|^2 \tag{6.40}$$

where we use the notation ψ for $|\psi\rangle$ as a convenience to simplify formulas. Intuitively, D_k is a measure of the deviation after k steps caused by the oracle, from the evolution that would otherwise have ensued. If this quantity is small, then all the states $|\psi_k^x\rangle$ are roughly the same, and it is not possible to correctly identify x with high probability. The strategy of the proof is to demonstrate two things: (a) a bound on D_k that shows it can grow no faster than $O(k^2)$; and (b) a proof that D_k must be $\Omega(N)$ if it is to be possible to distinguish N alternatives. Combining these two results gives the desired lower bound.

First, we give an inductive proof that $D_k \leq 4k^2$. This is clearly true for $k = 0$, where $D_k = 0$. Note that

$$D_{k+1} = \sum_x \|O_x \psi_k^x - \psi_k\|^2 \tag{6.41}$$

$$= \sum_x \|O_x (\psi_k^x - \psi_k) + (O_x - I)\psi_k\|^2 . \tag{6.42}$$

Applying $\|b + c\|^2 \leq \|b\|^2 + 2\|b\|\|c\| + \|c\|^2$ with $b \equiv O_x(\psi_k^x - \psi_k)$ and $c \equiv (O_x - I)\psi_k = -2\langle x \mid \psi_k\rangle |x\rangle$, gives

$$D_{k+1} \leq \sum_x \left(\|\psi_k^x - \psi_k\|^2 + 4\|\psi_k^x - \psi_k\| \, |\langle x \mid \psi_k\rangle| + 4|\langle \psi_k \mid x\rangle|^2 \right). \tag{6.43}$$

Applying the Cauchy-Schwarz inequality to the second term on the right hand side, and noting that $\sum_x |\langle x \mid \psi_k\rangle|^2 = 1$ gives

$$D_{k+1} \leq D_k + 4\left(\sum_x \|\psi_k^x - \psi_k\|^2 \right)^{\frac{1}{2}} \left(\sum_{x'} |\langle \psi_k \mid x'\rangle|^2 \right)^{\frac{1}{2}} + 4 \tag{6.44}$$

$$\leq D_k + 4\sqrt{D_k} + 4. \tag{6.45}$$

By the inductive hypothesis $D_k \leq 4k^2$ we obtain

$$D_{k+1} \leq 4k^2 + 8k + 4 = 4(k+1)^2 \tag{6.46}$$

which completes the induction.
To complete the proof we need to show that the probability of success can only be high if D_k is $\Omega(N)$. We suppose $|\langle x \mid \psi_k^x\rangle|^2 \geq 1/2$ for all x, so that an observation yields a solution to the search problem with probability at least one-half. Replacing $|x\rangle$ by $e^{i\theta}|x\rangle$ does not change the probability of success, so without loss of generality we may assume that $\langle x \mid \psi_k^x\rangle = |\langle x \mid \psi_k^x\rangle|$, and therefore

$$\|\psi_k^x - x\|^2 = 2 - 2\,|\langle x \mid \psi_k^x\rangle| \leq 2 - \sqrt{2}. \tag{6.47}$$

Defining $E_k \equiv \sum_x \|\psi_k^x - x\|^2$ we see that $E_k \leq (2-\sqrt{2})N$. We are now in position to prove that D_k is $\Omega(N)$. Defining $F_k \equiv \sum_x \|x - \psi_k\|^2$ we have

$$\begin{aligned} D_k &= \sum_x \|(\psi_k^x - x) + (x - \psi_k)\|^2 && (6.48)\\ &\geq \sum_x \|\psi_k^x - x\|^2 - 2\sum_x \|\psi_k^x - x\|\,\|x - \psi_k\| + \sum_x \|x - \psi_k\|^2 && (6.49)\\ &= E_k + F_k - 2\sum_x \|\psi_k^x - x\|\,\|x - \psi_k\|\,. && (6.50) \end{aligned}$$

Applying the Cauchy-Schwarz inequality gives $\sum_x \|\psi_k^x - x\|\,\|x - \psi_k\| \leq \sqrt{E_k F_k}$, so we have

$$D_k \geq E_k + F_k - 2\sqrt{E_k F_k} = \left(\sqrt{F_k} - \sqrt{E_k}\right)^2. \tag{6.51}$$

In Exercise 6.15 you will show that $F_k \geq 2N - 2\sqrt{N}$. Combining this with the result $E_k \leq (2-\sqrt{2})N$ gives $D_k \geq cN$ for sufficiently large N, where c is any constant less than $(\sqrt{2} - \sqrt{2-\sqrt{2}})^2 \approx 0.42$. Since $D_k \leq 4k^2$ this implies that

$$k \geq \sqrt{cN/4} \tag{6.52}$$

Summarizing, to achieve a probability of success at least one-half for finding a solution to the search problem we must call the oracle $\Omega(\sqrt{N})$ times.

Exercise 6.15: Use the Cauchy-Schwarz inequality to show that for any normalized state vector $|\psi\rangle$ and set of N orthonormal basis vectors $|x\rangle$,

$$\sum_x \|\psi - x\|^2 \geq 2N - 2\sqrt{N} \tag{6.53}$$

Exercise 6.16: Suppose we merely require that the probability of an error being made is less than $1/2$ when averaged uniformly over the possible values for x, instead of for all values of x. Show that $O(\sqrt{N})$ oracle calls are still required to solve the search problem.

This result, that the quantum search algorithm is essentially optimal, is both exciting and disappointing. It is exciting because it tells us that for this problem, at least, we have fully plumbed the depths of quantum mechanics; no further improvement is possible. The disappointment arises because we might have hoped to do much better than the square root speedup offered by the quantum search algorithm. The sort of dream result
we might have hoped for a priori is that it would be possible to search an N item search space using $O(\log N)$ oracle calls. If such an algorithm existed, it would allow us to solve NP-complete problems efficiently on a quantum computer, since it could search all $2^{w(n)}$ possible witnesses using roughly $w(n)$ oracle calls, where the polynomial $w(n)$ is the length of a witness in bits. Unfortunately, such an algorithm is not possible. This is useful information for would-be algorithm designers, since it indicates that a naive search-based method for attacking NP-complete problems is guaranteed to fail.

Venturing into the realm of opinion, we note that many researchers believe that the essential reason for the difficulty of NP-complete problems is that their search space has essentially no structure, and that (up to polynomial factors) the best possible method for solving such a problem is to adopt a search method. If one takes this point of view, then it is bad news for quantum computing, indicating that the class of problems efficiently soluble on a quantum computer, **BQP**, does not contain the NP-complete problems. Of course, this is merely opinion, and it is still possible that the NP-complete problems contain some unknown structure that allows them to be efficiently solved on a quantum computer, or perhaps even on a classical computer. A nice example to illustrate this point is the problem of factoring, widely believed to be in the class NPI of problems intermediate in difficulty between **P** and the NP-complete problems. The key to the efficient quantum mechanical solution of the factoring problem was the exploitation of a structure 'hidden' within the problem - a structure revealed by the reduction to orderfinding. Even with this amazing structure revealed, it has not been found possible to exploit the structure to develop an efficient classical algorithm for factoring, although, of course, quantum mechanically the structure can be harnessed to give an efficient factoring algorithm! Perhaps a similar structure lurks in other problems suspected to be in NPI, such as the graph isomorphism problem, or perhaps even in the NP-complete problems themselves.

Exercise 6.17: (Optimality for multiple solutions) Suppose the search problem has M solutions. Show that $O(\sqrt{N/M})$ oracle applications are required to find a solution.

8.3.11 6.7 Black box algorithm limits

We conclude this chapter with a generalization of the quantum search algorithm which provides insightful bounds on the power of quantum computation. At the beginning of the chapter, we described the search problem as finding an n-bit integer x such that the function $f : \{0,1\}^n \rightarrow \{0,1\}$ evaluates to $f(x) = 1$. Related to this is the decision problem of whether or not there exists x such that $f(x) = 1$. Solving this decision problem is equivalently difficult, and can be expressed as computing the Boolean function $F(X) = X_0 \vee X_1 \vee \cdots \vee X_{N-1}$, where $\vee$ denotes the binary OR operation, $X_k \equiv f(k)$, and X denotes the set $\{X_0, X_1, \ldots, X_{N-1}\}$. More generally, we may wish to compute some function other than OR. For example, $F(X)$ could be the AND, PARITY (sum modulo two), or MAJORITY ($F(X) = 1$ if and only if more $X_k = 1$ than not) functions. In general, we can consider F to be any Boolean function. How fast (measured in number of queries) can a computer, classical or quantum, compute these functions, given an oracle for f ?

It might seem difficult to answer such questions without knowing something about the function f, but in fact a great deal can be determined even in this 'black box' model, where the means by which the oracle accomplishes its task is taken for granted, and complexity is measured only in terms of the number of required oracle queries. The analysis of the search algorithm in the previous sections demonstrated one way to approach such problems, but a more powerful approach for obtaining query complexities is the method of polynomials, which we now briefly describe.

Let us begin with some useful definitions. The deterministic query complexity $D(F)$ is the minimum number of oracle queries a classical computer must perform to compute F with certainty. The quantum equivalent, $Q_E(F)$, is the minimum number of oracle queries a quantum computer requires to compute F with certainty. Since a quantum computer produces probabilistic outputs by nature, a more interesting quantity is the bounded error complexity $Q_2(F)$, the minimum number of oracle queries a quantum computer requires to produce an output which equals F with probability at least 2/3. (The 2/3 is an arbitrary number - the probability need only be bounded finitely away from 1/2 in order to be boosted close to 1 by repetitions.) A related measure is the zeroerror complexity $Q_0(F)$, the minimum number of

oracle queries a quantum computer requires to produce an output which either equals F with certainty, or, with probability less than $1/2$, an admission of an inconclusive result. All these bounds must hold for any oracle function f (or in other words, any input X into F). Note that $Q_2(F) \leq Q_0(F) \leq Q_E(F) \leq D(F) \leq N$.

The method of polynomials is based upon the properties of minimum-degree multilinear polynomials (over the real numbers) which represent Boolean functions. All the polynomials we shall consider below are functions of $X_k \in \{0,1\}$ and are thus multilinear, since $X_k^2 = X_k$. We say that a polynomial $p : \mathbf{R}^N \to \mathbf{R}$ represents F if $p(X) = F(X)$ for all $X \in \{0,1\}^N$ (where $\mathbf{R}$ denotes the real numbers). Such a polynomial p always exists, since we can explicitly construct a suitable candidate:

$$p(X) = \sum_{Y \in \{0,1\}^N} F(Y) \prod_{k=0}^{N-1} \left[1 - (Y_k - X_k)^2\right] \tag{6.54}$$

That the minimum degree p is unique is left as Exercise 6.18 for the reader. The minimum degree of such a representation for F, denoted as $\deg(F)$, is a useful measure of the complexity of F. For example, it is known that $\deg(\text{OR}), \deg(\text{AND})$, and $\deg(\text{ PARITY })$ are all equal to N. In fact, it is known that the degree of most functions is of order N. Moreover, it has also been proven that

$$D(F) \leq 2 \deg(F)^4 \tag{6.55}$$

This result places an upper bound on the performance of deterministic classical computation in calculating most Boolean functions. Extending this concept, if a polynomial satisfies $|p(X) - F(X)| \leq 1/3$ for all $X \in \{0,1\}^N$, we say p approximates F, and $\widetilde{\deg}(F)$ denotes the minimum degree of such an approximating polynomial. Such measures are important in randomized classical computation and, as we shall see, in describing the quantum case. It is known that $\deg(\text{ PARITY }) = N$,

$$\widetilde{\deg}(\text{OR}) \in \Theta(\sqrt{N}) \quad \text{and} \quad \widetilde{\deg}(\text{AND}) \in \Theta(\sqrt{N}), \tag{6.56}$$

and

$$D(F) \leq 216 \widetilde{\deg}(F)^6 \tag{6.57}$$

The bounds of Equations (6.55) and (6.57) are only the best known at the time of writing; their proof is outside the scope of this book, but you may find further information about them in 'History and further reading'. It is believed that tighter bounds are possible, but these will be good enough for our purposes.

Exercise 6.18: Prove that the minimum degree polynomial representing a Boolean function $F(X)$ is unique.

Exercise 6.19: Show that $P(X) = 1 - (1 - X_0)(1 - X_1) \ldots (1 - X_{N-1})$ represents OR.

Polynomials naturally arise in describing the results of quantum algorithms. Let us write the output of a quantum algorithm $\mathcal{Q}$ which performs T queries to an oracle O as

$$\sum_{k=0}^{2^n-1} c_k |k\rangle. \tag{6.58}$$

We will show that the amplitudes c_k are polynomials of degree at most T in the variables $X_0, X_1, \ldots, X_{N-1}$. Any $\mathcal{Q}$ can be realized using the quantum circuit shown in Figure 6.10. The state $|\psi_0\rangle$ right before the first oracle query can be written as

$$|\psi_0\rangle = \sum_{ij} \left(a_{i0j}|i\rangle|0\rangle + a_{i1j}|i\rangle|1\rangle\right)|j\rangle, \tag{6.59}$$

where the first label corresponds to the n qubit oracle query, the next to a single qubit in which the oracle leaves its result, and the last to the $m-n-1$ working qubits used by $\mathcal{Q}$. After the oracle query, we obtain the state

$$|\psi_1\rangle = \sum_{ij} \left(a_{i0j}|i\rangle\,|X_i\rangle + a_{i1j}|i\rangle\,|X_i \oplus 1\rangle\right)|j\rangle, \tag{6.60}$$

but since X_i is either 0 or 1 , we can re-express this as

$$|\psi_1\rangle = \sum_{ij} \left[\left((1-X_i)\,a_{i0j} + X_i a_{i1j}\right)|i0\rangle + \left((1-X_i)\,a_{i1j} + X_i a_{i0j}\right)|i1\rangle\right]|j\rangle. \tag{6.61}$$

Note that in $|\psi_0\rangle$, the amplitudes of the computational basis states were of degree 0 in X, while those of $|\psi_1\rangle$ are of degree 1 (linear in X). The important observation is that any unitary operation which $\mathcal{Q}$ performs before or after the oracle query cannot change the degree of these polynomials, but each oracle call can increase the degree by at most one. Thus, after T queries, the amplitudes are polynomials of at most degree T. Moreover, measuring the final output (6.58) in the computational basis produces a result k with probability $P_k(X) = |c_k|^2$, which are real-valued polynomials in X of degree at most $2T$.

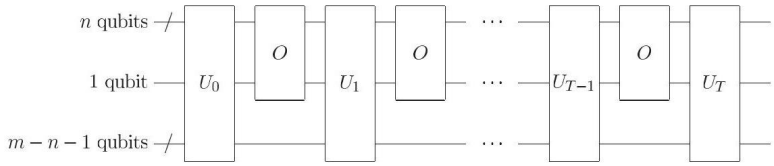


Figure 6.10. General quantum circuit for a quantum algorithm which performs T queries to an oracle O. $U_{0
, U_{1}, ···, U_{T}$ are arbitrary unitary transforms on m qubits, and the oracle acts on $n+1$ qubits.}

The total probability $P(X)$ of obtaining a one as the output from the algorithm is a sum over some subset of the polynomials $P_k(X)$, and thus also has degree at most $2T$. In the case that $\mathcal{Q}$ produces the correct answer with certainty we must have $P(X) = F(X)$, and thus $\deg(F) \leq 2T$, from which we deduce

$$Q_E(F) \geq \frac{\deg(F)}{2} \tag{6.62}$$

In the case where $\mathcal{Q}$ produces an answer with bounded probability of error it follows that $P(X)$ approximates $F(X)$, and thus $\widetilde{\deg}(F) \leq 2T$, from which we deduce

$$Q_2(F) \geq \frac{\widetilde{\deg}(F)}{2} \tag{6.63}$$

Combining (6.55) and (6.62), we find that

$$Q_E(F) \geq \left\lceil \frac{D(F)}{32} \right\rceil^{1/4} \tag{6.64}$$

Similarly, combining (6.57) and (6.63), we find that

$$Q_2(F) \geq \left\lceil \frac{D(F)}{13824} \right\rceil^{1/6} \tag{6.65}$$

This means that in computing Boolean functions using a black box, quantum algorithms may only provide a polynomial speedup over classical algorithms, at best - and even that is not generally possible (since $\deg(F)$ is $\Omega(N)$ for most functions). On the other hand, it is known that for $F = \mathrm{OR}, D(F) = N$, and the randomized classical query complexity $R(F) \in \Theta(N)$, whereas combining (6.63) and (6.56), and the known performance of the quantum search algorithm, shows that $Q_2(F) \in \Theta(\sqrt{N})$. This square root speedup is just what the quantum search algorithm achieves, and the method of polynomials indicates that the result can perhaps be generalized to a somewhat wider class of problems, but without extra information about the structure of the black box oracle function f, no exponential speedup over classical algorithms is possible.

Exercise 6.20: Show that $Q_0(\mathrm{OR}) \geq N$ by constructing a polynomial which represents the OR function from the output of a quantum circuit which computes OR with zero error.

Problem 6.1: (Finding the minimum) Suppose $x_1, \ldots, x_N$ is a database of numbers held in memory, as in Section 6.5. Show that only $O(\log(N)\sqrt{N})$ accesses to the memory are required on a quantum computer, in order to find the smallest element on the list, with probability at least one-half.

Problem 6.2: (Generalized quantum searching) Let $|\psi\rangle$ be a quantum state, and define $U_{|\psi\rangle} \equiv I - 2|\psi\rangle\langle\psi|$. That is, $U_{|\psi\rangle}$ gives the state $|\psi\rangle$ a -1 phase, and leaves states orthogonal to $|\psi\rangle$ invariant.
(1) Suppose we have a quantum circuit implementing a unitary operator U such that $U|0\rangle^{\otimes n} = |\psi\rangle$. Explain how to implement $U_{|\psi\rangle}$.
(2) Let $|\psi_1\rangle = |1\rangle, |\psi_2\rangle = (|0\rangle - |1\rangle)/\sqrt{2}, |\psi_3\rangle = (|0\rangle - i|1\rangle)/\sqrt{2}$. Suppose an unknown oracle O is selected from the set $U_{|\psi_1\rangle}, U_{|\psi_2\rangle}, U_{|\psi_3\rangle}$. Give a quantum algorithm which identifies the oracle with just one application of the oracle. (Hint: consider superdense coding.)
(3) Research: More generally, given k states $|\psi_1\rangle, \ldots, |\psi_k\rangle$, and an unknown oracle O selected from the set $U_{|\psi_1\rangle}, \ldots, U_{|\psi_k\rangle}$, how many oracle applications are required to identify the oracle, with high probability?

Problem 6.3: (Database retrieval) Given a quantum oracle which returns $|k, y \oplus X_k\rangle$ given an n qubit query (and one scratchpad qubit) $|k, y\rangle$, show that with high probability, all $N = 2^n$ bits of X can be obtained using only $N/2 + \sqrt{N}$ queries. This implies the general upper bound $Q_2(F) \leq N/2 + \sqrt{N}$ for any F.

Problem 6.4: (Quantum searching and cryptography) Quantum searching can, potentially, be used to speed up the search for cryptographic keys. The idea is to search through the space of all possible keys for decryption, in each case trying the key, and checking to see whether the decrypted message makes 'sense'. Explain why this idea doesn't work for the Vernam cipher (Section 12.6). When might it work for cryptosystems such as DES? (For a description of DES see, for example, [MvOV96] or [Sch96a].)

8.3.12 Summary of Chapter 6: Quantum search algorithms

- Quantum search algorithm: For a search problem with M solutions out of $N = 2^n$ possibilities, prepare $\sum_x |x\rangle$ and then repeat $G \equiv H^{\otimes n} U H^{\otimes n} O$ a total of $O(\sqrt{N/M})$ times, where O is the search oracle, $|x\rangle \rightarrow -|x\rangle$ if x is a solution, no change otherwise, and U takes $|0\rangle \rightarrow -|0\rangle$ and leaves all other computational basis states alone. Measuring yields a solution to the search problem with high probability.

- Quantum counting algorithm: Suppose a search problem has an unknown number M of

solutions. G has eigenvalues $\exp(\pm i\theta)$ where $\sin^2(\theta/2) = M/N$. The Fourier transform based phase estimation procedure enables us to estimate M to high accuracy using $O(\sqrt{N})$ oracle applications. Quantum counting, in turn, allows us to determine whether a given search problem has any solutions, and to find one if there are, even if the number of solutions is not known in advance.

- Polynomial bounds: For problems which are described as evaluations of total functions F (as opposed to partial functions, or 'promise' problems), quantum algorithms can give no more than a polynomial speedup over classical algorithms. Specifically, $Q_2(F) \geq [D(F)/13824]^{1/6}$. Moreover, the performance of the quantum search is optimal: it is $\Theta(\sqrt{N})$.

History and further reading

The quantum search algorithm and much of its further development and elaboration is due to Grover [Gro96, Gro97]. Boyer, Brassard, Høyer and Tapp [BBHT98] wrote an influential paper in which they developed the quantum search algorithm for cases where the number of solutions M is greater than one, and outlined the quantum counting algorithm, later developed in more detail by Brassard, Høyer, and Tapp [BHT98], and from the point of view of phase estimation by Mosca[Mos98]. That the Grover iteration can be understood as a product of two reflections was first pointed out in a review by Aharonov [Aha99b] . The continuous-time Hamiltonian (6.18) was first investigated by Farhi and Gutmann [FG98], from a rather different point of view than we take in Section 6.2. That Grover's algorithm is the best possible oracle-based search algorithm was proved by Bennett, Bernstein, Brassard and Vazirani[BBBV97]. The version of this proof we have presented is based upon that given by Boyer, Brassard, Høyer and Tapp [BBHT98]. Zalka[Zal99] has refined these proofs to show that the quantum search algorithm is, asymptotically, exactly optimal.

The method of polynomials for bounding the power of quantum algorithms was introduced into quantum computing by Beals, Buhrman, Cleve, Mosca, and de Wolf[BBC +98]. An excellent discussion is also available in Mosca's Ph.D. thesis [Mos99], on which much of the discussion in Section 6.7 is based. A number of results are quoted in that section without proof; here are the citations: Equation (6.55) is attributed to Nisan and Smolensky in [BBC+98], but otherwise is presently unpublished, (6.56) is derived from a theorem by Paturi [Pat92] and (6.57) is derived in [BBC+98]. A better bound than (6.65) is given in [BBC+98], but requires concepts such as block sensitivity which are outside the scope of this book. A completely different approach for bounding quantum black box algorithms, using arguments based on entanglement, was presented by Ambainis [Amb00].

Problem 6.1 is due to Dürr and Høyer [DH96]. Problem 6.3 is due to van Dam [van98a].

8.4 7 Quantum computers: physical realization

Computers in the future may weigh no more than 1.5 tons.

- Popular Mechanics, forecasting the relentless march of science, 1949

I think there is a world market for maybe five computers.

- Thomas Watson, chairman of IBM, 1943

Quantum computation and quantum information is a field of fundamental interest because we believe quantum information processing machines can actually be realized in Nature. Otherwise, the field would be just a mathematical curiosity! Nevertheless, experimental realization

of quantum circuits, algorithms, and communication systems has proven extremely challenging. In this chapter we explore some of the guiding principles and model systems for physical implementation of quantum information processing devices and systems.

We begin in Section 7.1 with an overview of the tradeoffs in selecting a physical realization of a quantum computer. This discussion provides perspective for an elaboration of a set of conditions sufficient for the experimental realization of quantum computation in Section 7.2. These conditions are illustrated in Sections 7.3 through 7.7, through a series of case studies, which consider five different model physical systems: the simple harmonic oscillator, photons and nonlinear optical media, cavity quantum electrodynamics devices, ion traps, and nuclear magnetic resonance with molecules. For each system, we briefly describe the physical apparatus, the Hamiltonian which governs its dynamics, means for controlling the system to perform quantum computation, and its principal drawbacks. We do not go into much depth in describing the physics of these systems; as each of these are entire fields unto themselves, that would be outside the scope of this book! Instead, we summarize just the concepts relevant to quantum computation and quantum information such that both the experimental challenge and theoretical potential can be appreciated. On the other hand, analyzing these systems from the standpoint of quantum information also provides a fresh perspective which we hope you will find insightful and useful, as it also allows strikingly simple derivations of some important physics. We conclude the chapter in Section 7.8 by discussing aspects of some other physical systems - quantum dots, superconducting gates, and spins in semiconductors - which are also of interest to this field. For the benefit of the reader wishing to catch just the highlights of each implementation, a summary is provided at the end of each section.

8.4.1 7.1 Guiding principles

What are the experimental requirements for building a quantum computer? The elementary units of the theory are quantum bits - two-level quantum systems; in Section 1.5 we took a brief look at why it is believed that qubits exist in Nature, and what physical forms they may take on. To realize a quantum computer, we must not only give qubits
some robust physical representation (in which they retain their quantum properties), but also select a system in which they can be made to evolve as desired. Furthermore, we must be able to prepare qubits in some specified set of initial states, and to measure the final output state of the system.

The challenge of experimental realization is that these basic requirements can often only be partially met. A coin has two states, and makes a good bit, but a poor qubit because it cannot remain in a superposition state (of 'heads' and 'tails') for very long. A single nuclear spin can be a very good qubit, because superpositions of being aligned with or against an external magnetic field can last a long time - even for days. But it can be difficult to build a quantum computer from nuclear spins because their coupling to the world is so small that it is hard to measure the orientation of single nuclei. The observation that the constraints are opposing is general: a quantum computer has to be well isolated in order to retain its quantum properties, but at the same time its qubits have to be accessible so that they can be manipulated to perform a computation and to read out the results. A realistic implementation must strike a delicate balance between these constraints, so that the relevant question is not how to build a quantum computer, but rather, how good a quantum computer can be built.

System	τ_Q	τ_{op}	$n_{op} = \lambda^{-1}$
Nuclear spin	$10^{-2} - 10^{8}$	$10^{-3} - 10^{-6}$	$10^{5} - 10^{14}$
Electron spin	10^{-3}	10^{-7}	10^{4}
Ion trap (In^{+})	10^{-1}	10^{-14}	10^{13}
Electron - Au	10^{-8}	10^{-14}	10^{6}
Electron - GaAs	10^{-10}	10^{-13}	10^{3}
Quantum dot	10^{-6}	10^{-9}	10^{3}
Optical cavity	10^{-5}	10^{-14}	10^{9}
Microwave cavity	10^{0}	10^{-4}	10^{4}

Figure 7.1. Crude estimates for decoherence times $\tau_{Q} (seconds), operation times τ_{op} (seconds), and maximum number of operations $n_{op} = \lambda^{-1} = \tau_Q/\tau_{op}$ for various candidate physical realizations of interacting systems of quantum bits. Despite the number of entries in this table, only three fundamentally different qubit representations are given: spin, charge, and photon. The ion trap utilizes either fine or hyperfine transitions of a trapped atom (Section 7.6), which correspond to electron and nuclear spin flips. The estimates for electrons in gold and GaAs, and in quantum dots are given for a charge representation, with an electrode or some confined area either containing an electron or not. In optical and microwave cavities, photons (of frequencies from gigahertz to hundreds of terahertz) populating different modes of the cavities represent the qubit. Take these estimates with a grain of salt: they are only meant to give some perspective on the wide range of possibilities.}

What physical systems are potentially good candidates for handling quantum information? A key concept in understanding the merit of a particular quantum computer realization is the notion of quantum noise (sometimes called decoherence), the subject of Chapter 8: processes corrupting the desired evolution of the system. This is because the length of the longest possible quantum computation is roughly given by the ratio of τ_Q, the time for which a system remains quantum-mechanically coherent, to τ_{op}, the time it takes to perform elementary unitary transformations (which involve at least two qubits). These two times are actually related to each other in many systems, since they are both
determined by the strength of coupling of the system to the external world. Nevertheless, $\lambda = \tau_{op}/\tau_Q$ can vary over a surprisingly wide range, as shown in Figure 7.1.

These estimates give some insight into the merits of different possible physical realizations of a quantum information processing machine, but many other important sources of noise and imperfections arise in actual implementations. For example, manipulations of a qubit represented by two electronic levels of an atom by using light to cause transitions between levels would also cause transitions to other electronic levels with some probability. These would also be considered noise processes, since they take the system out of the two states which define the qubit. Generally speaking, anything which causes loss of (quantum) information is a noise process - later, in Chapter 8, we discuss the theory of quantum noise in more depth.

8.4.2 7.2 Conditions for quantum computation

Let us return to discuss in detail the four basic requirements for quantum computation which were mentioned at the beginning of the previous section. These requirements are the abilities to:

1. Robustly represent quantum information

2. Perform a universal family of unitary transformations

3. Prepare a fiducial initial state

4. Measure the output result

8.4.3 7.2.1 Representation of quantum information

Quantum computation is based on transformation of quantum states. Quantum bits are two-level quantum systems, and as the simplest elementary building blocks for a quantum computer, they provide a convenient labeling for pairs of states and their physical realizations. Thus, for example, the four states of a spin- 3/2 particle, $|m = +3/2\rangle, |\ m = +1/2\rangle, |m = -1/2\rangle, |m = -3/2\rangle$, could be used to represent two qubits.

For the purpose of computation, the crucial realization is that the set of accessible states should be finite. The position x of a particle along a one-dimensional line is not generally a good set of states for computation, even though the particle may be in a quantum state $|x\rangle$, or even some superposition $\sum_x c_x|x\rangle$. This is because x has a continuous range of possibilities, and the Hilbert space has infinite size, so that in the absence of noise the information capacity is infinite. For example, in a perfect world, the entire texts of Shakespeare could be stored in (and retrieved from) the infinite number of digits in the binary fraction $x = 0.010111011001\ldots$. This is clearly unrealistic; what happens in reality is that the presence of noise reduces the number of distinguishable states to a finite number.

In fact, it is generally desirable to have some aspect of symmetry dictate the finiteness of the state space, in order to minimize decoherence. For example, a spin- 1/2 particle lives in a Hilbert space spanned by the $|\uparrow\rangle$ and $|\downarrow\rangle$ states; the spin state cannot be anything outside this two-dimensional space, and thus is a nearly ideal quantum bit when well isolated.

If the choice of representation is poor, then decoherence will result. For example, as described in Box 7.1, a particle in a finite square well which is just deep enough to contain two bound states would make a mediocre quantum bit, because transitions from
the bound states to the continuum of unbound states would be possible. These would lead to decoherence since they could destroy qubit superposition states. For single qubits, the figure of merit is the minimum lifetime of arbitrary superposition states; a good measure, used for spin states and atomic systems, is T_2, the ('transverse') relaxation time of states such as $(|0\rangle + |1\rangle)/\sqrt{2}$. Note that T_1, the ('longitudinal') relaxation time of the higher energy $|1\rangle$ state, is just a classical state lifetime, which is usually longer than T_2.

Box 7.1: Square wells and qubits

A prototypical quantum system is known as the 'square well,' which is a particle in a one-dimensional box, behaving according to Schrödinger's equation, (2.86). The Hamiltonian for this system is $H = p^2/2m + V(x)$, where $V(x) = 0$ for $0 < x < L$, and $V(x) = \infty$ otherwise. The energy eigenstates, expressed as wavefunctions in the position basis, are

$$|\psi_n\rangle = \sqrt{\frac{2}{L}} \sin\left(\frac{n\pi}{L}x\right) \tag{7.1}$$

where n is an integer, and $|\psi_n(t)\rangle = e^{-iE_n t}|\psi_n\rangle$, with $E_n = n^2\pi^2 m/2L^2$. These states have a discrete spectrum. In particular, suppose that we arrange matters such that only the two lowest energy levels need be considered in an experiment. We define an arbitrary wavefunction of interest as $|\psi\rangle = a|\psi_1\rangle + b|\psi_2\rangle$. Since

$$|\psi(t)\rangle = e^{-i(E_1+E_2)/2t}\left[ae^{-i\omega t}|\psi_1\rangle + be^{i\omega t}|\psi_2\rangle\right] \tag{7.2}$$

where $\omega = (E_1 - E_2)/2$, we can just forget about everything except a and b, and write our state abstractly as the two-component vector $|\psi\rangle = \begin{bmatrix} a \\ b \end{bmatrix}$. This two-level system represents a qubit! Does our two-level system transform like a qubit? Under time evolution, this qubit evolves under the effective Hamiltonian $H = \hbar\omega Z$, which can be disregarded by moving into the rotating frame. To perform operations to this qubit, we perturb H. Consider the effect of adding the additional term

$$\delta V(x) = -V_0(t)\frac{9\pi^2}{16L}\left(\frac{x}{L} - \frac{1}{2}\right) \tag{7.3}$$

to $V(x)$. In the basis of our two-level system, this can be rewritten by taking the matrix elements $V_{nm} = \langle\psi_n|\,\delta V(x)\,|\psi_m\rangle$, giving $V_{11} = V_{22} = 0$, and $V_{12} = V_{21} = V_0$, such that, to lowest order in V_0, the perturbation to H is $H_1 = V_0(t)X$. This generates rotations about the $\hat{x}$ axis. Similar techniques can be used to perform other single qubit operations, by manipulating the potential function.

This shows how a single qubit can be represented by the two lowest levels in a square well potential, and how simple perturbations of the potential can effect computational operations on the qubit. However, perturbations also introduce higher order effects, and in real physical systems boxes are not infinitely deep, other levels begin to enter the picture, and our two-level approximation begins to fail. Also, in reality, the controlling system is just another quantum system, and it couples to the one we are trying to do quantum computation with. These problems lead to decoherence.

8.4.4 7.2.2 Performance of unitary transformations

Closed quantum systems evolve unitarily as determined by their Hamiltonians, but to perform quantum computation one must be able to control the Hamiltonian to effect an arbitrary selection from a universal family of unitary transformations (as described in Section 4.5). For example, a single spin might evolve under the Hamiltonian $H = P_x(t)X + P_y(t)Y$, where $P_{\{x,y\}}$ are classically controllable parameters. From Exercise 4.10, we know that by manipulating P_x and P_y appropriately, one can perform arbitrary single spin rotations.

According to the theorems of Section 4.5, any unitary transform can be composed from single spin operations and controlled-not gates, and thus realization of those two kinds of quantum logic gates are natural goals for experimental quantum computation. However, implicitly required also is the ability to address individual qubits, and to apply these gates to select qubits or pairs of qubits. This is not simple to accomplish in many physical systems. For example, in an ion trap, one can direct a laser at one of many individual ions to selectively excite it, but only as long as the ions are spatially separated by a wavelength or more.

Unrecorded imperfections in unitary transforms can lead to decoherence. In Chapter 8 we shall see how the average effect of random kicks (small rotations to a single spin about its $\hat{z}$ axis) leads to loss of quantum information which is represented by the relative phases in a quantum state. Similarly, the cumulative effect of systematic errors is decoherence, when the information needed to be able to reverse them is lost. Furthermore, the control parameters in the Hamiltonian are only approximately classical controls: in reality, the controlling system is just another quantum system, and the true Hamiltonian should include the back-action of the control system upon the quantum computer. For example, instead of $P_x(t)$ in the above example, one actually has a Jaynes-Cummings type atomphoton interaction Hamiltonian (Section 7.5.2), with $P_x(t) = \sum_k \omega_k(t)\left(a_k + a_k^\dagger\right)$ or something similar being the cavity photon field. After interacting with a qubit, a photon can carry away information about the state of the qubit, and this is thus a decoherence process.

Two important figures of merit for unitary transforms are the minimum achievable fidelity $\mathcal{F}$ (Chapter 9), and the maximum time t_{op} required to perform elementary operations such as single spin rotations or a controlled-not gate.

8.4.5 7.2.3 Preparation of fiducial initial states

One of the most important requirements for being able to perform a useful computation, even classically, is to be able to prepare the desired input. If one has a box which can perform perfect computations, what use is it if numbers cannot be input? With classical machines, establishing a definite input state is rarely a difficulty - one merely sets some switches in the desired configuration and that defines the input state. However, with quantum systems this can be very difficult, depending on the realization of qubits.

Note that it is only necessary to be able to (repeatedly) produce one specific quantum state with high fidelity, since a unitary transform can turn it into any other desired input state. For example, being able to put n spins into the $|00\ldots0\rangle$ state is good enough. The fact that they may not stay there for very long due to thermal heating is a problem with the choice of representation.

Input state preparation is a significant problem for most physical systems. For example, ions can be prepared in good input states by physically cooling them into their ground state (Section 7.6), but this is challenging. Moreover, for physical systems in which ensembles of quantum computers are involved, extra concerns arise. In nuclear magnetic resonance (Section 7.7), each molecule can be thought of as a single quantum computer, and a large number of molecules is needed to obtain a measurable signal strength. Although qubits can remain in arbitrary superposition states for relatively long times, it is difficult to put all of the qubits in all of the molecules into the same state, because the energy difference $\hbar\omega$ between the $|0\rangle$ and $|1\rangle$ states is much smaller than $k_{\rm B}T$. On the other hand, simply letting the system equilibrate establishes it in a very well-known state, the thermal one, with the density matrix $\rho \approx e^{-\mathcal{H}/k_{\rm B}T}/\mathcal{Z}$, where $\mathcal{Z}$ is a normalization factor required to maintain $\mathrm{tr}(\rho) = 1$.

Two figures of merit are relevant to input state preparation: the minimum fidelity with which the initial state can be prepared in a given state $\rho_{\rm in}$, and the entropy of $\rho_{\rm in}$. The entropy is important because, for example, it is very easy to prepare the state $\rho_{\rm in} = I/2^n$ with high fidelity, but that is a useless state for quantum computation, since it is invariant under unitary transforms! Ideally, the input state is a pure state, with zero entropy. Generally, input states with non-zero entropy reduce the accessibility of the answer from the output result.

8.4.6 7.2.4 Measurement of output result

What measurement capability is required for quantum computation? For the purpose of the present discussion, let us think of measurement as a process of coupling one or more qubits to a classical system such that after some interval of time, the state of the qubits is indicated by the state of the classical system. For example, a qubit state $a|0\rangle + b|1\rangle$, represented by the ground and excited states of a two-level atom, might be measured by pumping the excited state and looking for fluorescence. If an electrometer indicates that fluorescence had been detected by a photomultiplier tube, then the qubit would collapse into the $|1\rangle$ state; this would happen with probability $|b|^2$. Otherwise, the electrometer would detect no charge, and the qubit would collapse into the $|0\rangle$ state.

An important characteristic of the measurement process for quantum computation is the wavefunction collapse which describes what happens when a projective measurement is performed (Section 2.2.5). The output from a good quantum algorithm is a superposition state which gives a useful answer with high probability when measured. For example, one step in

Shor's quantum factoring algorithm is to find an integer r from the measurement result, which is an integer close to qc/r, where q is the dimension of a Hilbert space. The output state is actually in a nearly uniform superposition of all possible values of c, but a measurement collapses this into a single, random integer, thus allowing r to be determined with high probability (using a continued fraction expansion, as was described in Chapter 5).

Many difficulties with measurement can be imagined; for example, inefficient photon counters and amplifier thermal noise can reduce the information obtained about measured qubit states in the scheme just described. Furthermore, projective measurements (sometimes called 'strong' measurements) are often difficult to implement. They require that the coupling between the quantum and classical systems be large, and switchable. Measurements should not occur when not desired; otherwise they can be a decoherence process.

Surprisingly, however, strong measurements are not necessary; weak measurements which are performed continuously and never switched off, are usable for quantum computation. This is made possible by completing the computation in time short compared with the measurement coupling, and by using large ensembles of quantum computers. These ensembles together give an aggregate signal which is macroscopically observable and indicative of the quantum state. Use of an ensemble introduces additional problems. For example, in the factoring algorithm, if the measurement output is $q\langle c\rangle/r$, the algorithm would fail because $\langle c\rangle$, the average value of c, is not necessarily an integer (and thus the continued fraction expansion would not be possible). Fortunately, it is possible to modify quantum algorithms to work with ensemble average readouts. This will be discussed further in Section 7.7.

A good figure of merit for measurement capability is the signal to noise ratio (SNR). This accounts for measurement inefficiency as well as inherent signal strength available from coupling a measurement apparatus to the quantum system.

8.4.7 7.3 Harmonic oscillator quantum computer

Before continuing on to describe a complete physical model for a realizable quantum computer, let us pause for a moment to consider a very elementary system - the simple harmonic oscillator - and discuss why it does not serve as a good quantum computer. The formalism used in this example will also serve as a basis for studying other physical systems.

8.4.8 7.3.1 Physical apparatus

An example of a simple harmonic oscillator is a particle in a parabolic potential well, $V(x) = m\omega^2 x^2/2$. In the classical world, this could be a mass on a spring, which oscillates back and forth as energy is transfered between the potential energy of the spring and the kinetic energy of the mass. It could also be a resonant electrical circuit, where the energy sloshes back and forth between the inductor and the capacitor. In these systems, the total energy of the system is a continuous parameter.

In the quantum domain, which is reached when the coupling to the external world becomes very small, the total energy of the system can only take on a discrete set of values. An example is given by a single mode of electromagnetic radiation trapped in a high Q cavity; the total amount of energy (up to a fixed offset) can only be integer multiples of $\hbar\omega$, an energy scale which is determined by the fundamental constant $\hbar$ and the frequency of the trapped radiation, ω.

The set of discrete energy eigenstates of a simple harmonic oscillator can be labeled as $|n\rangle$, where $n = 0, 1, \ldots, \infty$. The relationship to quantum computation comes by taking a finite subset of these states to represent qubits. These qubits will have lifetimes determined by physical parameters such as the cavity quality factor Q, which can be made very large by

increasing the reflectivity of the cavity walls. Moreover, unitary transforms can be applied by simply allowing the system to evolve in time. However, there are problems with this scheme, as will become clear below. We begin by studying the system Hamiltonian, then discuss how one might implement simple quantum logic gates such as the controlled-not.

8.4.9 7.3.2 The Hamiltonian

The Hamiltonian for a particle in a one-dimensional parabolic potential is

$$H = \frac{p^2}{2m} + \frac{1}{2}m\omega^2 x^2, \tag{7.4}$$

where p is the particle momentum operator, m is the mass, x is the position operator, and ω is related to the potential depth. Recall that x and p are operators in this expression (see Box 7.2), which can be rewritten as

$$H = \hbar\omega\left(a^\dagger a + \frac{1}{2}\right) \tag{7.5}$$

where $a^\dagger$ and a are creation and annihilation operators, defined as

$$a = \frac{1}{\sqrt{2m\hbar\omega}}(m\omega x + ip) \tag{7.6}$$

$$a^\dagger = \frac{1}{\sqrt{2m\hbar\omega}}(m\omega x - ip) \tag{7.7}$$

The zero point energy $\hbar\omega/2$ contributes an unobservable overall phase factor, which can be disregarded for our present purpose.

The eigenstates $|n\rangle$ of H, where $n = 0, 1, \ldots$, have the properties

$$a^\dagger a|n\rangle = n|n\rangle \tag{7.10}$$

$$a^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle \tag{7.11}$$

$$a|n\rangle = \sqrt{n}|n-1\rangle \tag{7.12}$$

Later, we will find it convenient to express interactions with a simple harmonic oscillator by introducing additional terms involving a and $a^\dagger$, and interactions between oscillators with terms such as $a_1^\dagger a_2 + a_1 a_2^\dagger$. For now, however, we confine our attention to a single oscillator.

Exercise 7.1: Using the fact that x and p do not commute, and that in fact $[x, p] = i\hbar$, explicitly show that $a^\dagger a = H/\hbar\omega - 1/2$.

Exercise 7.2: Given that $[x, p] = i\hbar$, compute $\left[a, a^\dagger\right]$.

Exercise 7.3: Compute $[H, a]$ and use the result to show that if $|\psi\rangle$ is an eigenstate of H with energy $E \geq n\hbar\omega$, then $a^n|\psi\rangle$ is an eigenstate with energy $E - n\hbar\omega$.

Exercise 7.4: Show that $|n\rangle = \frac{\left(a^\dagger\right)^n}{\sqrt{n!}}|0\rangle$.

Exercise 7.5: Verify that Equations (7.11) and (7.12) are consistent with (7.10) and the normalization condition $\langle n \mid n\rangle = 1$.

Time evolution of the eigenstates is given by solving the Schrödinger equation, (2.86), from which we find that the state $|\psi(0)\rangle = \sum_n c_n(0)|n\rangle$ evolves in time to become

$$|\psi(t)\rangle = e^{-iHt/\hbar}|\psi(0)\rangle = \sum_n c_n e^{-in\omega t}|n\rangle. \tag{7.13}$$

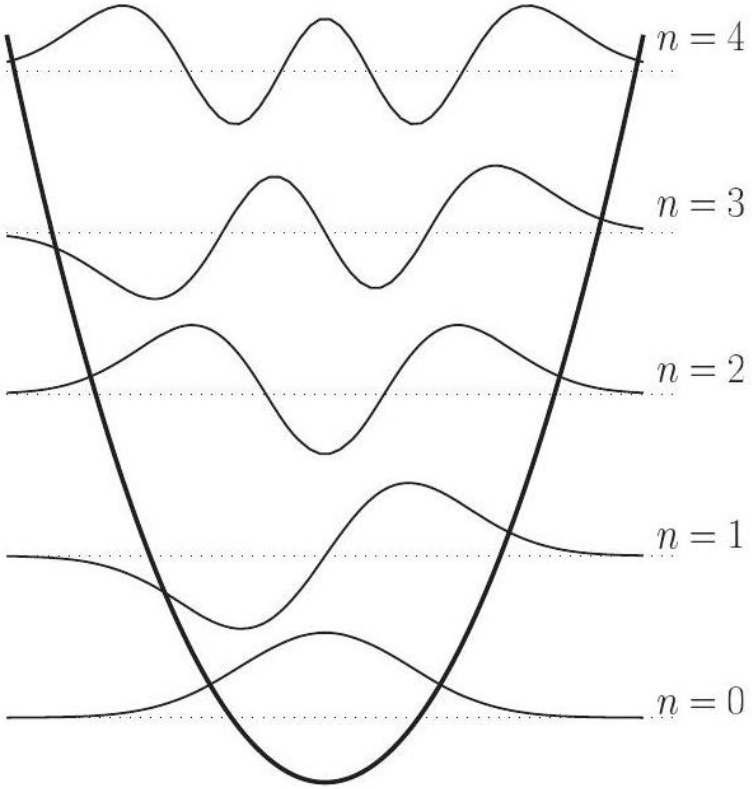
We will assume for the purpose of discussion that an arbitrary state can be perfectly prepared, and that the state of the system can be projectively measured (Section 2.2.3),

Box 7.2: The quantum harmonic oscillator

The harmonic oscillator is an extremely important and useful concept in the quantum description of the physical world, and a good way to begin to understand its properties is to determine the energy eigenstates of its Hamiltonian, (7.4). One way to do this is simply to solve the Schrödinger equation

$$\frac{\hbar^2}{2m}\frac{d^2\psi_n(x)}{dx^2} + \frac{1}{2}m\omega^2 x^2\psi_n(x) = E\psi_n(x) \tag{7.8}$$

for $\psi_n(x)$ and the eigenenergies E, subject to $\psi(x) \to 0$ at $x = \pm\infty$, and $\int |\psi(x)|^2 = 1$; the first five solutions are sketched here:



These wavefunctions describe the probability amplitudes that a particle in the harmonic oscillator will be found at different positions within the potential.
Although these pictures may give some intuition about what a physical system is doing in co-ordinate space, we will generally be more interested in the abstract algebraic properties of the states. Specifically, suppose $|\psi\rangle$ satisfies (7.8) with energy E. Then defining operators a and $a^\dagger$ as in (7.6)-(7.7), we find that since $\left[H, a^\dagger\right] = \hbar\omega a^\dagger$,

$$Ha^\dagger|\psi\rangle = \left(\left[H, a^\dagger\right] + a^\dagger H\right)|\psi\rangle = (\hbar\omega + E)a^\dagger|\psi\rangle, \tag{7.9}$$

that is, $a^\dagger|\psi\rangle$ is an eigenstate of H, with energy $E+\hbar\omega$! Similarly, $a|\psi\rangle$ is an eigenstate with energy $E - \hbar\omega$. Because of this, $a^\dagger$ and a are called raising and lowering operators. It follows that $a^{\dagger^n}|\psi\rangle$ are eigenstates for any integer n, with energies $E + n\hbar\omega$. There are thus an infinite number of energy eigenstates, whose energies are equally spaced apart, by $\hbar\omega$. Moreover, since H is positive definite, there must be some $|\psi_0\rangle$ for which $a\,|\psi_0\rangle = 0$; this is the ground state - the eigenstate of H with lowest energy. These results efficiently capture the essence of the quantum harmonic oscillator, and allow us to use a compact notation $|n\rangle$ for the eigenstates, where n is an integer, and $H|n\rangle = \hbar(n + 1/2)|n\rangle$. We shall often work with $|n\rangle, a$, and $a^\dagger$ in this chapter, as harmonic oscillators arise in the guise of many different physical systems.
but otherwise, there are no interactions with the external world, so that the system is perfectly closed.

8.4.10 7.3.3 Quantum computation

Suppose we want to perform quantum computation with the single simple harmonic oscillator described above. What can be done? The most natural choice for representation of qubits are the energy eigenstates $|n\rangle$. This choice allows us to perform a controlled-not gate in the following way. Recall that this transformation performs the mapping

$$\begin{aligned} |00\rangle_L \rightarrow \quad & |00\rangle_L \\ |01\rangle_L \rightarrow \quad & |01\rangle_L \\ |10\rangle_L \rightarrow \quad & |11\rangle_L \\ |11\rangle_L \rightarrow \quad & |10\rangle_L, \end{aligned} \tag{7.14}$$

on two qubit states (here, the subscript L is used to clearly distinguish 'logical' states in contrast to the harmonic oscillator basis states). Let us encode these two qubits using the mapping

$$\begin{aligned} |00\rangle_L &= |0\rangle \\ |01\rangle_L &= |2\rangle \\ |10\rangle_L &= (|4\rangle + |1\rangle)/\sqrt{2} \\ |11\rangle_L &= (|4\rangle - |1\rangle)/\sqrt{2}. \end{aligned} \tag{7.15}$$

Now suppose that at $t = 0$ the system is started in a state spanned by these basis states, and we simply evolve the system forward to time $t = \pi/\hbar\omega$. This causes the energy eigenstates to undergo the transformation $|n\rangle \rightarrow \exp\left(-i\pi a^\dagger a\right)|n\rangle = (-1)^n|n\rangle$, such that $|0\rangle, |2\rangle$, and $|4\rangle$ stay unchanged, but $|1\rangle \rightarrow -|1\rangle$. As a result, we obtain the desired controlled-NOT gate transformation.

In general, a necessary and sufficient condition for a physical system to be able to perform a unitary transform U is simply that the time evolution operator for the system, $T = \exp(-iHt)$, defined by its Hamiltonian H, has nearly the same eigenvalue spectrum as U. In the case above, the controlled-NOT gate was simple to implement because it only has eigenvalues +1 and -1 ; it was straightforward to arrange an encoding to obtain the same eigenvalues from the time evolution operator for the harmonic oscillator. The Hamiltonian for an oscillator could be perturbed to realize nearly any eigenvalue spectrum, and any number of qubits could be represented by simply mapping them into the infinite number of eigenstates of the system. This suggests that perhaps one might be able to realize an entire quantum computer in a single simple harmonic oscillator!

8.4.11 7.3.4 Drawbacks

Of course, there are many problems with the above scenario. Clearly, one will not always know the eigenvalue spectrum of the unitary operator for a certain quantum computation, even though one may know how to construct the operator from elementary gates. In fact, for most problems addressed by quantum algorithms, knowledge of the eigenvalue spectrum is tantamount to knowledge of the solution!

Another obvious problem is that the technique used above does not allow one computation to be cascaded with another, because in general, cascading two unitary transforms results in a new transform with unrelated eigenvalues.

Finally, the idea of using a single harmonic oscillator to perform quantum computation is flawed because it neglects the principle of digital representation of information. A Hilbert

space of 2^n dimensions mapped into the state space of a single harmonic oscillator would have to allow for the possibility of states with energy $2^n\hbar\omega$. In contrast, the same Hilbert space could be obtained by using n two-level quantum systems, which has an energy of at most $n\hbar\omega$. Similar comparisons can be made between a classical dial with 2^n settings, and a register of n classical bits. Quantum computation builds upon digital computation, not analog computation.

The main features of the harmonic oscillator quantum computer are summarized below (each system we consider will be summarized similarly, at the end of the corresponding section). With this, we leave behind us the study of single oscillators, and turn next to systems of harmonic oscillators, made of photons and atoms.

Harmonic oscillator quantum computer

- Qubit representation: Energy levels $|0\rangle, |1\rangle, \ldots, |2^n\rangle$ of a single quantum oscillator give n qubits.
- Unitary evolution: Arbitrary transforms U are realized by matching their eigenvalue spectrums to that given by the Hamiltonian $H = a^\dagger a$.
- Initial state preparation: Not considered.
- Readout: Not considered.
- Drawbacks: Not a digital representation! Also, matching eigenvalues to realize transformations is not feasible for arbitrary U, which generally have unknown eigenvalues.

8.4.12 7.4 Optical photon quantum computer

An attractive physical system for representing a quantum bit is the optical photon. Photons are chargeless particles, and do not interact very strongly with each other, or even with most matter. They can be guided along long distances with low loss in optical fibers, delayed efficiently using phase shifters, and combined easily using beamsplitters. Photons exhibit signature quantum phenomena, such as the interference produced in two-slit experiments. Furthermore, in principle, photons can be made to interact with each other, using nonlinear optical media which mediate interactions. There are problems with this ideal scenario; nevertheless, many things can be learned from studying the components, architecture, and drawbacks of an optical photon quantum information processor, as we shall see in this section.

8.4.13 7.4.1 Physical apparatus

Let us begin by considering what single photons are, how they can represent quantum states, and the experimental components useful for manipulating photons. The classical behavior of phase shifters, beamsplitters, and nonlinear optical Kerr media is described.

Photons can represent qubits in the following manner. As we saw in the discussion of the simple harmonic oscillator, the energy in an electromagnetic cavity is quantized in units of $\hbar\omega$. Each such quantum is called a photon. It is possible for a cavity to contain a superposition of zero or one photon, a state which could be expressed as a qubit $c_0|0\rangle + c_1|1\rangle$, but we shall do something different. Let us consider two cavities, whose total energy is $\hbar\omega$, and take the two states of a qubit as being whether the photon is in
one cavity ($|01\rangle$) or the other ($|10\rangle$). The physical state of a superposition would thus be written as $c_0|01\rangle + c_1|10\rangle$; we shall call this the dual-rail representation. Note that we shall focus on single photons traveling as a wavepacket through free space, rather than inside a cavity; one

can imagine this as having a cavity moving along with the wavepacket. Each cavity in our qubit state will thus correspond to a different spatial mode.

One scheme for generating single photons in the laboratory is by attenuating the output of a laser. A laser outputs a state known as a coherent state, $|\alpha\rangle$, defined as

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle, \tag{7.16}$$

where $|n\rangle$ is an n-photon energy eigenstate. This state, which has been the subject of thorough study in the field of quantum optics, has many beautiful properties which we shall not describe here. It suffices to understand just that coherent states are naturally radiated from driven oscillators such as a laser when pumped high above its lasing threshold. Note that the mean energy is $\langle\alpha|n|\alpha\rangle = |\alpha|^2$. When attenuated, a coherent state just becomes a weaker coherent state, and a weak coherent state can be made to have just one photon, with high probability.

Exercise 7.6: (Eigenstates of photon annihilation) Prove that a coherent state is an eigenstate of the photon annihilation operator, that is, show $a|\alpha\rangle = \lambda|\alpha\rangle$ for some constant λ.

For example, for $\alpha = \sqrt{0.1}$, we obtain the state $\sqrt{0.90}|0\rangle + \sqrt{0.09}|1\rangle + \sqrt{0.002}|2\rangle + \ldots$. Thus if light ever makes it through the attenuator, one knows it is a single photon with probability better than 95%; the failure probability is thus 5%. Note also that 90% of the time, no photons come through at all; this source thus has a rate of 0.1 photons per unit time. Finally, this source does not indicate (by means of some classical readout) when a photon has been output or not; two of these sources cannot be synchronized.

Better synchronicity can be achieved using parametric down-conversion. This involves sending photons of frequency ω_0 into a nonlinear optical medium such as KH_2PO_4 to generate photon pairs at frequencies $\omega_1 + \omega_2 = \omega_0$. Momentum is also conserved, such that $\vec{k}_1 + \vec{k}_2 = \vec{k}_3$, so that when a single ω_2 photon is (destructively) detected, then a single ω_1 photon is known to exist (Figure 7.2). By coupling this to a gate, which is opened only when a single photon (as opposed to two or more) is detected, and by appropriately delaying the outputs of multiple down-conversion sources, one can, in principle, obtain multiple single photons propagating in time synchronously, within the time resolution of the detector and gate.

Single photons can be detected with high quantum efficiency for a wide range of wavelengths, using a variety of technologies. For our purposes, the most important characteristic of a detector is its capability of determining, with high probability, whether zero or one photon exists in a particular spatial mode. For the dual-rail representation, this translates into a projective measurement in the computational basis. In practice, imperfections reduce the probability of being able to detect a single photon; the quantum efficiency $\eta (0 \leq \eta \leq 1)$ of a photodetector is the probability that a single photon incident on the detector generates a photocarrier pair that contributes to detector current. Other important characteristics of a detector are its bandwidth (time responsivity), noise, and 'dark counts' which are photocarriers generated even when no photons are incident.

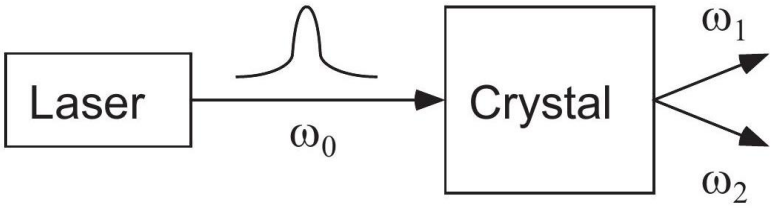


Figure 7.2. Parametric down-conversion scheme for generation of single photons.

Three of the most experimentally accessible devices for manipulating photon states are mirrors, phase shifters and beamsplitters. High reflectivity mirrors reflect photons and change their propagation direction in space. Mirrors with 0.01% loss are not unusual. We shall take these for granted in our scenario. A phase shifter is nothing more than a slab of transparent medium with index of refraction n different from that of free space, n_0; for example, ordinary borosilicate glass has $n \approx 1.5n_0$ at optical wavelengths. Propagation in such a medium through a distance L changes a photon's phase by e^{ikL}, where $k = n\omega/c_0$, and c_0 is the speed of light in vacuum. Thus, a photon propagating through a phase shifter will experience a phase shift of $e^{i(n-n_0)L\omega/c_0}$ compared to a photon going the same distance through free space.

Another useful component, the beamsplitter, is nothing more than a partially silvered piece of glass, which reflects a fraction R of the incident light, and transmits $1-R$. In the laboratory, a beamsplitter is usually fabricated from two prisms, with a thin metallic layer sandwiched in-between, schematically drawn as shown in Figure 7.3. It is convenient to define the angle θ of a beamsplitter as $\cos\theta = R$; note that the angle parameterizes the amount of partial reflection, and does not necessarily have anything to do with the physical orientation of the beamsplitter. The two inputs and two outputs of this device are related by

$$a_{\text{out}} = a_{in}\cos\theta + b_{in}\sin\theta \tag{7.17}$$

$$b_{\text{out}} = -a_{in}\sin\theta + b_{in}\cos\theta, \tag{7.18}$$

where classically we think of a and b as being the electromagnetic fields of the radiation at the two ports. Note that in this definition we have chosen a non-standard phase convention convenient for our purposes. In the special case of a 50/50 beamsplitter, $\theta = 45°$.

Nonlinear optics provides one final useful component for this exercise: a material

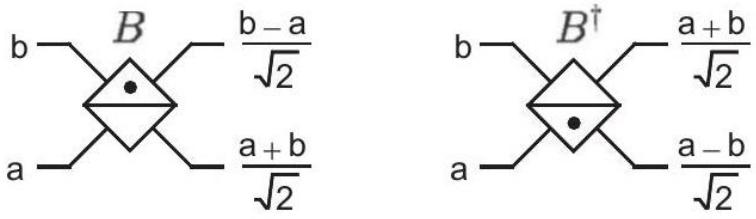


Figure 7.3. Schematic of an optical beamsplitter, showing the two input ports, the two output ports, and the phase conventions for a 50/50 beamsplitter ($\theta = \pi/4$). The beamsplitter on the right is the inverse of the one on the left (the two are distinguished by the dot drawn inside). The input-output relations for the mode operators a and b are given for $\theta = \pi/4$.

whose index of refraction n is proportional to the total intensity I of light going through it:

$$n(I) = n + n_2 I. \tag{7.19}$$

This is known as the optical Kerr effect, and it occurs (very weakly) in materials as mundane as glass and sugar water. In doped glasses, n_2 ranges from 10^{-14} to 10^{-7} cm^2/W, and in semiconductors, from 10^{-10} to 10^2. Experimentally, the relevant behavior is that when two beams of light of equal intensity are nearly co-propagated through a Kerr medium, each beam will experience an extra phase shift of $e^{in_2 IL\omega/c_0}$ compared to what happens in the single beam case. This would be ideal if the length L could be arbitrarily long, but unfortunately that fails because most Kerr media are also highly absorptive, or scatter light out of the desired spatial mode. This is the primary reason why a single photon quantum computer is impractical, as we shall discuss in Section 7.4.3.

We turn next to a quantum description of these optical components.

8.4.14 7.4.2 Quantum computation

Arbitrary unitary transforms can be applied to quantum information, encoded with single photons in the $c_0|01\rangle + c_1|10\rangle$ dual-rail representation, using phase shifters, beamsplitters, and nonlinear optical Kerr media. How this works can be understood in the following manner, by giving a quantum-mechanical Hamiltonian description of each of these devices.

The time evolution of a cavity mode of electromagnetic radiation is modeled quantum-mechanically by a harmonic oscillator, as we saw in Section 7.3.2. $|0\rangle$ is the vacuum state, $|1\rangle = a^\dagger|0\rangle$ is a single photon state, and in general, $|n\rangle = \frac{a^{\dagger n}}{\sqrt{n!}}|0\rangle$ is an n-photon state, where $a^\dagger$ is the creation operator for the mode. Free space evolution is described by the Hamiltonian

$$H = \hbar\omega a^\dagger a \tag{7.20}$$

and applying (7.13), we find that the state $|\psi\rangle = c_0|0\rangle + c_1|1\rangle$ evolves in time to become $|\psi(t)\rangle = c_0|0\rangle + c_1 e^{-i\omega t}|1\rangle$. Note that the dual-rail representation is convenient because free evolution only changes $|\varphi\rangle = c_0|01\rangle + c_1|10\rangle$ by an overall phase, which is undetectable. Thus, for that manifold of states, the evolution Hamiltonian is zero.

Phase shifter. A phase shifter P acts just like normal time evolution, but at a different rate, and localized to only the modes going through it. That is because light slows down in a medium with larger index of refraction; specifically, it takes $\Delta \equiv (n - n_0)\, L/c_0$ more time to propagate a distance L in a medium with index of refraction n than in vacuum. For example, the action of P on the vacuum state is to do nothing: $P|0\rangle = |0\rangle$, but on a single photon state, one obtains $P|1\rangle = e^{i\Delta}|1\rangle$.

P performs a useful logical operation on a dual-rail state. Placing a phase shifter in one mode retards its phase evolution with respect to another mode, which travels the same distance but without going through the shifter. For dual-rail states this transforms $c_0|01\rangle + c_1|10\rangle$ to $c_0 e^{-i\Delta/2}|01\rangle + c_1 e^{i\Delta/2}|10\rangle$, up to an irrelevant overall phase. Recall from Section 4.2 that this operation is nothing more than a rotation,

$$R_z(\Delta) = e^{-iZ\Delta/2} \tag{7.21}$$

where we take as the logical zero $|0_L\rangle = |01\rangle$ and one $|1_L\rangle = |10\rangle$, and Z is the usual

Pauli operator. One can thus think of P as resulting from time evolution under the Hamiltonian

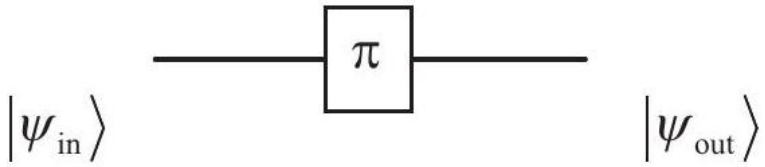
$$H = (n_0 - n)\, Z, \tag{7.22}$$

where $P = \exp(-iHL/c_0)$.

Exercise 7.7: Show that the circuit below transforms a dual-rail state by

$$|\psi_{\text{out}}\rangle = \begin{bmatrix} e^{i\pi} & 0 \\ 0 & 1 \end{bmatrix} |\psi_{\text{in}}\rangle\,, \tag{7.23}$$

if we take the top wire to represent the $|01\rangle$ mode, and $|10\rangle$ the bottom mode, and the boxed π to represent a phase shift by π :



Note that in such 'optical circuits', propagation in space is explicitly represented by putting in lumped circuit elements such as in the above, to represent phase evolution. In the dual-rail representation, evolution according to (7.20) changes the logical state only by an unobservable global phase, and thus we are free to disregard it and keep only relative phase shifts.

Exercise 7.8: Show that $P|\alpha\rangle = \left|\alpha e^{i\Delta}\right\rangle$ where $|\alpha\rangle$ is a coherent state (note that, in general, α is a complex number!).

Beamsplitter. A similar Hamiltonian description of the beamsplitter also exists, but instead of motivating it phenomenologically, let us begin with the Hamiltonian and show how the expected classical behavior, Equations (7.17)-(7.18) arises from it. Recall that the beamsplitter acts on two modes, which we shall describe by the creation (annihilation) operators $a\left(a^\dagger\right)$ and $b\left(b^\dagger\right)$. The Hamiltonian is

$$H_{bs} = i\theta\left(ab^\dagger - a^\dagger b\right), \tag{7.24}$$

and the beamsplitter performs the unitary operation

$$B = \exp\left[\theta\left(a^\dagger b - ab^\dagger\right)\right]. \tag{7.25}$$

The transformations effected by B on a and b, which will later be useful, are found to be

$$BaB^\dagger = a\cos\theta + b\sin\theta \quad \text{and} \quad BbB^\dagger = -a\sin\theta + b\cos\theta. \tag{7.26}$$

We verify these relations using the Baker-Campbell-Hausdorf formula (also see Exercise 4.49)

$$e^{\lambda G}Ae^{-\lambda G} = \sum_{n=0}^{\infty}\frac{\lambda^n}{n!}C_n, \tag{7.27}$$

where λ is a complex number, A, G, and C_n are operators, and C_n is defined recursively as the sequence of commutators $C_0 = A, C_1 = [G, C_0], C_2 = [G, C_1], C_3 = [G, C_2], \ldots, C_n = [G, C_{n-1}]$. Since it follows from $\left[a, a^\dagger\right] = 1$ and $\left[b, b^\dagger\right] = 1$ that $[G, a] = -b$ and $[G, b] = a$, for $G \equiv a^\dagger b - ab^\dagger$, we obtain for the expansion of $BaB^\dagger$ the series coefficients
$C_0 = a, C_1 = [G, a] = -b, C_2 = [G, C_1] = -a, C_3 = [G, C_2] = -[G, C_0] = b$, which in general are

$$C_{n\ \text{even}} = i^n a \tag{7.28}$$
$$C_{n\ \text{odd}} = i^{n+1} b. \tag{7.29}$$

From this, our desired result follows straightforwardly:

$$BaB^\dagger = e^{\theta G}ae^{-\theta G} \tag{7.30}$$
$$= \sum_{n=0}^{\infty}\frac{\theta^n}{n!}C_n \tag{7.31}$$
$$= \sum_{n\ \text{even}}\frac{(i\theta)^n}{n!}a + i\sum_{n\ \text{odd}}\frac{(i\theta)^n}{n!}b \tag{7.32}$$
$$= a\cos\theta - b\sin\theta \tag{7.33}$$

The transform $BbB^\dagger$ is trivially found by swapping a and b in the above solution. Note that the beamsplitter operator arises from a deep relationship between the beamsplitter and the algebra of $SU(2)$, as explained in Box 7.3.

In terms of quantum logic gates, B performs a useful operation. First note that $B|00\rangle = |00\rangle$, that is, when no photons in either input mode exist, no photons will exist in either output mode. When one photon exists in mode a, recalling that $|1\rangle = a^\dagger|0\rangle$, we find that

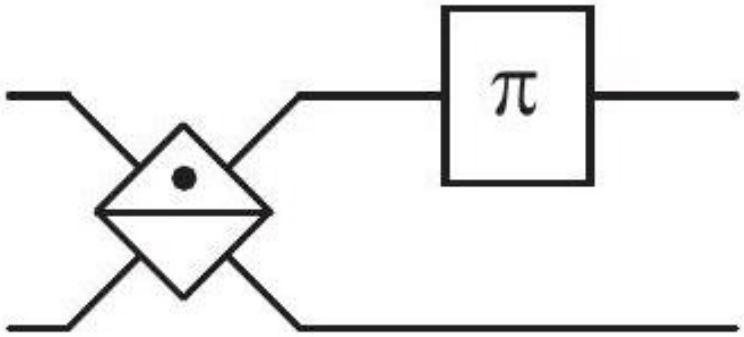
$$B|01\rangle = Ba^\dagger|00\rangle = Ba^\dagger B^\dagger B|00\rangle = \left(a^\dagger \cos\theta + b^\dagger \sin\theta\right)|00\rangle = \cos\theta|01\rangle + \sin\theta|10\rangle. \quad (7.34)$$

Similarly, $B|10\rangle = \cos\theta|10\rangle - \sin\theta|01\rangle$. Thus, on the $|0_L\rangle$ and $|1_L\rangle$ manifold of states, we may write B as

$$B = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} = e^{i\theta Y}. \quad (7.35)$$

Phase shifters and beamsplitters together allow arbitrary single qubit operations to be performed to our optical qubit. This a consequence of Theorem 4.1 on page 175, which states that all single qubit operations can be generated from $\hat{z}$-axis rotations $R_z(\alpha) = \exp(-i\alpha Z/2)$, and $\hat{y}$-axis rotations, $R_y(\alpha) = \exp(-i\alpha Y/2)$. A phase shifter performs R_z rotations, and a beamsplitter performs R_y rotations.

Exercise 7.9: (Optical Hadamard gate) Show that the following circuit acts as a Hadamard gate on dual-rail single photon states, that is, $|01\rangle \rightarrow (|01\rangle + |10\rangle)/\sqrt{2}$ and $|10\rangle \rightarrow (|01\rangle - |10\rangle)/\sqrt{2}$ up to an overall phase:



Exercise 7.10: (Mach-Zehnder interferometer) Interferometers are optical tools used to measure small phase shifts, which are constructed from two beamsplitters. Their basic principle of operation can be understood by this simple exercise.

1. Note that this circuit performs the identity operation:

Box 7.3: $SU(2)$ **Symmetry and quantum beamsplitters**

There is an interesting connection between the Lie group $SU(2)$ and the algebra of two coupled harmonic oscillators, which is useful for understanding the quantum beamsplitter transformation. Identify

$$a^\dagger a - b^\dagger b \rightarrow Z \quad (7.36)$$

$$a^\dagger b \rightarrow \sigma_+ \quad (7.37)$$

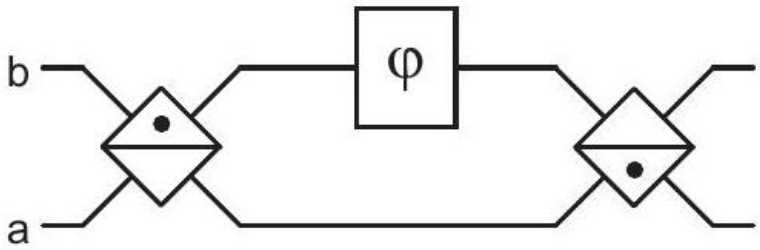
$$ab^\dagger \rightarrow \sigma_-, \quad (7.38)$$

where Z is the Pauli operator, and $\sigma_\pm = (X \pm iY)/2$ are raising and lowering operators defined in terms of Pauli X and Y. From the commutation relations for a, $a^\dagger, b$, and $b^\dagger$, it is easy to verify that these definitions satisfy the usual commutation relations for the Pauli operators, (2.40). Also note that the total number operator, $a^\dagger a + b^\dagger b$, commutes with σ_z, σ_+, and σ_-, as it should, being an invariant quantity under rotations in the $SU(2)$ space. Using $X = a^\dagger b + ab^\dagger$ and $Y = -i\left(a^\dagger b - ab^\dagger\right)$ in the traditional $SU(2)$ rotation operator

$$R(\hat{n}, \theta) = e^{-i\theta\vec{\sigma}\cdot\hat{n}/2} \quad (7.39)$$

gives us the desired beamsplitter operator when $\hat{n}$ is taken to be the $-\hat{y}$-axis.

2. Compute the rotation operation (on dual-rail states) which this circuit performs, as a function of the phase shift φ :



Exercise 7.11: What is $B|2,0\rangle$ for $\theta = \pi/4$?

Exercise 7.12: (Quantum beamsplitter with classical inputs) What is $B|\alpha\rangle|\beta\rangle$ where $|\alpha\rangle$ and $|\beta\rangle$ are two coherent states as in Equation (7.16)? (Hint: recall that $|n\rangle = \frac{\left(a^\dagger\right)^n}{\sqrt{n!}}|0\rangle$.)

Nonlinear Kerr media. The most important effect of a Kerr medium is the cross phase modulation it provides between two modes of light. That is classically described by the n_2 term in (7.19), which is effectively an interaction between photons, mediated by atoms in the Kerr medium. Quantum-mechanically, this effect is described by the Hamiltonian

$$H_{xpm} = -\chi a^\dagger a b^\dagger b, \tag{7.40}$$

where a and b describe two modes propagating through the medium, and for a crystal of length L we obtain the unitary transform

$$K = e^{i\chi L a^\dagger a b^\dagger b} \tag{7.41}$$

χ is a coefficient related to n_2, and the third order nonlinear susceptibility coefficient usually denoted as $\chi^{(3)}$. That the expected classical behavior arises from this Hamiltonian is left as Exercise 7.14 for the reader.

By combining Kerr media with beamsplitters, a controlled-NOT gate can be constructed in the following manner. For single photon states, we find that

$$K|00\rangle = |00\rangle \tag{7.42}$$
$$K|01\rangle = |01\rangle \tag{7.43}$$
$$K|10\rangle = |10\rangle \tag{7.44}$$
$$K|11\rangle = e^{i\chi L}|11\rangle \tag{7.45}$$

and let us take $\chi L = \pi$, such that $K|11\rangle = -|11\rangle$. Now consider two dual-rail states, that is, four modes of light. These live in a space spanned by the four basis states $|e_{00}\rangle = |1001\rangle, |e_{01}\rangle = |1010\rangle, |e_{10}\rangle = |0101\rangle, |e_{11}\rangle = |0110\rangle$. Note that we have flipped the usual order of the two modes for the first pair, for convenience (physically, the two modes are easily swapped using mirrors). Now, if a Kerr medium is applied to act upon the two middle modes, then we find that $K|e_i\rangle = |e_i\rangle$ for all i except $K|e_{11}\rangle = -|e_{11}\rangle$. This is useful because the controlled-NOT operation can be factored into

$$\underbrace{\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}}_{U_{CN}} = \underbrace{\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}}_{I \otimes H} \underbrace{\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}}_{K} \underbrace{\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}}_{I \otimes H}, \quad (7.46)$$

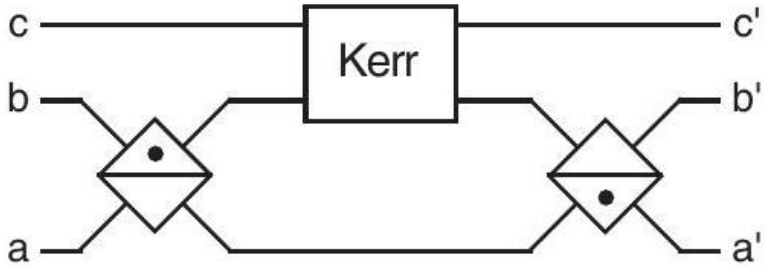
where H is the single qubit Hadamard transform (simply implemented with beamsplitters and phase shifters), and K is the Kerr interaction we just considered, with $\chi L = \pi$. Such an apparatus has been considered before, for constructing a reversible classical optical logic gate, as described in Box 7.4; in the single photon regime, it also functions as a quantum logic gate.

Summarizing, the CNOT can be constructed from Kerr media, and arbitrary single qubit operations realized using beamsplitters and phase shifters. Single photons can be created using attenuated lasers, and detected with photodetectors. Thus, in theory, a quantum computer can be implemented using these optical components!

Exercise 7.13: (Optical Deutsch-Jozsa quantum circuit) In Section 1.4.4 (page 34), we described a quantum circuit for solving the one-bit Deutsch-Jozsa problem. Here is a version of that circuit for single photon states (in the dual-rail representation), using beamsplitters, phase shifters, and nonlinear Kerr media:

Box 7.4: The quantum optical Fredkin gate

An optical Fredkin gate can be built using two beamsplitters and a nonlinear Kerr medium as shown in this schematic diagram:



This performs the unitary transform $U = B^\dagger K B$, where B is a 50/50 beamsplitter, K is the Kerr cross phase modulation operator $K = e^{i\xi b^\dagger b c^\dagger c}$, and $\xi = \chi L$ is the product of the coupling constant and the interaction distance. This simplifies to give

$$U = \exp\left[i\xi c^\dagger c \left(\frac{b^\dagger - a^\dagger}{2}\right)\left(\frac{b - a}{2}\right)\right] \quad (7.47)$$

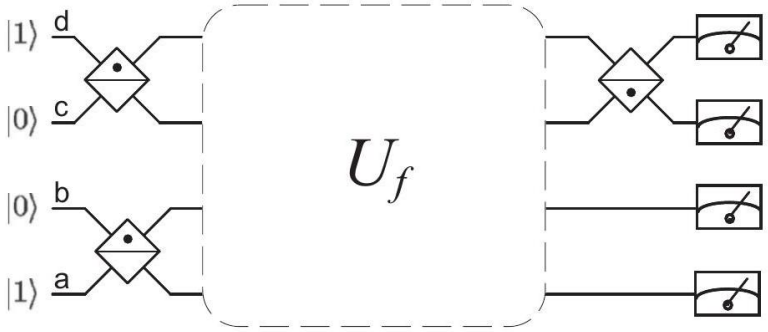
$$= e^{i\frac{\pi}{2}b^\dagger b} e^{\frac{\xi}{2}c^\dagger c\left(a^\dagger b - b^\dagger a\right)} e^{-i\frac{\pi}{2}b^\dagger b} e^{i\frac{\xi}{2}a^\dagger a c^\dagger c} e^{i\frac{\xi}{2}b^\dagger b c^\dagger c}. \quad (7.48)$$

The first and third exponentials are constant phase shifts, and the last two phase shifts come from cross phase modulation. All those effects are not fundamental, and can be compensated for. The interesting term is the second exponential, which is defines the quantum Fredkin operator

$$F(\xi) = \exp\left[\frac{\xi}{2} c^\dagger c \left(a^\dagger b - b^\dagger a\right)\right]. \quad (7.49)$$

The usual (classical) Fredkin gate operation is obtained for $\xi = \pi$, in which case when no photons are input at c, then $a' = a$ and $b' = b$, but when a single photon is input at c, then $a' = b$ and $b' = a$. This can be understood by realizing that $F(\chi)$ is like a controlled-beamsplitter

operator, where the rotation angle is $\xi c^\dagger c$. Note that this description does not use the dual-rail representation; in that representation, this Fredkin gate corresponds to a controlled-not gate.



1. Construct circuits for the four possible classical functions U_f using Fredkin gates and beamsplitters.

2. Why are no phase shifters necessary in this construction?

3. For each U_f show explicitly how interference can be used to explain how the quantum algorithm works.

4. Does this implementation work if the single photon states are replaced by coherent states?

Exercise 7.14: (Classical cross phase modulation) To see that the expected classical behavior of a Kerr medium is obtained from the definition of K, Equation (7.41), apply it to two modes, one with a coherent state and the other in state $|n\rangle$; that is, show that

$$K|\alpha\rangle|n\rangle = \left|\alpha e^{i\chi L n}\right\rangle |n\rangle. \tag{7.50}$$

Use this to compute

$$\rho_a = \mathrm{Tr}_b \left[K|\alpha\rangle|\beta\rangle\langle\beta|\langle\alpha|K^\dagger\right] \tag{7.51}$$

$$= e^{-|\beta|^2} \sum_m \frac{|\beta|^{2m}}{m!} \left|\alpha e^{i\chi L m}\right\rangle \left\langle \alpha e^{i\chi L m}\right|, \tag{7.52}$$

and show that the main contribution to the sum is for $m = |\beta|^2$.

8.4.15 7.4.3 Drawbacks

The single photon representation of a qubit is attractive. Single photons are relatively simple to generate and measure, and in the dual-rail representation, arbitrary single qubit operations are possible. Unfortunately, interacting photons is difficult - the best nonlinear Kerr media available are very weak, and cannot provide a cross phase modulation of π between single photon states. In fact, because a nonlinear index of refraction is usually obtained by using a medium near an optical resonance, there is always some absorption associated with the nonlinearity, and it can theoretically be estimated that in the best such arrangement, approximately 50 photons must be absorbed for each photon which experiences a π cross phase modulation. This means that the outlook for building quantum computers from traditional nonlinear optics components is slim at best.

Nevertheless, from studying this optical quantum computer, we have gained some valuable insight into the nature of the architecture and system design of a quantum computer. We now can see what an actual quantum computer might look like in the laboratory (if only sufficiently

good components were available to construct it), and a striking feature is that it is constructed nearly completely from optical interferometers. In the apparatus, information is encoded both in the photon number and the phase of the photon, and interferometers are used to convert between the two representations. Although it is feasible to construct stable optical interferometers, if an alternate, massive representation of a qubit were chosen, then it could rapidly become difficult to build stable interferometers because of the shortness of typical de Broglie wavelengths. Even with the optical representation, the multiple interlocked interferometers which would be needed to realize a large quantum algorithm would be a challenge to stabilize in the laboratory.

Historically, optical classical computers were once thought to be promising replacements for electronic machines, but they ultimately failed to live up to expectations when sufficiently nonlinear optical materials were not discovered, and when their speed and parallelism advantages did not sufficiently outweigh their alignment and power disadvantages. On the other hand, optical communications is a vital and important area; one reason for this is that for distances longer than one centimeter, the energy needed to transmit
a bit using a photon over a fiber is smaller than the energy required to charge a typical 50 ohm electronic transmission line covering the same distance. Similarly, it may be that optical qubits may find a natural home in communication of quantum information, such as in quantum cryptography, rather than in computation.

Despite the drawbacks facing optical quantum computer realizations, the theoretical formalism which describes them is absolutely fundamental in all the other realizations we shall study in the remainder of this chapter. In fact, you may think of what we shall turn to next as being just another kind of optical quantum computer, but with a different (and better!) kind of nonlinear medium.

Optical photon quantum computer

- Qubit representation: Location of single photon between two modes, $|01\rangle$ and $|10\rangle$, or polarization.
- Unitary evolution: Arbitrary transforms are constructed from phase shifters (R_z rotations), beamsplitters (R_y rotations), and nonlinear Kerr media, which allow two single photons to cross phase modulate, performing $\exp[i\chi L|11\rangle\langle 11|]$.
- Initial state preparation: Create single photon states (e.g. by attenuating laser light).
- Readout: Detect single photons (e.g. using a photomultipler tube).
- Drawbacks: Nonlinear Kerr media with large ratio of cross phase modulation strength to absorption loss are difficult to realize.

8.4.16 7.5 Optical cavity quantum electrodynamics

Cavity quantum electrodynamics (QED) is a field of study which accesses an important regime involving coupling of single atoms to only a few optical modes. Experimentally, this is made possible by placing single atoms within optical cavities of very high Q; because only one or two electromagnetic modes exist within the cavity, and each of these has a very high electric field strength, the dipole coupling between the atom and the field is very high. Because of the high Q, photons within the cavity have an opportunity to interact many times with the atoms before escaping. Theoretically, this technique presents a unique opportunity to control and study single quantum systems, opening many opportunities in quantum chaos, quantum feedback control, and quantum computation.

In particular, single-atom cavity QED methods offer a potential solution to the dilemma with the optical quantum computer described in the previous section. Single photons can be good carriers of quantum information, but they require some other medium in order to interact with each other. Because they are bulk materials, traditional nonlinear optical Kerr media are unsatisfactory in satisfying this need. However, well isolated single atoms might not necessarily suffer from the same decoherence effects, and moreover, they could also provide cross phase modulation between photons. In fact, what if the state of single photons could be efficiently transfered to and from single atoms, whose interactions could be controlled? This potential scenario is the topic of this section.

8.4.17 7.5.1 Physical apparatus

The two main experimental components of a cavity QED system are the electromagnetic cavity and the atom. We begin by describing the basic physics of cavity modes, and then summarize basic ideas about atomic structure and the interaction of atoms with light.

Fabry-Perot cavity

The main interaction involved in cavity QED is the dipolar interaction $\vec{d} \cdot \vec{E}$ between an electric dipole moment $\vec{d}$ and an electric field $\vec{E}$. How large can this interaction be? It is difficult in practice to change the size of $\vec{d}$; however, $|\vec{E}|$ is experimentally accessible, and one of the most important tools for realizing a very large electric field in a narrow band of frequencies and in a small volume of space, is the Fabry-Perot cavity.

In the approximation that the electric field is monochromatic and occupies a single spatial mode, it can be given a very simple quantum-mechanical description:

$$\vec{E}(r) = i\vec{\epsilon}E_0 \left[ae^{ikr} - a^\dagger e^{-ikr}\right] \tag{7.56}$$

As described in Box 7.5, these approximations are appropriate for the field in a FabryPerot cavity. Here, $k = \omega/c$ is the spatial frequency of the light, E_0 is the field strength, $\vec{\epsilon}$ is the polarization, and r is the position at which the field is desired. a and $a^\dagger$ are creation and annihilation operators for photons in the mode, and behave as described in Section 7.4.2. Note that the Hamiltonian governing the evolution of the field in the cavity is simply

$$H_{\text{field}} = \hbar\omega a^\dagger a \tag{7.57}$$

and this is consistent with the semiclassical notion that the energy is the volume integral of $|\vec{E}|^2$ in the cavity.

Exercise 7.15: Plot (7.55) as a function of field detuning φ, for $R_1 = R_2 = 0.9$.

Two-level atoms

Until this section of the chapter, we have discussed only photons, or interactions such as the cross phase modulation between photons mediated by a semiclassical medium. Now, let us turn our attention to atoms, their electronic structure, and their interactions with photons. This is, of course, a very deep and well-developed field of study; we shall only describe a small part of it that touches upon quantum computation.

The electronic energy eigenstates of an atom can be very complicated (see Box 7.6), but for our purposes modeling an atom as having only two states is an excellent approximation. This two-level atom approximation can be valid because we shall be concerned with the interaction with monochromatic light and, in this case, the only relevant energy levels are those satisfying two conditions: their energy difference matches the energy of the incident photons, and

symmetries ('selection rules') do not inhibit the transition. These conditions arise from basic conservation laws for energy, angular momentum, and parity. Energy conservation is no more than the condition that

$$\hbar\omega = E_2 - E_1, \tag{7.58}$$

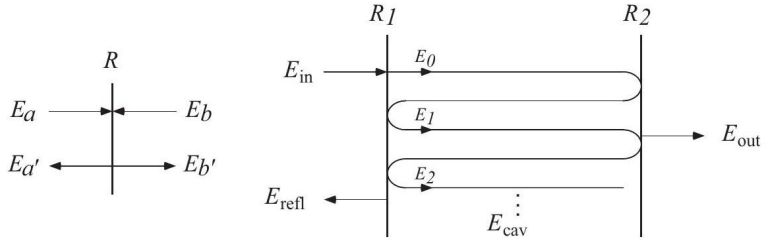
where E_2 and E_1 are two eigenenergies of the atom. Angular momentum and parity conservation requirements can be illustrated by considering the matrix element of $\hat{r}$ between two orbital wavefunctions, $\langle l_1, m_1 | \hat{r} | l_2, m_2 \rangle$. Without loss of generality, we can

Box 7.5: The Fabry-Perot cavity

A basic component of a Fabry-Perot cavity is a partially silvered mirror, off which incident light E_a and E_b partially reflect and partially transmit, producing the output fields $E_{a'}$ and $E_{b'}$. These are related by the unitary transform

$$\begin{bmatrix} E_{a'} \\ E_{b'} \end{bmatrix} = \begin{bmatrix} \sqrt{R} & \sqrt{1-R} \\ \sqrt{1-R} & -\sqrt{R} \end{bmatrix} \begin{bmatrix} E_a \\ E_b \end{bmatrix} \tag{7.53}$$

where R is the reflectivity of the mirror, and the location of the '-' sign is a convention chosen as given here for convenience.



A Fabry-Perot cavity is made from two plane parallel mirrors of reflectivities R_1 and R_2, upon which light $E_{\rm in}$ is incident from the outside, as shown in the figure. Inside the cavity, light bounces back and forth between the two mirrors, such that the field acquires a phase shift $e^{i\varphi}$ on each round-trip; φ is a function of the path length and the frequency of the light. Thus, using (7.53), we find the cavity internal field to be

$$E_{\rm cav} = \sum_k E_k = \frac{\sqrt{1-R_1}E_{\rm in}}{1 + e^{i\varphi}\sqrt{R_1 R_2}}, \tag{7.54}$$

where $E_0 = \sqrt{1-R_1}E_{\rm in}$, and $E_k = -e^{i\varphi}\sqrt{R_1 R_2}E_{k-1}$. Similarly, we find $E_{\rm out} = e^{i\varphi}/2\sqrt{1-R_2}$, and $E_{\rm refl} = \sqrt{R_1}E_{\rm in} + \sqrt{1-R_1}\sqrt{R_2}e^{i\varphi}E_{\rm cav}$.
One of the most important characteristics of a Fabry-Perot cavity for our purpose is the power in the cavity internal field as a function of the input power and field frequency,

$$\frac{P_{\rm cav}}{P_{\rm in}} = \left|\frac{E_{\rm cav}}{E_{\rm in}}\right|^2 = \frac{1-R_1}{\left|1 + e^{i\varphi}\sqrt{R_1 R_2}\right|^2} \tag{7.55}$$

Two aspects are noteworthy. First, frequency selectivity is given by the fact that $\varphi = \omega d/c$, where d is the mirror separation, c is the speed of light, and ω is the frequency of the field. Physically, it comes about because of constructive and destructive interference between the cavity field and the front surface reflected light. And second, on resonance, the cavity field achieves a maximum value which is approximately $1/(1-R)$ times the incident field. This property is invaluable for cavity QED.
take $\hat{r}$ to be in the $\hat{x} - \hat{y}$ plane, such that it can be expressed in terms of spherical harmonics (Box 7.6) as

$$\hat{r} = \sqrt{\frac{3}{8\pi}} \left[(-r_x + ir_y) Y_{1,+1} + (r_x + ir_y) Y_{1,-1} \right] \tag{7.59}$$

In this basis, the relevant terms in $\langle l, m_1 | \hat{r} | l, m_2 \rangle$ are

$$\int Y^*_{l_1 m_1} Y_{1m} Y_{l_2 m_2} d\Omega \tag{7.60}$$

Recall that $m = \pm 1$; this integral is non-zero only when $m_2 - m_1 = \pm 1$ and $\Delta l = \pm 1$. The first condition is the conservation of angular momentum, and the second, parity, under the dipole approximation where $\langle l_1, m_1 | \hat{r} | l_2, m_2 \rangle$ becomes relevant. These conditions are selection rules which are important in the two-level atom approximation.

Exercise 7.16: (Electric dipole selection rules) Show that (7.60) is non-zero only when $m_2 - m_1 = \pm 1$ and $\Delta l = \pm 1$.

In reality, light is never perfectly monochromatic; it is generated from some source such as a laser, in which longitudinal modes, pump noise, and other sources give rise to a finite linewidth. Also, an atom coupled to the external world never has perfectly defined energy eigenstates; small perturbations such as nearby fluctuating electric potentials, or even interaction with the vacuum, cause each energy level to be smeared out and become a distribution with finite width.

Nevertheless, by choosing an atom and excitation energy carefully, and by taking advantage of the selection rules, it is possible to arrange circumstances such that the two-level atom approximation is superb. The whole point of this procedure is that in this approximation, if $|\psi_1\rangle$ and $|\psi_2\rangle$ are the two selected levels, then the matrix elements of the $\hat{r}$ are

$$r_{ij} = \langle \psi_i | \hat{r} | \psi_j \rangle \approx r_0 Y, \tag{7.65}$$

where r_0 is some constant, and Y is a Pauli operator (Section 2.1.3; that we obtain Y as opposed to X doesn't really matter - it is a matter of convention, and convenience, for later calculations). This will be relevant in describing interactions between the atom and incident electric fields. The Hamiltonian of the atom itself, in this two-level subspace, is simply

$$H_{\text{atom}} = \frac{\hbar \omega_0}{2} Z \tag{7.66}$$

where $\hbar\omega_0$ is the difference of the energies of the two levels, since the two states are energy eigenstates.

8.4.18 7.5.2 The Hamiltonian

The $\vec{d} \cdot \vec{E}$ interaction between an atom and a cavity confined electric field can be approximated quite well by a much simpler model, in the two-level approximation of the atom, using the quantization of the field in the cavity, and the minute size of the electron compared to the wavelength of the field. Using the fact that $\vec{d} \propto \hat{r}$ (the electric dipole size is charge times distance), we can combine (7.56) with (7.65) to obtain the interaction

$$H_I = -igY \left(a - a^\dagger \right), \tag{7.67}$$

Box 7.6: Energy levels of an atom

The electrons of an atom behave like particles in a three dimensional box, with a Hamiltonian of the form

$$H_{\rm A} = \sum_k \frac{|\vec{p}_k|^2}{2m} - \frac{Ze^2}{r_k} + H_{\rm rel} + H_{\rm ee} + H_{\rm so} + H_{\rm hf} \tag{7.61}$$

where the first two terms describe the balance of the electrons' kinetic energy with the Coulomb attraction of the negatively charged electrons to the positively charged nucleus, $H_{\rm rel}$ is a relativistic correction term, $H_{\rm ee}$ describes electron-electron couplings and contributions from the fermionic nature of the electrons, $H_{\rm so}$ is the spin orbit interaction, which can be interpreted as the spin of the electron interacting with a magnetic field generated by its orbit around the atom, and $H_{\rm hf}$ is the hyperfine interaction: the electron spin interacting with the magnetic field generated by the nucleus. The energy eigenstates of $H_{\rm A}$ are generally pretty well categorized according to three integers or half-integers (quantum numbers): n, the principle quantum number; l, the orbital angular momentum; and m, its $\hat{z}$ component. In addition, S, the total electron spin, and I, the nuclear spin, are often important. The eigenvalues of H are roughly determined to order α^2 by n, to slightly smaller order by $H_{\rm ee}$, to order α^4 by $H_{\rm rel}$ and $H_{\rm so}$, and to order $\approx 10^{-3}\alpha^4$ by $H_{\rm hf}$, where $\alpha = 1/137$ is the dimensionless fine structure constant.

The derivation of n is simple and follows the usual one-dimensional Schrödinger equation solutions for a particle in a box, since the Coulomb confining potential is dependent on radial distance only. However, orbital angular momentum is a feature of being in three dimensions which deserves some explanation. The essential properties arise from the angular dependence of the coordinate representation of $H_{\rm A}$, in which $\vec{p}$ becomes the Laplacian operator $\vec{\nabla}^2$, giving the Schrödinger equation

$$\frac{\Phi(\varphi)}{\sin\theta}\frac{d}{d\theta}\left(\sin\theta\frac{d\Theta}{d\theta}\right) + \frac{\Theta(\theta)}{\sin^2\theta}\frac{d\Phi(\varphi)}{d\varphi^2} + l(l+1)\Theta(\theta)\Phi(\varphi) = 0 \tag{7.62}$$

where θ and φ are the usual spherical coordinates, and Φ and Θ are the eigenfunctions we desire. The solutions $Y_{lm}(\theta,\varphi) = \Theta_{lm}(\theta)\Phi_m(\varphi)$ are the spherical harmonics

$$Y_{lm}(\theta,\varphi) \equiv (-1)^m\sqrt{\frac{2l+1}{4\pi}\frac{(l-m)!}{(l+m)!}}P_{lm}(\cos\theta)e^{im\varphi}, \tag{7.63}$$

where P_{lm} are the usual Legendre functions

$$P_{lm}(x) = \frac{(1-x^2)^{m/2}}{2^l l!}\frac{d^{m+l}}{dx^{m+l}}\left(x^2-1\right)^l \tag{7.64}$$

In these equations, $-l \le m \le l$, and it can be shown that m and l must be either integer or half-integer. l is known as the orbital angular momentum, and m is its component along the $\hat{z}$ axis. Similarly, the electron spins S and the nuclear spin I have components m_s and m_i. As you can see, the description of the energy states of an atom can be quite complicated! Summarizing: for our purposes we may think of the eigenenergies of an atom as being determined by seven numbers: n, l, m, S, m_s, I, and m_i.

where we have chosen $r = 0$ as the point to place the atom (and thus evaluate $\vec{E}$), and also oriented the atom such that $\hat{r}$ is aligned properly with the electric field vector. g is some constant (we need not be concerned about the specific values here, just the forms) which describes the strength of the interaction. The i is present simply to allow g to be real, since H_I must be Hermitian. H_I can be simplified further, by recognizing that it contains terms which are generally small; to see these, it is useful to define the Pauli raising and lowering operators,

$$\sigma_\pm = \frac{X \pm iY}{2}, \tag{7.68}$$

such that we can re-express H_I as

$$H_I = g\left(\sigma_+ - \sigma_-\right)\left(a - a^\dagger\right) \tag{7.69}$$

The terms containing $\sigma_+ a^\dagger$ and $\sigma_- a$ oscillate at twice the frequencies of interest, which are ω and ω_0, and dropping them is a fairly good approximation (the rotating wave approximation) which leads us to the total Hamiltonian $H = H_{\text{atom}} + H_{\text{field}} + H_I$,

$$H = \frac{\hbar\omega_0}{2} Z + \hbar\omega a^\dagger a + g\left(a^\dagger\sigma_- + a\sigma_+\right) \tag{7.70}$$

where, again, just to recap: the Pauli operators act on the two-level atom, $a^\dagger, a$ are raising and lowering operators on the single mode field, ω is the frequency of the field, ω_0 is the frequency of the atom, and g is the coupling constant for the interaction between atom and field. This is the fundamental theoretical tool in the study of cavity QED, the Faynes-Cummings Hamiltonian, which describes interactions between two-level atoms and an electromagnetic field.

This Hamiltonian can be written in another convenient form by noting that $N = a^\dagger a + Z/2$ is a constant of the motion, that is $[H, N] = 0$, so that we find

$$H = \hbar\omega N + \delta Z + g\left(a^\dagger\sigma_- + a\sigma_+\right) \tag{7.71}$$

where $\delta = (\omega_0 - \omega)/2$ is known as the detuning - the frequency difference between the field and atomic resonance. This Hamiltonian, the Jaynes-Cummings Hamiltonian, is very important, and we shall be spending nearly all of the rest of the chapter studying its properties and guises in different physical systems.

Exercise 7.17: (Eigenstates of the Jaynes-Cummings Hamiltonian) Show that

$$|\chi_n\rangle = \frac{1}{\sqrt{2}}[|n,1\rangle + |n+1,0\rangle] \tag{7.72}$$

$$|\bar{\chi}_n\rangle = \frac{1}{\sqrt{2}}[|n,1\rangle - |n+1,0\rangle] \tag{7.73}$$

are eigenstates of the Jaynes-Cummings Hamiltonian (7.71) for $\omega = \delta = 0$, with the eigenvalues

$$H|\chi_n\rangle = g\sqrt{n+1}\,|\chi_n\rangle \tag{7.74}$$

$$H|\bar{\chi}_n\rangle = -g\sqrt{n+1}\,|\bar{\chi}_n\rangle \tag{7.75}$$

where the labels in the ket are | field, atom $\rangle$.

8.4.19 7.5.3 Single-photon single-atom absorption and refraction

The most interesting regime in cavity QED, for our purposes, is that in which single photons interact with single atoms. This is an unusual regime, in which traditional concepts (such as index of refraction and permittivity) in classical theories of electromagnetism break down. In particular, we would like to utilize a single atom to obtain a nonlinear interaction between photons.

Let us begin by showing one striking and general characteristic of the atom-field system known as Rabi oscillations. Without loss of generality we may neglect N, since it only contributes a fixed phase. Recalling that time evolution is given by $U = e^{-iHt}$ (here and in the following, it will often be convenient to drop $\hbar$, and we shall do so freely), and focusing on the case of at most a single excitation in the field mode, where

$$H = -\begin{bmatrix} \delta & 0 & 0 \\ 0 & \delta & g \\ 0 & g & -\delta \end{bmatrix} \tag{7.76}$$

(the basis states are $|00\rangle, |01\rangle, |10\rangle$, from left to right and top to bottom, where the left label corresponds to the field, and the right one to the atom), we find that

$$\begin{aligned} U &= e^{-i\delta t}|00\rangle\langle 00| \\ &+ \left(\cos\Omega t + i\frac{\delta}{\Omega}\sin\Omega t\right)|01\rangle\langle 01| \\ &+ \left(\cos\Omega t - i\frac{\delta}{\Omega}\sin\Omega t\right)|10\rangle\langle 10| \\ &- i\frac{g}{\Omega}\sin\Omega t(|01\rangle\langle 10| + |10\rangle\langle 01|) \end{aligned} \tag{7.77}$$

The interesting behavior is in the last line of this equation, which shows that the atom and field oscillate back and forth exchanging a quantum of energy, at the Rabi frequency $\Omega = \sqrt{g^2 + \delta^2}$.

Exercise 7.18: (Rabi oscillations) Show that (7.77) is correct by using

$$e^{i\vec{n}\cdot\vec{\sigma}} = \sin|n| + i\hat{n}\cdot\vec{\sigma}\cos|n| \tag{7.78}$$

to exponentiate H. This is an unusually simple derivation of the Rabi oscillations and the Rabi frequency; ordinarily, one solves coupled differential equations to obtain Ω, but here we obtain the essential dynamics just by focusing on the single-atom, single-photon subspace!

The transformation of the photon, in interacting with a single atom, can be obtained by tracing over the atom's state (Section 2.4.3). The probability that an initial photon $|1\rangle$ is absorbed by the atom (which we assume starts in its ground state, $|0\rangle$) is simply

$$\chi_r = \sum_k |\langle 0k|U|10\rangle|^2 = \frac{g^2}{g^2+\delta^2}\sin^2\Omega t \tag{7.79}$$

This has the usual Lorentzian profile expected for absorption as a function of detuning δ from resonance.

The refractive index (of the single atom!) is given by the matrix elements of U in which the atom stays in the ground state. The phase shift experienced by the photon is
the difference in the angle of rotation experienced by the $|1\rangle$ and the $|0\rangle$ states of the field, tracing over the atom. This is found to be

$$\chi_i = \arg\left[e^{i\delta t}\left(\cos\Omega t - i\frac{\delta}{\Omega}\sin\Omega t\right)\right]. \tag{7.80}$$

For fixed non-zero δ, as the coupling g is decreased, the absorption probability χ_r decreases as g^2, but the phase shift χ_i remains nearly constant. This is the origin of materials which can perform phase shifts without scattering much light.

Exercise 7.19: (Lorentzian absorption profile) Plot (7.79) for $t = 1$ and $g = 1.2$, as a function of the detuning δ, and (if you know it) the corresponding classical result. What are the oscillations due to?

Exercise 7.20: (Single photon phase shift) Derive (7.80) from U, and plot it for $t = 1$ and $g = 1.2$, as a function of the detuning δ. Compare with δ/Ω^2.

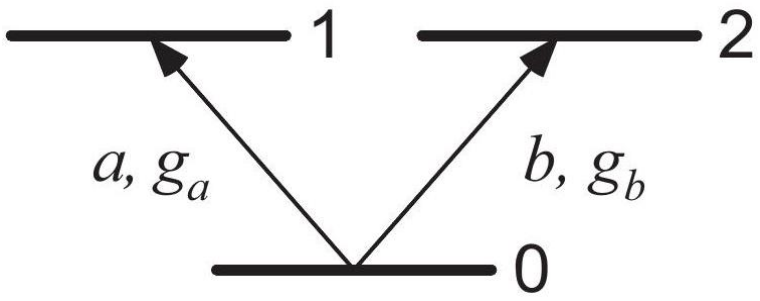


Figure 7.4. Three level atom (with levels 0,1 , and 2) interacting with two orthogonal polarizations of light, described by the operators a and b. The atom-photon couplings are respectively $g_{a} $ and g_b. The energy differences between 0 and 1 , and between 0 and 2 are assumed to be nearly equal.}

A natural application of the atom-photon interaction is to study what happens when two different photon modes (each containing at most one photon) interact with the same atom. This can give rise to a nonlinear interaction between the two modes. Recall from Section 7.4.2 that nonlinear Kerr media can be described phenomenologically as media which induce a cross phase modulation with Hamiltonian of the form $H = \chi a^\dagger a b^\dagger b$. There, we did not see how that effect arises from fundamental interactions. Using the present formalism, the origin of the Kerr effect can be illustrated using a simple model, in which two polarizations of light interact with a three-level atom, as shown in Figure 7.4. This is described by a modified version of the Jaynes-Cummings Hamiltonian,

$$H = \delta \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} + g_a \left(a \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} + a^\dagger \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \right) + g_b \left(b \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} + b^\dagger \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \right), \tag{7.81}$$

where the basis elements for the 3×3 atom operators are $|0\rangle, |1\rangle$, and $|2\rangle$. In matrix form, the relevant terms in H are found to be the block-diagonal matrix

$$H = \begin{bmatrix} H_0 & 0 & 0 \\ 0 & H_1 & 0 \\ 0 & 0 & H_2 \end{bmatrix}, \tag{7.82}$$

where

$$H_0 = -\delta \tag{7.83}$$

$$H_1 = \begin{bmatrix} -\delta & g_a & 0 & 0 \\ g_a & \delta & 0 & 0 \\ 0 & 0 & -\delta & g_b \\ 0 & 0 & g_b & \delta \end{bmatrix} \tag{7.84}$$

$$H_2 = \begin{bmatrix} -\delta & g_a & g_b \\ g_a & \delta & 0 \\ g_b & 0 & \delta \end{bmatrix}. \tag{7.85}$$

in the basis $\mid a, b, \text{ atom } \rangle = |000\rangle$ for $H_0, |100\rangle, |001\rangle, |010\rangle, |002\rangle$ for H_1, and $|110\rangle$, $|011\rangle, |102\rangle$ for H_2, across the columns from left to right. Exponentiating to give $U = \exp(iHt)$ allows one to find the single photon phase shifts $\varphi_a = \arg(\langle 100|U|100\rangle) - \arg(\langle 000|U|000\rangle)$ and $\varphi_b = \arg(\langle 010|U|010\rangle) - \arg(\langle 000|U|000\rangle)$ and the two photon phase shift $\varphi_{ab} = \arg(\langle 110|U|110\rangle) - \arg(\langle 000|U|000\rangle)$. For linear media, one would expect that $\varphi_{ab} = \varphi_a + \varphi_b$, that is, the two photon state has twice the phase shift of the single photon state, since $\exp\left[-i\omega\left(a^\dagger a + b^\dagger b\right)\right]|11\rangle = \exp(-2i\omega)|11\rangle$. However, this system behaves nonlinearly, and gives $\chi_3 \equiv \varphi_{ab} - \varphi_a - \varphi_b$ as shown in Figure 7.5. In this physical system, this Kerr effect arises from the slight amplitude for the atom to exchange quanta between the two optical modes.

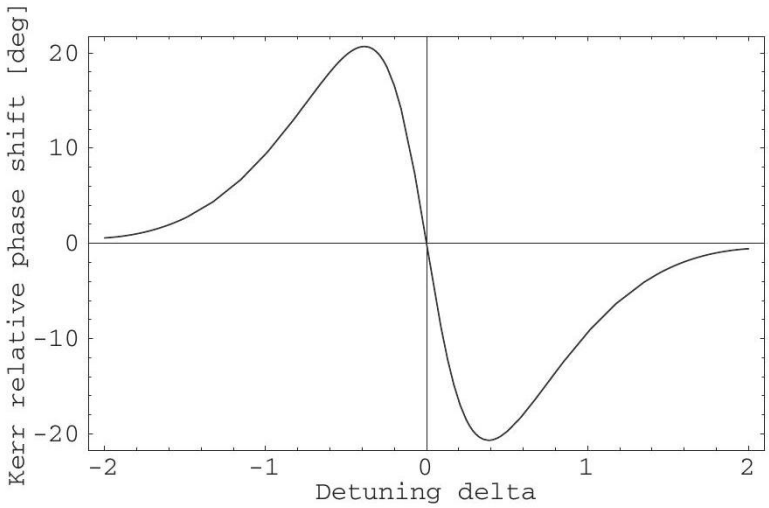


Figure 7.5. Kerr phase shift χ_3 in degrees, for $t = 0.98$ and $g_a = g_b = 1$, plotted as a function of the detuning δ, computed from (7.82) for single photons interacting with a single three-level atom.}

Exercise 7.21: Explicitly exponentiate (7.82) and show that

$$\varphi_{ab} = \arg\left[e^{i\delta t}\left(\cos\Omega' t - i\frac{\delta}{\Omega'}\sin\Omega' t\right)\right], \tag{7.86}$$

where $\Omega' = \sqrt{\delta^2 + g_a^2 + g_b^2}$. Use this to compute χ_3, the nonlinear Kerr phase shift. This is a very simple way to model and understand the Kerr interaction, which sidesteps much of the complication typically involved in classical nonlinear optics.

Exercise 7.22: Associated with the cross phase modulation is also a certain amount of loss, which is given by the probability that a photon is absorbed by the atom. Compute this probability, $1 - \langle 110|U|110\rangle$, where $U = \exp(-iHt)$ for H as in (7.82); compare with $1 - \langle 100|U|100\rangle$ as a function of δ, g_a, g_b, and t.

8.4.20 7.5.4 Quantum computation

Broadly speaking, cavity QED techniques can be used to perform quantum computation in a number of different ways, two of which are the following: quantum information can be represented by photon states, using cavities with atoms to provide nonlinear interactions between photons; or quantum information can be represented using atoms, using photons to communicate between the atoms. Let us now close out this subject by describing an experiment which demonstrates the first of these methods to realize a quantum logic gate.

As we saw in Section 7.4.2, a quantum computer can be constructed using single photon states, phase shifters, beamsplitters, and nonlinear Kerr media, but the π cross phase modulation required to produce a controlled-not gate is nearly infeasible with standard bulk nonlinear optics techniques. Cavity QED can be used to implement a Kerr interaction, as shown in Section 7.5.3; unlike for bulk media, this can have a very strong effect even at the single photon level, because of the strong field provided by a Fabry-Perot type cavity.

Figure 7.6 illustrates a cavity QED experiment which was performed (see 'History and further reading' at the end of the chapter) to demonstrate the potential for realizing a logic gate with the unitary transform

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & e^{i\varphi_a} & 0 & 0 \\ 0 & 0 & e^{i\varphi_b} & 0 \\ 0 & 0 & 0 & e^{i(\varphi_a+\varphi_b+\Delta)} \end{bmatrix}, \tag{7.87}$$

where $\Delta = 16°$, using single photons. In the experiment, two modes of light (distinguished by a very small frequency difference) with weak coherent states are prepared, one linearly polarized (the probe), and one circularly polarized (the pump), as input to the cavity. This state can be expressed as

$$|\psi_{\text{in}}\rangle = \left|\beta^+\right\rangle \left[\frac{|\alpha^+\rangle + |\alpha^-\rangle}{\sqrt{2}}\right] \tag{7.88}$$

recalling that linearly polarized light is an equal superposition of the two possible circularly polarized states, + and - . Approximating the weak coherent states as $|\alpha\rangle \approx |0\rangle + \alpha|1\rangle$ and similarly for $|\beta\rangle$ (and leaving out normalizations for the moment) gives

$$|\psi_{\text{in}}\rangle \approx \left[\left|0^+\right\rangle + \beta\left|1^+\right\rangle\right]\left[\left|0^+\right\rangle + \alpha\left|1^+\right\rangle + \left|0^-\right\rangle + \alpha\left|1^-\right\rangle\right]. \tag{7.89}$$

These photons pass through the optical cavity and interact with the atom, which is modeled as causing a different phase shift to occur to states depending on the total number of photons in each polarization (independent of which mode the photons are
in). Specifically, we assume that a photon in the $|1^+\rangle$state experiences a $e^{i\varphi_a}$ phase shift if it is in the probe beam, and $e^{i\varphi_b}$ for the pump. In addition to this single photon phase shift, the state $|1^+1^+\rangle$experiences an additional Kerr phase shift Δ, so it becomes $e^{i(\varphi_a+\varphi_b+\Delta)}|1^+1^+\rangle$. Other states (and in particular, other polarizations) remain unchanged. The physics which leads to this behavior is similar to that described in Section 7.5.3, and the end effect is the same: a cross phase modulation between the pump and the probe light. The output from the cavity is thus

$$\begin{aligned} |\psi_{\text{out}}\rangle &\approx \left|0^+\right\rangle\left[\left|0^+\right\rangle + \alpha e^{i\varphi_a}\left|1^+\right\rangle + \left|0^-\right\rangle + \alpha\left|1^-\right\rangle\right] \\ &\quad + e^{i\varphi_b}\beta\left|1^+\right\rangle\left[\left|0^+\right\rangle + \alpha e^{i(\varphi_a+\Delta)}\left|1^+\right\rangle + \left|0^-\right\rangle + \alpha\left|1^-\right\rangle\right] \qquad (7.90) \\ &\approx \left|0^+\right\rangle|\alpha, \varphi_a/2\rangle + e^{i\varphi_b}\beta\left|1^+\right\rangle|\alpha, (\varphi_a+\Delta)/2\rangle \qquad (7.91) \end{aligned}$$

where $|\alpha, \varphi_a/2\rangle$ denotes a linearly polarized probe field rotated from the vertical by $\varphi_a/2$. The field polarizations are measured by the detector, giving $\varphi_a \approx 17.5°, \varphi_b \approx 12.5°$ and $\Delta \approx 16°$. Since Δ is a non-trivial value, this result suggests that a universal two qubit logic gate (Exercise 7.23) is possible using single photons, and a single atom in a cavity as a nonlinear optical Kerr medium to interact photons.

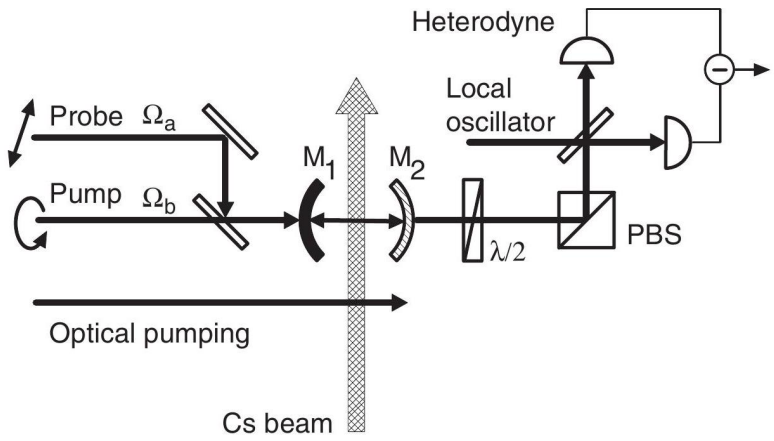


Figure 7.6. Schematic of an experimental apparatus used to demonstrate the possibility of using a single atom to provide cross phase modulation between single photons, as an elementary quantum logic gate. A linearly polarized weak probe beam of light Ω_{a, and a stronger circularly polarized pump beam Ω_b are prepared and shone on an optical cavity with high reflectivity mirrors M_1 and M_2. Cesium atoms prepared in the electronic state $6\,S_{1/2}, F = 4, m = 4$ by optical pumping fall (the figure shows the atoms upside down) such that the average number of atoms in the cavity is around one. The light traverses the cavity, interacting with the atom; σ_+polarized light causes strong transitions to the $6P_{3/2}, F' = 5, m' = 5$ state, and the orthogonal σ_-polarized light causes weak transitions to the $6P_{3/2}, F' = 5, m' = 3$ state. The polarization of the output light is then measured, using a half wave plate, a polarizing beamsplitter (PBS), and a sensitive balanced heterodyne detector (which selectively detects light at a specific frequency, as determined by the local oscillator). Figure courtesy of Q. Turchette.}

Several important caveats must be kept in mind in interpreting these experimental results. The incident photons are absorbed with non-trivial probability when traversing the cavity and atom, and thus the true quantum operation performed is not unitary; this problem would be aggravated if multiple gates were cascaded, which would be required, for example, to realize a controlled-NOT gate (which requires $\Delta = \pi$). In fact, reflection losses of the cavity arrangement used in this experiment would significantly impede cascading; to understand how to get around this, a proper time-dependent model would have to be developed and studied. Also, although the cross phase modulation model is consistent with data measured, the photon-atom interaction model used is an ansatz, and other models are not ruled out by the experiment. In fact, it would be possible in principle to use single photon states (as opposed to attenuated coherent states) in the experiment, and measurements of the resulting entanglement of the two modes in $|\psi_{\rm out}\rangle$ would be a good test. At the time this experiment was carried out, no general procedure was known for fully characterizing a quantum operation and its suitability as a quantum logic gate. However, a method for doing this, known as process tomography, is now well understood (Chapter 8), and remarkably it even allows full characterization of dissipation and other non-unitary behavior. Performing such a test would unambiguously determine exactly the extent to which the experiment described here actually reflects a quantum computation.

Despite these drawbacks, the experiment does demonstrate fundamental concepts required for quantum information processing. It certifies that nonlinear optical behavior such as the Kerr interaction really does occur at the single photon level, thus validating the essence of the Jaynes-Cummings model. Also, this experiment is performed in what is called the bad cavity regime, where the atom's coherent coupling rate g^2/κ to the cavity mode dominates incoherent

emission rate γ into free space, but this coupling is weaker than the rate κ at which input photons enter and leave the cavity. The strong coupling operating regime, in which $g > \kappa > \gamma$, offers an alternative in which larger conditional phase shifts Δ may be obtained.

Most importantly, perhaps, cavity QED opens the door to a wealth of additional interactions which are valuable for quantum information processing. We have also seen how the quantum information perspective - focusing on single photons and single atoms - has allowed us take the Jaynes-Cummings Hamiltonian, the basic cavity QED interaction, and construct from it some of the most fundamental physics of the interaction of electromagnetic waves with matter. We now leave the subject of cavity QED , but as we continue on next to ion traps, and then to magnetic resonance, we shall keep with us these notions of photon-atom interactions, single atoms and photons, and the Jaynes-Cummings Hamiltonian.

Exercise 7.23: Show that the two qubit gate of (7.87) can be used to realize a controlled-NOT gate, when augmented with arbitrary single qubit operations, for any φ_a and φ_b, and $\Delta = \pi$. It turns out that for nearly any value of Δ this gate is universal when augmented with single qubit unitaries.

Optical cavity quantum electrodynamics

- Qubit representation: Location of single photon between two modes, $|01\rangle$ and $|10\rangle$, or polarization.
- Unitary evolution: Arbitrary transforms are constructed from phase shifters (R_z rotations), beamsplitters (R_y rotations), and a cavity QED system, comprised of a Fabry-Perot cavity containing a few atoms, to which the optical field is coupled.
- Initial state preparation: Create single photon states (e.g. by attenuating laser light).
- Readout: Detect single photons (e.g. using a photomultipler tube).
- Drawbacks: The coupling of two photons is mediated by an atom, and thus it is desirable to increase the atom-field coupling. However, coupling the photon into and out of the cavity then becomes difficult, and limits cascadibility.

8.4.21 7.6 Ion traps

Thus far in this chapter, we have focused mainly on representing qubits using photons. Let us now turn to representations which use atomic and nuclear states. Specifically, as we saw in Section 7.1, electron and nuclear spins provide potentially good representations for qubits. Spin is a strange (but very real!) concept (Box 7.7), but since the energy difference between different spin states is typically very small compared with other energy scales (such as the kinetic energy of typical atoms at room temperature), the spin states of an atom are usually difficult to observe, and even more difficult to control. In carefully crafted environments, however, exquisite control is possible. Such circumstances are provided by isolating and trapping small numbers of charged atoms in electromagnetic traps, then cooling the atoms until their kinetic energy is much lower than the spin energy contribution. After doing this, incident monochromatic light can be tuned to selectively cause transitions which change certain spin states depending on other spin states. This is the essence of how trapped ions can be made to perform quantum computation, as we describe in this section. We begin with an overview of the experimental apparatus and its main components, then we present a Hamiltonian modeling the system. We describe an experiment which has been performed to demonstrate a controlled-not gate with trapped ^{9}Be ions, and then close with a few comments on the potential and limitations of the method.

Exercise 7.24: The energy of a nuclear spin in a magnetic field is approximately $\mu_{\rm N}B$, where $\mu_{\rm N} = eh/4\pi m_{\rm p} \approx 5 \times 10^{-27}$ joules per tesla is the nuclear Bohr magneton. Compute the energy of a nuclear spin in a $B = 10$ tesla field, and compare with the thermal energy $k_{\rm B}T$ at $T = 300$ K.

8.4.22 7.6.1 Physical apparatus

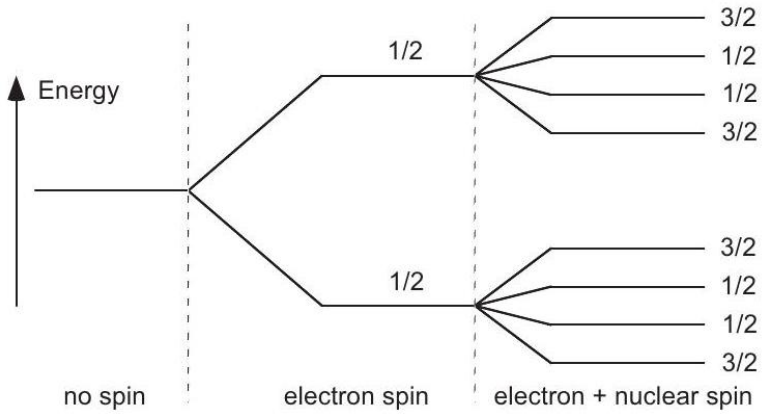
An ion trap quantum computer has as its main components an electromagnetic trap with lasers and photodetectors, and ions.

Trap geometry and lasers

The main experimental apparatus, an electromagnetic trap constructed from four cylindrical electrodes, is shown in Figure 7.7. The end segments of the electrodes are biased at a different voltage U_0 than the middle, so that the ions are axially confined by a static potential $\Phi_{\rm dc} = \kappa U_0 \left[z^2 - (x^2 + y^2)\right]/2$ along the $\hat{z}$ axis (κ is a geometrical factor). However, a result known as Earnshaw's theorem states that a charge cannot be confined in three dimensions by static potentials. Thus, to provide confinement, two of the electrodes

Box 7.7: Spin

Spin is a strange concept. When a particle has spin, it possesses a magnetic moment as if it were a composite particle with some current running around in a loop. But electrons are elementary particles, and the quarks which compose a nucleon are not known to produce spin by orbital motion. Furthermore, the spin of a particle is only ever either integer or half-integer. Spin is nevertheless quite real, and an important part of everyday physics. Integer spin particles, known as bosons, include the photon. Being massless, it is somewhat special and only has spin ± 1 (and no spin zero) components; these correspond to the two familiar orthogonal polarization states. Sunglasses made from cheap plastic polarizers are effective when driving because sunlight becomes partially polarized in the opposite direction after reflecting off of surfaces such as roadways (light polarized with the electric field transverse to the interface always partially reflects no matter the angle of incidence, in contrast with the transverse magnetic polarization which does not reflect when the angle of incidence is at Brewster's angle). Halfinteger spin particles, known as fermions, include the electron, proton, and neutron. These are 'spin- 1/2 ' particles, in that their spin component can either be $+1/2$ (spin 'up') or $-1/2$ (spin 'down'). When we say 'spin' often what is meant is a spin- 1/2 particle.
The energy eigenstates of an atom intimately involve spin, and the combination of multiple spins. For example, the nucleus of ^{9}Be has spin 3/2. Spins interact with a magnetic field just as magnetic moments do; in a magnetic field $\vec{B}$, an electron with spin $\vec{S}$ has energy $g_e\vec{S}\cdot\vec{B}$, and similarly, a nucleus $\vec{I}$ has energy $g_n\vec{I}\cdot\vec{B}$. Pictorially, for example, the spin contribution to an atom's energy levels can be viewed as:



where we have assumed a spin- 1/2 electron, and a spin- 3/2 nucleus. By tuning the frequency of an incident laser just right, any of these transitions could be selected, as long as conservation laws (Section 7.5.1) are satisfied. In particular, angular momentum conversation implies that when a photon is absorbed by an atom, one unit of angular momentum or spin must change between the initial and final states. These states thus must have definite values of angular momenta; this can be taken into account.

Unlike continuous variables such as position and momentum, and other infinite Hilbert space systems which must be artificially truncated to represent quantum bits, spin states provide good representations for quantum information because they live in an inherently finite state space.

are grounded, while the other two are driven by a fast oscillating voltage which creates a radiofrequency (RF) potential $\Phi_{\text{rf}} = (V_0 \cos \Omega_T t + U_r)\left(1 + (x^2 - y^2)/R^2\right)/2$, where R is a geometrical factor. The segments of the electrodes are capacitively coupled such that the RF potential is constant across them. The combination of Φ_{dc} and Φ_{rf} creates, on average (over Ω_T), a harmonic potential in x, y, and z. Together with the Coulomb repulsion of the ions, this gives a Hamiltonian governing the motion of the N ions in the trap,

$$H = \sum_{i=1}^{N} \frac{M}{2}\left(\omega_x^2 x_i^2 + \omega_y^2 y_i^2 + \omega_z^2 z_i^2 + \frac{|\vec{p}_i|^2}{M^2}\right) + \sum_{i=1}^{N}\sum_{j>i} \frac{e^2}{4\pi\epsilon_0 |\vec{r}_i - \vec{r}_j|}, \tag{7.92}$$

where M is the mass of each ion. Typically, $\omega_x, \omega_y \gg \omega_z$ by design, so that the ions all lie generally along the $\hat{z}$ axis. As the number of ions becomes large, the geometrical configuration of the ions can become quite complicated, forming zig-zag and other patterns, but we shall focus on the simple case where just a few ions are trapped, in a string-like configuration.

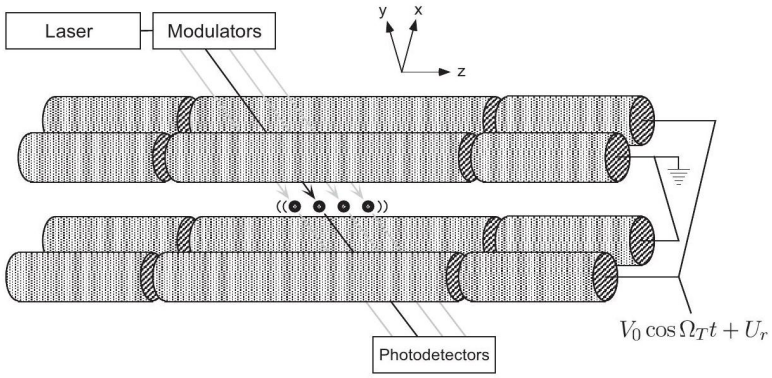


Figure 7.7. Schematic drawing (not to scale) of an ion trap quantum computer, depicting four ions trapped in the center of a potential created by four cylindrical electrodes. The apparatus is typically contained in a high vacuum \$\left(\approx 10^{-8 \mathrm{~Pa}}\right)\$, and the ions are loaded from a nearby oven. Modulated laser light incident on the ions through windows in vacuum chamber perform operations on and are used to readout the atomic states.}

Just as a mass on a spring can behave as a quantum system when the coupling to the external world becomes sufficiently small, the motion of the electromagnetically confined ion becomes quantized when it is sufficiently well isolated. Let us first understand what the quantization means, then consider the isolation criteria. As we saw in Section 7.3, the energy levels of a harmonic oscillator are equally spaced, in units of $\hbar\omega_z$. In the ion trap, in the regime which concerns us, these energy eigenstates represent different vibrational modes of the entire linear chain of ions moving together as one body, with mass NM. These are called the center of mass modes. Each $\hbar\omega_z$ quantum of vibrational energy is called a phonon, and can be thought of as a particle, just as a quantum of electromagnetic radiation in a cavity is a photon.

For the above phonon description to hold, certain criteria must hold. First, the coupling to the environment must be sufficiently small such that thermalization does not randomize the state of the system (and thus cause it to behave classically). Physically,
what can happen is that nearby fluctuating electric and magnetic fields push on the ions, causing their motional state to randomly transition between energy eigenstates. Such noise sources are nearly inevitable, in a technical sense, since, for example, one cannot drive the confining electrodes from a perfect voltage source; the source will always have a finite resistance, and this resistance gives rise to Johnson noise, which has fluctuations on time scales the ions are sensitive to. The electric field on local patches of the electrodes can also fluctuate, randomly driving the ions' motion. As the randomness increases, the quantum properties of the ions' state is lost, and their behavior becomes well described by classical statistical averages. For example, both their momentum and position become well defined, which cannot be simultaneously true for a quantum system. Nevertheless, in practice, most technical noise sources can indeed be controlled quite well, to the extent that they do not heat or dephase the trapped ions too much on the time scale of most experiments. In part, one important reason this is possible is that as long as the harmonic approximation holds, the trapped ions are very selective about the frequency of the noise they are sensitive to; just as transitions between atomic levels can be selected by radiation tuned only to the correct frequency, only fluctuations which have high spectral power density around ω_z will affect the ions.

It is also quite important for the ions to be sufficiently cool so as to make the onedimensional harmonic approximation valid. The true potential is non-quadratic for large displacements along any direction away from the trap center. And higher order vibrational modes in which the ions move relative to each other (instead of moving together) must have energies much

higher than the center of mass mode. When this holds, and the ions are cooled to their motional ground state, their transition to the next higher energy state is through absorption of a center of mass phonon; this process is related to the Mossbaüer effect, in which a photon is absorbed by atoms in a crystal without generating local phonons because the entire crystal recoils together.

How are the ions cooled to their motional ground state? The goal is to satisfy $k_{\rm B}T \ll \hbar\omega_z$, where T is the temperature reflecting the kinetic energy of the ions. Essentially, this can be done by using the fact that photons carry not only energy, but also momentum $p = h/\lambda$, where λ is the wavelength of the light. Just as the whistle of an approaching train has a higher pitch than a departing train, an atom moving toward a laser beam has transition frequencies which are slightly higher in energy than an atom moving away. If the laser is tuned such that it is absorbed only by approaching atoms, then the atoms slow down because the photons kick them in the opposite direction. This method is known as Doppler cooling. Shining a properly tuned laser (which has momentum vector components along each axis) at trapped atoms thus can cool the atoms down to the limit $k_{\rm B}T \approx \hbar\Gamma/2$, where Γ is the radiative width of the transition used for the cooling. To cool beyond this limit, another method, known as sideband cooling, is then applied, as illustrated in Figure 7.8. This allows one to reach the $k_{\rm B}T \ll \hbar\omega_z$ limit.

Another criterion which must be satisfied is that the width of the ion oscillation in the trap potential should be small compared to the wavelength of the incident light. This Lamb-Dicke criterion is conveniently expressed in terms of the Lamb-Dicke parameter $\eta \equiv 2\pi z_0/\lambda$, where λ is the wavelength, and $z_0 = \sqrt{\hbar/2NM\omega}$ is the characteristic length scale of the spacing between ions in the trap. The Lamb-Dicke criterion requires that $\eta \ll 1$; this does not strictly have to be met in order for ion traps to be useful for quantum computation, but it is desired to have that $\eta \approx 1$ at least, in order that the individual

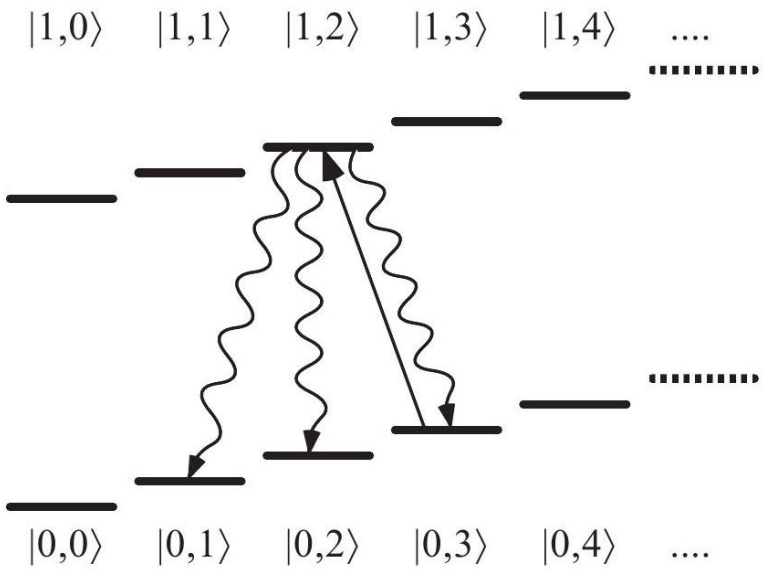


Figure 7.8. Sideband cooling method, showing transitions between $|0,n\rangle$ and $|1,m\rangle$, where 0 and 1 are two electronic levels, and n and m are phonon levels representing motional states of the ion. Laser light is tuned to have energy one phonon less than the electronic transition, such that, for example, the $|0,3\rangle$ state transitions to the $|1,2\rangle$ state, as shown. The atom then spontaneously decays into the lower energy 0 state (wiggly lines), randomly going to either $|0,1\rangle, |0,2\rangle$, or $|0,3\rangle$ (with nearly equal probabilities). Note that the laser light actually causes all possible transitions between $|0,n\rangle$ and $|1,n-1\rangle$, since these all have the same energy. However, this process does not touch the $|0,0\rangle$ state, and eventually that is the state in which the atom will be left.

ions can be resolved by different laser beams, but without making their motional state too difficult to optically excite in order to perform logic operations.

Atomic structure

The purpose of the trap apparatus described above is to allow ions to be cooled to the extent that their vibrational state is sufficiently close to having zero phonons ($|0\rangle$), an appropriate initial state for computation. Similarly, the internal states of the ions must be initialized appropriately, so they may be used to store quantum information. Let us now consider what these internal states are, and understand why they are good qubit representations by estimating their coherent lifetime.

The internal atomic states relevant to the trapped ion we shall consider result from the combination F of electron spin S and nuclear spin I, giving $F = S + I$. The formal piece of theory which describes this - known as the addition of angular momenta not only describes important physics for understanding atomic structure, but also is an interesting mechanism for quantum information. A single photon interacting with an atom can provide or carry away one unit of angular momentum, as we saw in Section 7.5.1. But there are numerous possible sources of angular momenta in an atom: orbital, electron spin, and nuclear spin. Where it comes from is partly determined by the energy levels selected by the energy of the photon, but beyond that, the photon cannot distinguish between different sources, and to describe what happens we must select a basis in which total angular momentum becomes a uniquely defined property of the state.

Consider, for example, two spin- 1/2 spins. The 'computational' basis for this two qubit space is $|00\rangle, |01\rangle, |10\rangle, |11\rangle$, but to span the state space we could equally well
choose the basis

$$|0,0\rangle_J = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \tag{7.93}$$

$$|1,-1\rangle_J = |00\rangle \tag{7.94}$$

$$|1,0\rangle_J = \frac{|01\rangle + |10\rangle}{\sqrt{2}} \tag{7.95}$$

$$|1,1\rangle_J = |11\rangle \tag{7.96}$$

These basis states are special, because they are eigenstates of the total momentum operator, defined by $j_x = (X_1 + X_2)/2, j_y = (Y_1 + Y_2)/2, j_z = (Z_1 + Z_2)/2$, and

$$J^2 = j_x^2 + j_y^2 + j_z^2 \tag{7.97}$$

The states $|j, m_j\rangle_J$ are eigenstates of J^2 with eigenvalue $j(j+1)$, and simultaneously eigenstates of j_z, with eigenvalue m_j. These states are the natural ones selected by many physical interactions; for example, in a $\hat{z}$ oriented magnetic field the magnetic moment μ in the Hamiltonian μB_z is proportional to m_j, the component of the total angular momentum in the $\hat{z}$ direction.

The theory of addition of angular momenta is sophisticated and well developed, and we have but scratched its surface (for the interested reader, some relevant exercises are provided below, and pointers to the literature are given in the 'History and further reading's section at the end of the chapter). Nevertheless, some interesting observations which concern quantum information can already be drawn from the above examples. Normally, we think of entangled states such as the Bell states (Section 1.3.6) as being unnatural states of matter, because they have strange, non-local properties. However, the state $|0,0\rangle_J$ is a Bell state! Why does Nature

prefer this state here? It is because of a symmetry under which the interaction involving the magnetic moment is invariant under interchange of the two spins. Such symmetries actually occur widely in Nature, and are potentially quite useful for performing entangling measurements and operations.

Exercise 7.25: Show that the total angular momenta operators obey the commutation relations for $SU(2)$, that is, $[j_i, j_k] = i\epsilon_{ikl} j_l$.

Exercise 7.26: Verify the properties of $|j, m_j\rangle_J$ by explicitly writing the 4×4 matrices J^2 and j_z in the basis defined by $|j, m_j\rangle_J$.

Exercise 7.27: (Three spin angular momenta states) Three spin-1/2 spins can combine together to give states of total angular momenta with $j = 1/2$ and $j = 3/2$. Show that the states

$$|3/2, 3/2\rangle = |111\rangle \tag{7.98}$$

$$|3/2, 1/2\rangle = \frac{1}{\sqrt{3}}[|011\rangle + |101\rangle + |110\rangle] \tag{7.99}$$

$$|3/2, -1/2\rangle = \frac{1}{\sqrt{3}}[|100\rangle + |010\rangle + |001\rangle] \tag{7.100}$$

$$|3/2, -3/2\rangle = |000\rangle \tag{7.101}$$

$$|1/2, 1/2\rangle_1 = \frac{1}{\sqrt{2}}[-|001\rangle + |100\rangle] \tag{7.102}$$

$$|1/2, -1/2\rangle_1 = \frac{1}{\sqrt{2}}[|110\rangle - |011\rangle] \tag{7.103}$$

$$|1/2, 1/2\rangle_2 = \frac{1}{\sqrt{6}}[|001\rangle - 2|010\rangle + |100\rangle] \tag{7.104}$$

$$|1/2, -1/2\rangle_2 = \frac{1}{\sqrt{6}}[-|110\rangle + 2|101\rangle - |011\rangle] \tag{7.105}$$

form a basis for the space, satisfying $J^2 |j, m_j\rangle = j(j+1) |j, m_j\rangle$ and $j_z |j, m_j\rangle = m_j |j, m_j\rangle$, for $j_z = (Z_1 + Z_2 + Z_3)/2$ (similarly for j_x and j_y) and $J^2 = j_x^2 + j_y^2 + j_z^2$. There are sophisticated ways to obtain these states, but a straightforward brute-force method is simply to simultaneously diagonalize the 8×8 matrices J^2 and j_z.

Exercise 7.28: (Hyperfine states) We shall be taking a look at beryllium in Section 7.6.4 - the total angular momenta states relevant there involve a nuclear spin $I = 3/2$ combining with an electron spin $S = 1/2$ to give $F = 2$ or $F = 1$. For a spin- 3/2 particle, the angular momenta operators are

$$i_x = \frac{1}{2}\begin{bmatrix} 0 & \sqrt{3} & 0 & 0 \\ \sqrt{3} & 0 & 2 & 0 \\ 0 & 2 & 0 & \sqrt{3} \\ 0 & 0 & \sqrt{3} & 0 \end{bmatrix} \tag{7.106}$$

$$i_y = \frac{1}{2}\begin{bmatrix} 0 & i\sqrt{3} & 0 & 0 \\ -i\sqrt{3} & 0 & 2i & 0 \\ 0 & -2i & 0 & i\sqrt{3} \\ 0 & 0 & -i\sqrt{3} & 0 \end{bmatrix} \tag{7.107}$$

$$i_z = \frac{1}{2}\begin{bmatrix} -3 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 3 \end{bmatrix} \tag{7.108}$$

1. Show that i_x, i_y, and i_z satisfy $SU(2)$ commutation rules.

2. Give 8×8 matrix representations of $f_z = i_z \otimes I + I \otimes Z/2$ (where I here represents the identity operator on the appropriate subspace) and similarly f_x and f_y, and, $F^2 = f_x^2 + f_y^2 + f_z^2$. Simultaneously diagonalize f_z and F^2 to obtain basis states $|F, m_F\rangle$ for which $F^2 |F, m_F\rangle = F(F+1) |F, m_F\rangle$ and $f_z |F, m_F\rangle = m_F |F, m_F\rangle$.

How long can a superposition of different spin states exist? The limiting process, known as spontaneous emission, occurs when an atom transitions from its excited state to its ground state by emitting a photon. This happens at some random time, at a rate which we shall estimate. It might seem that spontaneously emitting a photon is a strange thing for an atom to do, if it is simply sitting in free space with nothing apparently disturbing it. But this process is actually a very natural consequence of the coupling of the atom to electromagnetic fields, described simply by the Jaynes-Cummings interaction,

$$H_I = g\left(a^\dagger \sigma_- + a\sigma_+\right) \tag{7.109}$$

as we recall from Section 7.5.2. Previously, we used this model to describe how a laser interacts with an atom, but the model also describes what happens to an atom even when no optical field is present! Consider an atom in its excited state coupled to a single mode which contains no photon, the state $|01\rangle$ (using $|\text{field, atom}\rangle$). This is not an eigenstate of H_I, and thus it cannot remain stationary as time evolves. What happens is described by the unitary operator U in (7.77), by which we find that there is a probability $p_{\text{decay}} = |\langle 10|U|01\rangle|^2$ for the atom to decay into its ground state and emit a photon, where

$$p_{\text{decay}} = g^2 \frac{4\sin^2 \frac{1}{2}(\omega - \omega_0)^2 t}{(\omega - \omega_0)^2}, \tag{7.110}$$

to lowest order in g, the atom-field coupling. ω is the frequency of the photon, and $\hbar\omega_0$ the energy difference between the two levels of the atom. An atom sitting in free space interacts with many different optical modes; inserting the coupling

$$g^2 = \frac{\omega_0^2}{2\hbar\omega\epsilon_0 c^2} |\langle 0|\vec{\mu}|1\rangle|^2, \tag{7.111}$$

where $\vec{\mu}$ is the atomic dipole operator, integrating over all the optical modes (Exercise 7.29) and taking a time derivative gives the probability per second of decay,

$$\gamma_{\rm rad} = \frac{\omega_0^3 |\langle 0|\vec{\mu}|1\rangle|^2}{3\pi\hbar\epsilon_0 c^5} \tag{7.112}$$

If we make the approximation that $|\langle 0|\vec{\mu}|1\rangle| \approx \mu_{\rm B} \approx 9 \times 10^{-24}$ J/T, the Bohr magneton, and assume that $\omega_0/2\pi \approx 10$GHz, then $\gamma_{\rm rad} \approx 10^{-15}{\rm sec}^{-1}$, a spontaneous emission rate of less than one decay every 3000000 years. This calculation is representative of those done to estimate lifetimes of atomic states; as you can see, the hyperfine states can have remarkably long coherence times in theory, and this is generally consistent with experiments, in which lifetimes of tens of seconds to tens of hours have been observed.

Exercise 7.29: (Spontaneous emission) The spontaneous emission rate (7.112) can be derived from (7.110)-(7.111) by the following steps.

1. Integrate

$$\frac{1}{(2\pi c)^3}\frac{8\pi}{3}\int_0^\infty \omega^2 p_{\rm decay}\, d\omega \tag{7.113}$$

where the $8\pi/3$ comes from summing over polarizations and integrating over the solid angle $d\Omega$, and $\omega^2/(2\pi c)^3$ comes from the mode density in three-dimensional space. (Hint: you may want to extend the lower limit of the integral to $-\infty$.)
2. Differentiate the result with respect to t, to obtain $\gamma_{\rm rad}$.

The form of g^2 is a result of quantum electrodynamics; taking this for granted, the remainder of the calculation as presented here really stems from just the Jaynes-Cummings interaction. Again, we see how considering its properties in the single atom, single photon regime gives us a fundamental property of atoms, without resorting to perturbation theory!

Exercise 7.30: (Electronic state lifetimes) A calculation similar to that for $\gamma_{\rm red}$ can be done to estimate the lifetimes expected for electronic transitions, that is, those which involve energy level changes $\Delta n \neq 0$. For such transitions, the relevant
interaction couples the atom's electric dipole moment to the electromagnetic field, giving

$$g_{\rm ed}^2 = \frac{\omega_0^2}{2\hbar\omega\epsilon_0} \left|\langle 0|\vec{\mu}_{\rm ed}|\, 1\right\rangle|^2 . \tag{7.114}$$

This gives a spontaneous emission rate

$$\gamma_{\rm red}^{\rm ed} = \frac{\omega_0^3 \left|\langle 0|\vec{\mu}_{\rm ed}|\, 1\rangle\right|^2}{3\pi\hbar\epsilon_0 c^3}. \tag{7.115}$$

Give a value for $\gamma_{\rm red}^{\rm ed}$, taking $|\langle 0|\vec{\mu}_{\rm ed}\,|\,1\rangle| \approx qa_0$, where q is the electric charge, and a_0 the Bohr radius, and assuming $\omega_0/2\pi \approx 10^{15}$ Hz. The result show how much faster electronic states can decay compared with hyperfine states.

8.4.23 7.6.2 The Hamiltonian

Combining the simplified models given in the previous section for the harmonic electromagnetic trap and the atomic structure provides us with the following simplified toy model for an ion trap quantum information processor. Imagine a single two-level spin interacting via the usual magnetic dipole interaction $H_I = -\vec{\mu}\cdot\vec{B}$ with an electromagnetic field, where the dipole moment $\vec{\mu} = \mu_m\vec{S}$ is proportional to the spin operator S, and the magnetic field is $\vec{B} = B_1\hat{x}\cos(kz - \omega t + \varphi)$, and B_1 is the field strength, k its momentum in the $\hat{z}$ direction, ω its frequency, and φ its phase. Note that in this section, we shall use $S_x = X/2, S_y = Y/2$, and $S_z = Z/2$ as the spin operators; they are related to the Pauli operators by a factor of two.

In addition to the usual electromagnetic interaction, there are interactions with the vibrational modes. The spin is physically confined within a harmonic potential of energy scale $\hbar\omega_z$ (Figure 7.9), such that its position becomes quantized and we must describe it by an operator $z = z_0\left(a^\dagger + a\right)$, where $a^\dagger, a$ are raising and lowering operators for the vibrational modes of the particle, representing creation and annihilation of phonons.

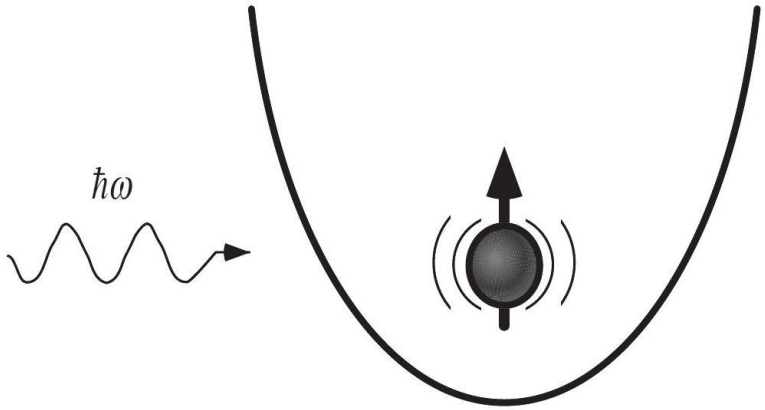


Figure 7.9. Toy model of a trapped ion: a single particle in a harmonic potential with two internal states, interacting with electromagnetic radiation.

Let us assume that the particle is cooled to near its lowest vibrational mode, such that the width of its oscillation in the well is small compared to the wavelength of the incident light, that is, the Lamb-Dicke parameter $\eta \equiv kz_0$ is small. Defining the Rabi frequency of the spin as $\Omega = \mu_m B_1/2\hbar$, and recalling that $S_x = \left(S_+ + S_-\right)/2$, we find that the interaction Hamiltonian simplifies in the small η limit to become

$$H_I = -\vec{\mu}\cdot\vec{B} \tag{7.116}$$

$$\approx\left[\frac{\hbar\Omega}{2}\left(S_+e^{i(\varphi-\omega t)} + S_-e^{-i(\varphi-\omega t)}\right)\right] + \left[i\frac{\eta\hbar\Omega}{2}\left\{S_+a + S_-a^\dagger + S_+a^\dagger + S_-a\right\}\left(e^{i(\varphi-\omega t)} - e^{-i(\varphi-\omega t)}\right)\right]. \tag{7.117}$$

The first term in brackets results from the usual Jaynes-Cummings Hamiltonian as we saw in Section 7.5.2, which occurs when the location z of the spin is a constant. However, it is simplified and does not contain photon operators because it turns out that as long as B_1 is a strong coherent state, we can neglect its quantum properties and leave ourselves with a Hamiltonian which describes just the evolution of the internal atomic state. It is in fact quite remarkable that a coherent state of the field does not become entangled with an atom after interacting with it (to an excellent degree of approximation); this is a deep result which you may explore further by looking at Problem 7.3 at the end of the chapter. We shall also touch on this fact in describing resonance in Section 7.7.2.

The second term in brackets describes the coupling of the motional state of the ion to its spin state, through the fact that the magnetic field it sees is dependent on its position. The four terms in braces correspond to four transitions (two up and two down) which are known as the red and blue motional sidebands, illustrated in Figure 7.10.

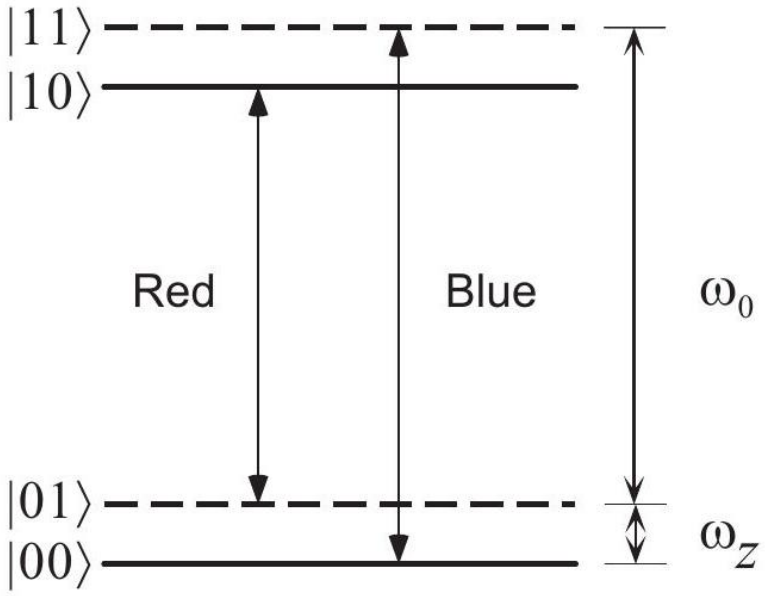


Figure 7.10. Energy levels of the toy model trapped ion showing the red and blue motional sideband transitions, which correspond to creation or annihilation of a single phonon. There is an infinite ladder of additional motional states, which are usually not involved. The states are labeled as $|n, m\rangle$ where n represents the spin state, and m the number of phonons.

Why these sideband transitions have frequencies $\omega_0 \pm \omega_z$ is easy to see, by including the free particle Hamiltonian

$$H_0 = \hbar\omega_0 S_z + \hbar\omega_z a^\dagger a \tag{7.118}$$

which causes the spin and phonon operators to evolve as

$$S_+(t) = S_+ e^{i\omega_0 t} \qquad S_-(t) = S_- e^{-i\omega_0 t} \tag{7.119}$$

$$a^\dagger(t) = a^\dagger e^{i\omega_z t} \qquad a(t) = a e^{-i\omega_z t} \tag{7.120}$$

Thus, in the frame of reference of H_0, the dominant terms of $H_I' = e^{iH_0 t/\hbar} H_I e^{-iH_0 t/\hbar}$ are found to be

$$H_I' = \begin{cases} i\frac{\eta\hbar\Omega}{2}\left(S_+ a^\dagger e^{i\varphi} - S_- a e^{-i\varphi}\right) & \omega = \omega_0 + \omega_z \\ i\frac{\eta\hbar\Omega}{2}\left(S_+ a e^{i\varphi} - S_- a^\dagger e^{-i\varphi}\right) & \omega = \omega_0 - \omega_z \end{cases} \tag{7.121}$$

where the frequency of the electromagnetic field, ω, is as shown on the right.
Extending the above model from one spin to N spins confined within the same harmonic potential is simple if we assume that they share a single center of mass vibrational mode, whose energy is much lower than any other vibrational mode of the system. A straightforward extension of the theory shows that the only required modification is replacement of Ω by $\Omega/\sqrt{N}$, since all N particles move together collectively.

8.4.24 7.6.3 Quantum computation

Quantum computation with trapped ions requires one to be able to construct arbitrary unitary transforms on the internal states of the atoms. We now show how this is done, in three steps: we describe (1) how arbitrary single qubit operations are performed on the internal atomic (spin) state, (2) a method for performing a controlled two qubit gate between the spin

and the phonon state, and (3) a way to swap quantum information between the spin and the phonon. Given these building blocks, we then describe an experiment which was performed to demonstrate a controlled-NOT gate, complete with state preparation and readout.

Single qubit operations

Applying an electromagnetic field tuned to frequency ω_0 turns on the internal Hamiltonian term

$$H_I^{\text{internal}} = \frac{\hbar\Omega}{2}\left(S_+ e^{i\varphi} + S_- e^{-i\varphi}\right) \tag{7.122}$$

By choosing φ and the duration of the interaction appropriately, this allows us to perform rotation operations $R_x(\theta) = \exp(-i\theta S_x)$ and $R_y(\theta) = \exp(-i\theta S_y)$, which, by Theorem 4.1 on page 175, thereby allow us to perform any single qubit operation on the spin state. We shall denote rotations on the j th ion by a subscript, for example, $R_{xj}(\theta)$.

Exercise 7.31: Construct a Hadamard gate from R_y and R_x rotations.

Controlled phase-flip gate

Suppose, now, that one qubit is stored in the atom's internal spin state, and another qubit is stored using the $|0\rangle$ and $|1\rangle$ phonon states. If this is the case, we can perform a controlled phase-flip gate, with the unitary transform

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \tag{7.123}$$

It is easiest to explain how to do this with an atom that has a third energy level, as shown in Figure 7.11 (the extra level is not fundamentally necessary; see Problem 7.4). A laser is tuned to the frequency $\omega_{\text{aux}} + \omega_z$, to cause transitions between the $|20\rangle$ and $|11\rangle$ states; this turns on a Hamiltonian of the form

$$H_{\text{aux}} = i\frac{\eta\hbar\Omega'}{2}\left(S'_+ e^{i\varphi} + S'_- e^{-i\varphi}\right), \tag{7.124}$$

where S'_+ and S'_- denote transitions between $|20\rangle$ and $|11\rangle$, and we assume that higher order motional states are unoccupied. Note that because of the uniqueness of this frequency, no other transitions are excited. We apply the laser with phase and duration to perform a 2π pulse, that is, the rotation $R_x(2\pi)$ on the space spanned by $|11\rangle$ and $|20\rangle$, which is just the unitary transform $|11\rangle \to -|11\rangle$. All the other states remain unchanged, assuming that undesired states such as $|1,2\rangle$ have no probability amplitude. This realizes the transform of (7.123), as desired. We shall write this gate as $C_j(Z)$ (denoting a controlled- Z operation), where j indicates which ion the gate is applied to. Note that the same phonon is shared by all the ions, since it is a center-of-mass phonon; because of this, adopting engineering terminology, this has been called the phonon 'bus' qubit in the literature.

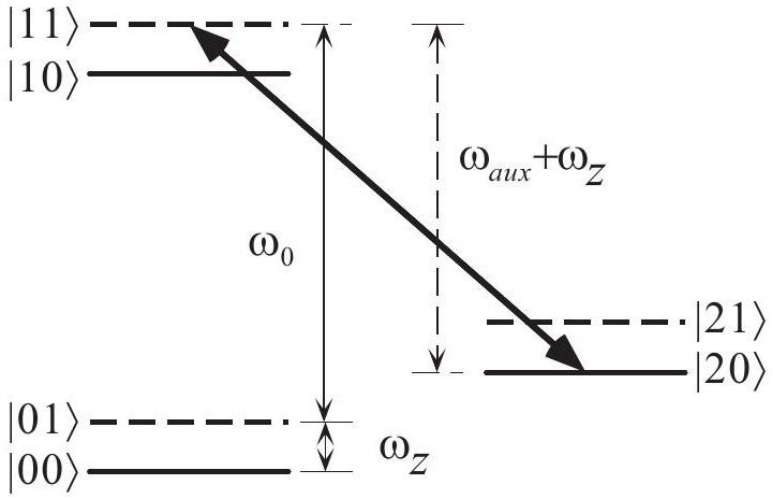


Figure 7.11. Energy levels of a three-level atom in an ion trap, with two phonon states each. The labels $|n, m\rangle$ indicate the atom's state n and the phonon state m. The $|20\rangle \leftrightarrow |11\rangle$ transition is used to perform a controlled phase-flip gate.

Swap gate

Finally, we need some way to swap qubits between the atom's internal spin state and the phonon state. This can be done by tuning a laser to the frequency $\omega_0 - \omega_z$, and arranging for the phase to be such that we perform the rotation $R_y(\pi)$ on the subspace spanned by $|01\rangle$ and $|10\rangle$, which is just the unitary transform

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{7.125}$$

on the $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ space. If the initial state is $a|00\rangle + b|10\rangle$ (that is, the phonon is initially $|0\rangle$), then the state after the swap is $a|00\rangle + b|01\rangle$, so this accomplishes the desired swap operation. We shall write this as SWAP_j when acting on ion j; the inverse operation $\overline{\mathrm{SWAP}}_j$ corresponds to $R_y(-\pi)$. Technically, because of the minus sign in the $|10\rangle\langle 01|$ entry of $R_y(\pi)$, this is not a perfect swap operation, but it is equivalent to one up relative phases (see Exercise 4.26). Thus, this is sometimes referred to as being a 'mapping operation' instead of as a swap.

Controlled-not gate

Putting these gates together allows us to construct a CNOT gate acting on ions j (control) and k (target) using the sequence of operations

$$\mathrm{CNOT}_{jk} = H_k \overline{\mathrm{SWAP}}_k C_j(Z) \mathrm{SWAP}_k H_k, \tag{7.126}$$

(time going from right to left, as usual for matrices) where H_k is a Hadamard gate (constructed from R_y and R_x rotations on ion k). This is very similar to how a controlled-not gate was constructed using beamsplitters and optical Kerr media, as in Equation (7.46).

8.4.25 7.6.4 Experiment

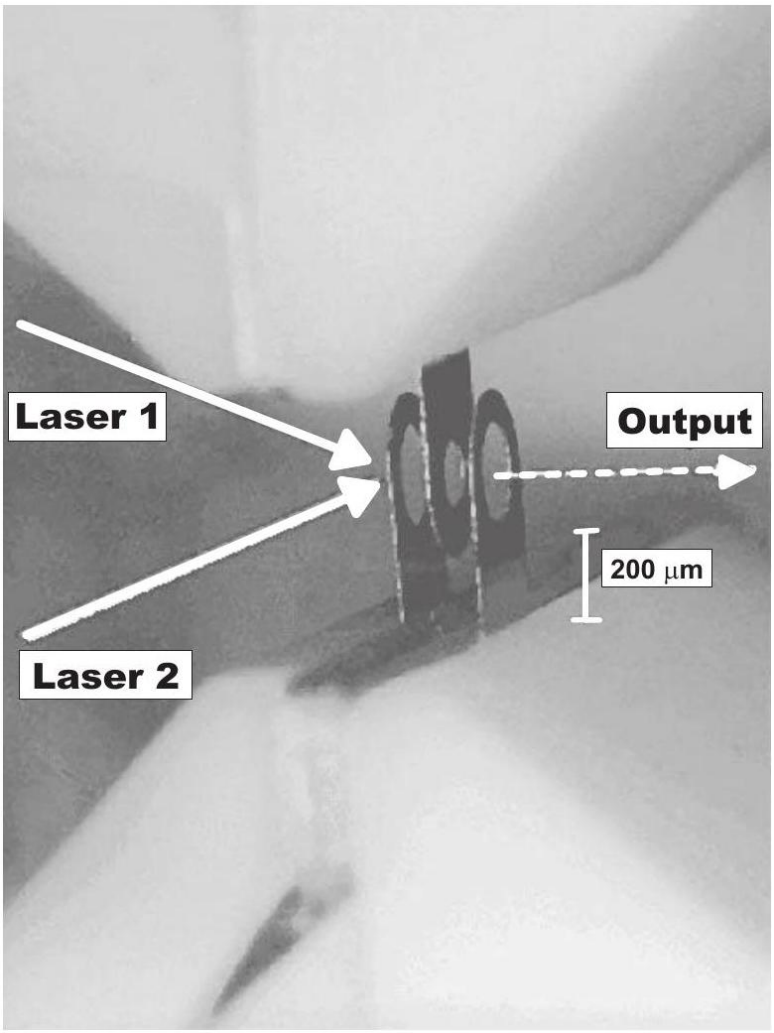


Figure 7.12. Photograph of a microfabricated elliptical electrode ion trap, in which ions have been confined. The ions in this trap are barium ions, rather than beryllium, but the basic principles are the same as described in the text. Reproduced courtesy of R. Devoe and C. Kurtsiefer, IBM Almaden Research Center.

A controlled-NOT gate using a single trapped ion has been demonstrated (see 'History and further reading' at the end of the chapter); precisely how this experiment is done is insightful. In the experiment, a single ion of $^9Be^+$is trapped in a coaxial resonator RF ion trap, different in geometry from the linear ion trap of Figure 7.7, but functionally equivalent, and similar to the photograph of an actual ion trap shown in Figure 7.12. Beryllium was chosen for its convenient hyperfine and electronic level structure, shown in Figure 7.13. The $^2\,S_{1/2}(1,1)$ and $^2\,S_{1/2}(2,2)$ energy levels (Exercise 7.28) are used as the atom's internal qubit state, and the $|0\rangle$ and $|1\rangle$ phonon states as another qubit (labeled

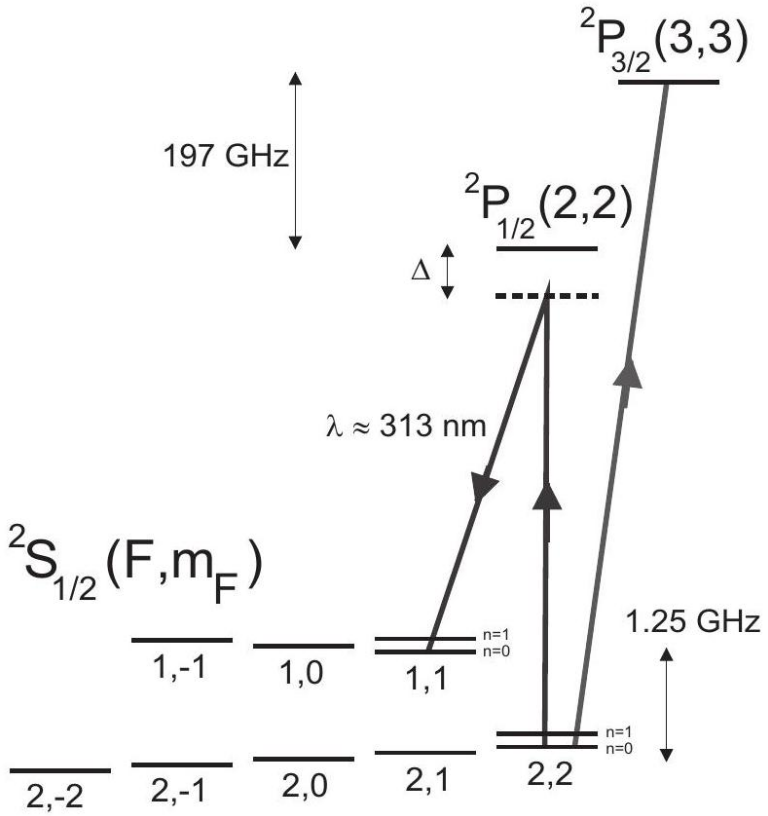


Figure 7.13. Energy levels of ${
ˆ{9} \mathrm{Be}ˆ{+}$used in the ion trap experiment. Figure courtesy of C. Monroe at NIST.}

in the figure as $n = 0$ and $n = 1$). The ≈ 313 nm transition between the ^{2} $S_{1/2}(1,1)$ and ^{2} $S_{1/2}(2,2)$ levels is accomplished not by tuning a single laser to the transition frequency, but rather two lasers whose difference frequency is that of the transition. This Raman transition method simplifies requirements for laser phase stability. The ^{2} $S_{1/2}(2,0)$ state is used as the auxiliary level; the ^{2} $S_{1/2}$ states have different energies by virtue of a 0.18 millitesla magnetic field applied to the system. The trapped ion has vibrational frequencies $(\omega_x, \omega_y, \omega_z)/2\pi = (11.2, 18.2, 29.8)$MHz in the trap, and a ground state $n_x = 0$ wavefunction spread of about 7 nm , giving a Lamb-Dicke parameter of about $\eta_x = 0.2$. The Rabi frequency of the on-resonance transition is $\Omega/2\pi = 140$kHz, the two motional sidebands, $\eta_x\Omega/2\pi = 30$kHz, and the auxiliary transition $\eta_x\Omega'/2\pi = 12$ kHz .

The state of the ion is initialized using Doppler and sideband cooling to obtain, with approximately 95% probability, the state $|00\rangle = \left|^2 S_{1/2}(2,2)\right\rangle |n_x = 0\rangle$. The internal and motional states of the ion are then prepared in one of the four basis states $|00\rangle, |01\rangle, |10\rangle$, or $|11\rangle$ using single qubit operations, then a controlled-NOT gate is performed using three pulses, which implement a $R_y(\pi/2)$ rotation on the internal state qubit, a controlled- Z operation between the two qubits, then a $R_y(-\pi/2)$ rotation on the internal state qubit. It is simple to show (Exercise 7.32) that this circuit, drawn in Figure 7.14, realizes a controlled-NOT gate.

Readout of the computational output is performed with two measurements. The first is to collect the fluorescence from the ion which occurs when + circularly polarized light tuned to the ^{2} $S_{1/2}(2,2) - {}^2P_{3/2}(3,3)$ 'cycling' transition is applied. The light does not couple appreciably to the ^{2} $S_{1/2}(1,1)$ state, and thus the intensity of the observed fluorescence is proportional to the probability of the internal state qubit being in the $|0\rangle$

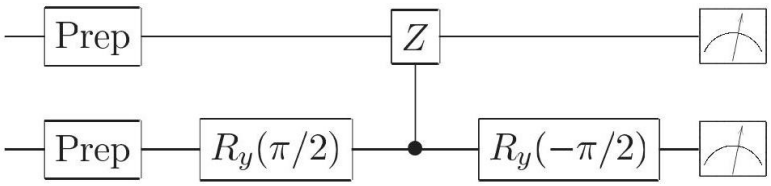


Figure 7.14. Quantum circuit modeling the ion trap controlled-not experiment. The top wire represents the phonon state, and the bottom, the ion's internal hyperfine state.

state; it is a projective measurement. This measurement technique is powerful because the transition cycles many times - the ion absorbs a photon, jumping to the $^2\mathrm{P}_{3/2}(3,3)$ state, then emits a photon, decaying back into the $^2\ \mathrm{S}_{1/2}(2,2)$ state where it started. Thousands or more cycles are possible, allowing good statistics to be accumulated. The second measurement is similar to the first, but a swap pulse is applied first to exchange the motional and internal state qubits; this projectively measures the motional state qubit.

The experiment as performed verifies the classical truth table of the controlled-NOT operation and, in principle, by preparing superposition input states and measuring output density matrices, the unitary transform could be completely characterized using process tomography (Chapter 8). The controlled-NOT gate requires about 50 microseconds to perform with the optical power used in the experiment. On the other hand, the coherence time was measured to be somewhere around hundreds to thousands of microseconds. The dominant decoherence mechanisms included instabilities in the laser beam power and the RF ion trap drive frequency and voltage amplitude, and fluctuating external magnetic fields. Moreover, the experiment involved only a single ion, and only two qubits, and thus was not useful for computation; to be useful, a controlled-NOT gate should generally be applied between different ions, and not just between a single ion and the motional state.

However, the technical limitations can probably be overcome, and lifetimes can be extended by using the short-lived motional state only intermittently, capitalizing on the much longer coherence times of the internal atomic states. And scaling to larger numbers of ions is conceptually viable. Shown in Figure 7.15 is a string of 40 mercury ions which have been trapped. There are many hurdles to making such systems behave as useful quantum information processing machines, but technological surprises are a neverending saga. Someday, perhaps, trapped ions such as these could be registers of qubits in a quantum computer.

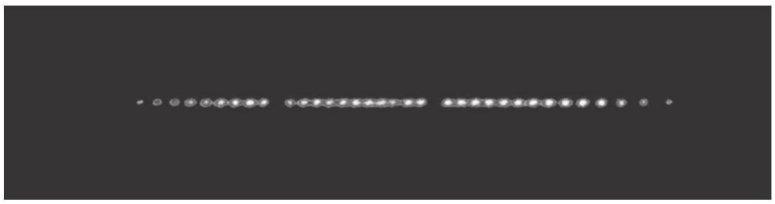


Figure 7.15. Image of fluorescence from about 40 trapped mercury (${ ˆ{199} \mathrm{Hg}ˆ{+}$) atomic ions. The ions are spaced by approximately 15 micrometers, and the two apparent gaps are different isotopes of mercury which do not respond to the probe laser. Reprinted courtesy of D. Wineland, at NIST.}

Exercise 7.32: Show that the circuit in Figure 7.14 is equivalent (up to relative phases) to a controlled-not gate, with the phonon state as the control qubit.

Ion trap quantum computer

- Qubit representation: Hyperfine (nuclear spin) state of an atom, and lowest level vibrational modes (phonons) of trapped atoms.
- Unitary evolution: Arbitrary transforms are constructed from application of laser pulses which externally manipulate the atomic state, via the Jaynes-Cummings interaction. Qubits interact via a shared phonon state.
- Initial state preparation: Cool the atoms (by trapping and using optical pumping) into their motional ground state, and hyperfine ground state.
- Readout: Measure population of hyperfine states.
- Drawbacks: Phonon lifetimes are short, and ions are difficult to prepare in their motional ground states.

8.4.26 7.7 Nuclear magnetic resonance

Nuclear spin systems would be nearly ideal for quantum computation if only spinspin couplings could be large and controllable; this is an important observation from our study of ion traps in the last section. The principal drawback of ion trap quantum computers is the weakness of the phonon mediated spin-spin coupling technique and its susceptibility to decoherence. One way this limitation could be circumvented would be to trap molecules instead of single atoms - the magnetic dipole and electron mediated Fermi contact interactions between neighboring nuclei would provide strong natural couplings. However, with their many vibrational modes, single molecules have been difficult to trap and cool, and thus optical manipulation and detection of nuclear spins in trapped molecules has not been feasible except in special circumstances.

On the other hand, direct manipulation and detection of nuclear spin states using radiofrequency electromagnetic waves is a well-developed field known as nuclear magnetic resonance (NMR). These techniques are widely used in chemistry, for example, to measure properties of liquids, solids, and gases, to determine the structure of molecules, and to image materials and even biological systems. These many applications have lead the technology of NMR to become quite sophisticated, allowing control and observation of tens to hundreds and thousands of nuclei in an experiment.

However, two problems arise in using NMR for quantum computation. First, because of the smallness of the nuclear magnetic moment, a large number (more than $\approx 10^8$) molecules must be present in order to produce a measurable induction signal. Conceptually, a single molecule might be a fine quantum computer, but how can this be true of an ensemble of molecules? In particular, the output of an NMR measurement is an average over all the molecule's signals; can the average output of an ensemble of quantum computers be meaningful? Second, NMR is typically applied to physical systems in equilibrium at room temperature, where the spin energy $\hbar\omega$ is much less than $k_{\mathrm{B}}T$. This means that the initial state of the spins is nearly completely random. Traditional quantum computation requires the system be prepared in a pure state; how can quantum computation be performed with a system which is in a high entropy mixed state?

Solutions to these two problems have made NMR a particularly attractive and insightful method for implementing quantum computation, despite stringent limitations which arise from the thermal nature of typical systems. Many lessons can be learned from NMR: for example, techniques for controlling realistic Hamiltonians to perform arbitrary unitary transforms,

methods for characterizing and circumventing decoherence (and systematic errors), and considerations which arise in assembling components in implementing full quantum algorithms on entire systems. We begin with a description of the physical apparatus and the main Hamiltonian involved, then we discuss how quantum information processing with NMR is possible despite the thermal input state and ensemble problems, concluding with some experiments which have been performed demonstrating quantum algorithms, and the drawbacks of this method.

8.4.27 7.7.1 Physical apparatus

Let us begin with a general description of the apparatus, whose workings will be mathematically modeled in detail later. The two main parts of a pulsed NMR system for liquid samples, which we shall focus on here, are the sample and the NMR spectrometer. A typical molecule which might be used would contain a number n of protons which have spin 1/2 (other possible nuclei include ^{13}C, ^{19} F, ^{15} N, and ^{31}P), and produce an NMR signal at about 500 MHz when placed in a magnetic field of about 11.7 tesla. The frequencies of different nuclei within a molecule can differ by a few kHz to hundreds of kHz because of differences in the local magnetic fields due to chemical environment shielding effects. The molecules are typically dissolved in a solvent, reducing the concentration to the extent that inter-molecular interactions become negligible, leaving a system that might well be described as an ensemble of n qubit quantum 'computers.'

The spectrometer itself is constructed from radiofrequency (RF) electronics and a large superconducting magnet, within the bore of which is held the sample in a glass tube, as shown in Figure 7.16. There, the static $\hat{z}$ oriented magnetic field B_0 is carefully trimmed to be uniform over approximately 1 cm^3 to better than one part in 10^9. Orthogonal saddle or Helmholtz coils lying in the transverse plane allow small, oscillating magnetic fields to be applied along the $\hat{x}$ and $\hat{y}$ directions. These fields can be rapidly pulsed on and off to manipulate nuclear spin states. The same coils are also part of tuned circuits which are used to pick up the RF signal generated by the precessing nuclei (much like how a spinning magnet inductively generates an alternating current in a nearby coil).

A typical experiment begins with a long waiting period in which the nuclei are allowed to thermalize to equilibrium; this can require several minutes for well-prepared liquid samples. Under control of a (classical) computer, RF pulses are then applied to effect the desired transformation on the state of the nuclei. The high power pulse amplifiers are then quickly switched off and a sensitive pre-amplifier is enabled, to measure the final state of the spins. This output, called the free induction decay, is Fourier transformed to obtain a frequency spectrum with peaks whose areas are functions of the spin states (Figure 7.17).

There are many important practical issues which lead to observable imperfections. For example, spatial inhomogeneities in the static magnetic field cause nuclei in different parts of the fields to precess at different frequencies. This broadens lines in the spectrum. An even more challenging problem is the homogeneity of the RF field, which is generated by a coil which must be orthogonal to the B_0 magnet; this geometric constraint and the requirement to simultaneously maintain high B_0 homogeneity usually forces the RF

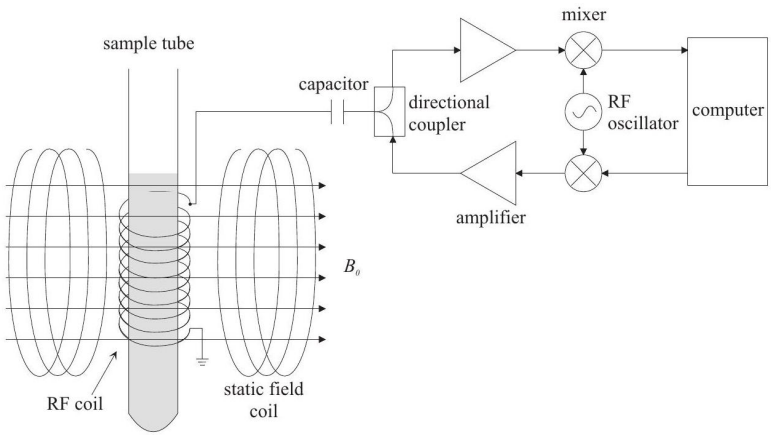


Figure 7.16. Schematic diagram of an NMR apparatus.

field to be inhomogeneous and generated by a small coil, leading to imperfect control of the nuclear system. Also, pulse timing, and stability of power, phase, and frequency are important issues; however, unlike the ion traps, because of the lower frequencies, good control of these parameters is more tractable. We shall return to imperfections in Section 7.7.4, after understanding the basic mathematical description of the system and the methodology for performing quantum information processing with NMR.

8.4.28 7.7.2 The Hamiltonian

The basic theory of NMR can be understood from an ideal model of one and two spins, which we describe here. The first step is to describe how electromagnetic radiation interacts with a single magnetic spin. We then consider the physical nature of couplings between spins which arise in molecules. These tools enable us to model readout of the magnetization which results from transformation of an initial state which is in thermal equilibrium. Finally, we describe a phenomenological model of decoherence, and how its T_1 and T_2 parameters can be experimentally determined.

Single spin dynamics

The magnetic interaction of a classical electromagnetic field with a two-state spin is described by the Hamiltonian $H = -\vec{\mu}\cdot\vec{B}$, where $\vec{\mu}$ is the spin, and $B = B_0\hat{z}+B_1(\hat{x}\cos\omega t+\hat{y}\sin\omega t)$ is a typical applied magnetic field. B_0 is static and very large, and B_1 is usually time varying and several orders of magnitude smaller than B_0 in strength, so that perturbation theory is traditionally employed to study this system. However, the Schrödinger equation for this system can be solved straightforwardly without perturbation theory, using the Pauli matrix techniques of Chapter 2, in terms of which the Hamiltonian can be written as

$$H = \frac{\omega_0}{2}Z + g(X\cos\omega t + Y\sin\omega t), \tag{7.127}$$

where g is related to the strength of the B_1 field, and ω_0 to B_0, and X, Y, Z are the Pauli matrices as usual. Define $|\varphi(t)\rangle = e^{i\omega tZ/2}|\chi(t)\rangle$, such that the Schrödinger equation

$$i\partial_t|\chi(t)\rangle = H|\chi(t)\rangle \tag{7.128}$$

can be re-expressed as

$$i\partial_t|\varphi(t)\rangle = \left[e^{i\omega Zt/2}He^{-i\omega Zt/2} - \frac{\omega}{2}Z\right]|\varphi(t)\rangle. \tag{7.129}$$

Since

$$e^{i\omega Zt/2} X e^{-i\omega Zt/2} = (X\cos\omega t - Y\sin\omega t), \tag{7.130}$$

(7.129) simplifies to become

$$i\partial_t|\varphi(t)\rangle = \left[\frac{\omega_0-\omega}{2}Z + gX\right]|\varphi(t)\rangle, \tag{7.131}$$

where the terms on the right multiplying the state can be identified as the effective 'rotating frame' Hamiltonian. The solution to this equation is

$$|\varphi(t)\rangle = e^{i\left[\frac{\omega_0-\omega}{2}Z+gX\right]t}|\varphi(0)\rangle. \tag{7.132}$$

The concept of resonance arises from the behavior of this solution, which can be understood using (4.8) to be a single qubit rotation about the axis

$$\hat{n} = \frac{\hat{z} + \frac{2g}{\omega_0-\omega}\hat{x}}{\sqrt{1+\left(\frac{2g}{\omega_0-\omega}\right)^2}} \tag{7.133}$$

by an angle

$$|\vec{n}| = t\sqrt{\left(\frac{\omega_0-\omega}{2}\right)^2 + g^2}. \tag{7.134}$$

When ω is far from ω_0, the spin is negligibly affected by the B_1 field; the axis of its rotation is nearly parallel with $\hat{z}$, and its time evolution is nearly exactly that of the free B_0 Hamiltonian. On the other hand, when $\omega_0 \approx \omega$, the B_0 contribution becomes negligible, and a small B_1 field can cause large changes in the state, corresponding to rotations about the $\hat{x}$ axis. The enormous effect a small perturbation can have on the spin system, when tuned to the appropriate frequency, is responsible for the 'resonance' in nuclear magnetic resonance. The same effect, of course, is also at the heart of the selectivity of two-level atoms for specifically tuned laser fields that was used (but not explained) in Section 7.5.1.

In general, when $\omega = \omega_0$, the single spin rotating frame Hamiltonian can be written as

$$H = g_1(t)X + g_2(t)Y, \tag{7.135}$$

where g_1 and g_2 are functions of the applied transverse RF fields.

Exercise 7.33: (Magnetic resonance) Show that (7.128) simplifies to become (7.129). What laboratory frame Hamiltonian gives rise to the rotating frame Hamiltonian (7.135)?

Exercise 7.34: (NMR frequencies) Starting with the nuclear Bohr magneton, compute the precession frequency of a proton in a magnetic field of 11.8 tesla. How many gauss should B_1 be to accomplish a 90° rotation in 10 microseconds?

Spin-spin couplings

More than one spin is usually present in systems of interest; ^{1}H, ^{13}C, ^{19} F, and ^{15} N all have nuclear spin 1/2. These spins interact through two dominant mechanisms: direct dipolar coupling, and indirect through-bond electron mediated interactions. Throughspace dipolar coupling is described by an interaction Hamiltonian of the form

$$H^{\mathrm{D}}_{1,2} = \frac{\gamma_1\gamma_2\hbar}{4r^3}\left[\vec{\sigma}_1\cdot\vec{\sigma}_2 - 3\left(\vec{\sigma}_1\cdot\hat{n}\right)\left(\vec{\sigma}_2\cdot\hat{n}\right)\right] \tag{7.136}$$

where $\hat{n}$ is the unit vector in the direction joining the two nuclei, and $\vec{\sigma}$ is the magnetic moment vector (times two). In a low viscosity liquid, dipolar interactions are rapidly averaged away; mathematically this is calculated by showing that the spherical average of $H^{\rm D}_{1,2}$ over $\hat{n}$ goes to zero as the averaging becomes rapid compared to the dipolar coupling energy scale.

Through-bond interactions, also known simply as ' J-coupling,' are indirect interactions mediated by electrons shared through a chemical bond; the magnetic field seen by one nucleus is perturbed by the state of its electronic cloud, which interacts with another nucleus through the overlap of the electronic wavefunction with the nucleus (a Fermi contact interaction). This coupling has the form

$$H^J_{1,2} = \frac{\hbar J}{4}\vec{\sigma}_1 \cdot \vec{\sigma}_2 = \frac{\hbar J}{4} Z_1 Z_2 + \frac{\hbar J}{8}\left[\sigma_+\sigma_- + \sigma_-\sigma_+\right] \tag{7.137}$$

We shall be interested in the case where J is a scalar (in general it may be a tensor), which is an excellent approximation in liquids and when couplings are weak, or when the interacting nuclear species have vastly different precession frequencies. This case is described by

$$H^J_{12} \approx \frac{\hbar}{4} J Z_1 Z_2 \tag{7.138}$$

Exercise 7.35: (Motional narrowing) Show that the spherical average of $H^{\rm D}_{1,2}$ over $\hat{n}$ is zero.

Thermal equilibrium

NMR differs significantly from the other physical systems we have studied previously in this chapter in that it uses an ensemble of systems, and the primary measurement is an ensemble average. Furthermore, no extensive procedures are employed to prepare the initial state in a special state such as the ground state; in fact, to do so is challenging with present technology.

Rather, the initial state is the thermal equilibrium state,

$$\rho = \frac{e^{-\beta H}}{\mathcal{Z}}, \tag{7.139}$$

where $\beta = 1/k_{\rm B}T$, and $\mathcal{Z} = {\rm tr}\, e^{-\beta H}$ is the usual partition function normalization, which ensures that ${\rm tr}(\rho) = 1$. Since $\beta \approx 10^{-4}$ at modest fields for typical nuclei at room temperature, the high temperature approximation

$$\rho \approx 2^{-n}[1 - \beta H] \tag{7.140}$$

is appropriate, for a system of n spins.

Since spin-spin couplings are very small compared with the precession frequencies, the thermal state density matrix is very nearly diagonal in the Z basis, and thus it can be interpreted as being a mixture of the pure states $|00\ldots0\rangle, |00\ldots01\rangle, \ldots, |11\ldots1\rangle$. What is actually the true physical state of each ensemble member is a matter of debate, because an infinite number of unravelings exist for a given density matrix. In principle, with NMR the true physical state can be measured if the ensemble members (individual molecules) are accessible, but this is experimentally difficult.

Exercise 7.36: (Thermal equilibrium NMR state) For $n = 1$ show that the thermal equilibrium state is

$$\rho \approx 1 - \frac{\hbar\omega}{2k_{\rm B}T}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \tag{7.141}$$

and for $n = 2$ (and $\omega_A \approx 4\omega_B$),

$$\rho \approx 1 - \frac{\hbar\omega_B}{4k_{\mathrm{B}}T} \begin{bmatrix} 5 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & -3 & 0 \\ 0 & 0 & 0 & -5 \end{bmatrix}. \tag{7.142}$$

Magnetization readout

The principal output of an experiment is the free induction decay signal, mathematically given as

$$V(t) = V_0 \operatorname{tr}\left[e^{-iHt}\rho e^{iHt}\left(iX_k + Y_k\right)\right], \tag{7.143}$$

where X_k and Y_k operate only on the k th spin, and V_0 is a constant factor dependent on coil geometry, quality factor, and maximum magnetic flux from the sample volume. This signal originates from the pickup coils detecting the magnetization of the sample in the $\hat{x} - \hat{y}$ plane. In the laboratory frame, this signal will oscillate at a frequency equal to the precession frequency ω_0 of the nuclei; however, $V(t)$ is usually mixed down with an oscillator locked at ω_0, then Fourier transformed, such that the final signal appears as shown in Figure 7.17.

Exercise 7.37: (NMR spectrum of coupled spins) Calculate $V(t)$ for $H = JZ_1Z_2$ and $\rho = e^{i\pi Y_1/4}\frac{1}{4}\left[1 - \beta\hbar\omega_0\left(Z_1 + Z_2\right)\right]e^{-i\pi Y_1/4}$. How many lines would there be in the spectrum of the first spin if the Hamiltonian were $H = JZ_1\left(Z_2 + Z_3 + Z_4\right)$ (with a similar initial density matrix) and what would their relative magnitudes be?

Decoherence

A prominent characteristic of the free induction decay whose description lies outside the simple models presented so far for NMR is the exponential decay of the magnetization signal. One cause of this is inhomogeneity in the static magnetic field, which leads to

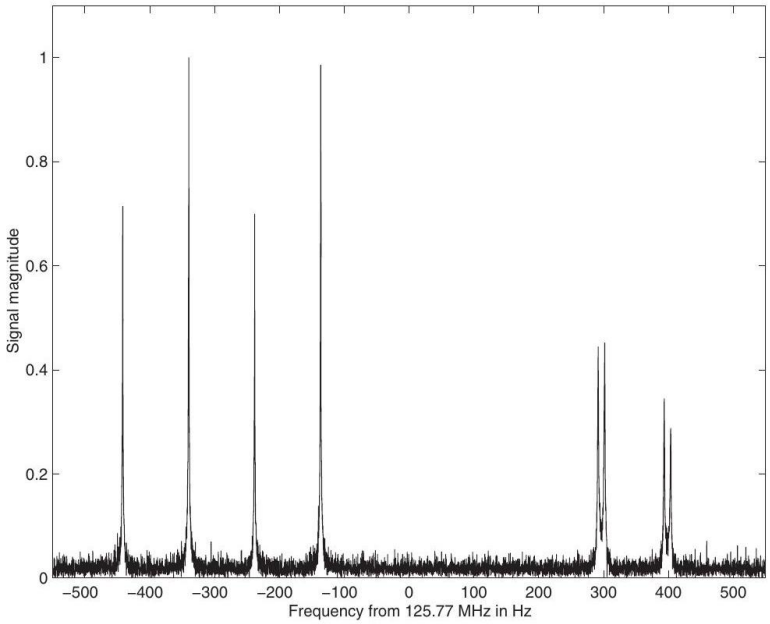


Figure 7.17. Carbon spectrum of ${
ˆ{13} \mathrm{C}$ labeled trichloroethylene. The four lines on the left come from the carbon nucleus directly bound to the proton; four lines appear because of couplings to the proton and to the second carbon nucleus, whose own signal gives the closely spaced four lines on the right. The second carbon nucleus is further away from the proton than the first, and thus has a much smaller coupling to it.}

precessing spins in one part of the sample getting out of phase with those in another part. Effects due to inhomogeneities are reversible in principle, but there are other sources of phase randomization which are fundamentally irreversible, such as those originating from spin-spin couplings. Another irreversible mechanism is the thermalization of the spins to equilibrium at the temperature of their environment, a process which involves exchange of energy. For a single qubit state, these effects may be phenomenologically characterized with a density matrix transformation model,

$$\begin{bmatrix} a & b \\ b^* & 1-a \end{bmatrix} \rightarrow \begin{bmatrix} (a-a_0)\,e^{-t/T_1}+a_0 & be^{-t/T_2} \\ b^*e^{-t/T_2} & (a_0-a)\,e^{-t/T_1}+1-a_0 \end{bmatrix}, \tag{7.144}$$

where T_1 and T_2 are known as the spin-lattice (or 'longitudinal') and spin-spin (or 'transverse') relaxation rates, respectively, and a_0 characterizes the thermal equilibrium state. They define important time scales for the lifetimes of non-equilibrium classical states and quantum superpositions. Theoretical tools for calculating T_1 and T_2 in NMR systems are well-developed, and, in fact, measurements of these rates play an important role in using NMR to distinguish between different chemical species.

Experimental methods for measuring T_1 and T_2 are well known in NMR. Let $R_x = e^{-i\pi X/4}$ be a 90° pulse about the $\hat{x}$ axis. To measure T_1, apply R_x^2, wait time τ, then R_x. The first pulse flips the spin by 180°, after which it relaxes for time τ back towards equilibrium (visualize this as the Bloch vector shrinking back towards the top of the Bloch sphere, the ground state), then the final 90° pulse puts the magnetization in the $\hat{x}-\hat{y}$ plane, where it is detected. The measured magnetization M from this inversion-recovery experiment is found to decay exponentially with τ as $M = M_0\,[1-2\exp(-\tau/T_1)]$. To
measure T_2, one can, to first order, simply measure the linewidth of a peak. A better way, the Carr-Purcell-Meiboom-Gill technique, is to apply an R_x operation, followed by k iterations

of 'wait time $\tau/2$, apply R_x^2, wait time $\tau/2$, apply R_x^2. This train of 180° pulses 'refocuses' couplings (Section 7.7.3) and partially cancels B_0 field inhomogeneities, so that one can better estimate the true T_2 of the system. The observed magnetization decays as $M = M_0 e^{-k\tau/T_2}$.

Multiple spin Hamiltonian

Summarizing our discussion of the NMR Hamiltonian, we can write H for an n spin coupled system as

$$H = \sum_k \omega_k Z_k + \sum_{j,k} H_{j,k}^J + H^{\mathrm{RF}} + \sum_{j,k} H_{j,k}^{\mathrm{D}} + H^{\mathrm{env}} \tag{7.145}$$

where the first term is the free precession of the spins in the ambient magnetic field, H^{D} is the magnetic dipole coupling of (7.136), H^J is the ' J ' coupling of (7.137), H^{RF} describes the effect of the externally applied radiofrequency magnetic fields of (7.135), and H^{env} describes interactions with the environment which lead to decoherence, as in (7.144).

For the sake of understanding the basic principles about how this Hamiltonian can be manipulated, we shall find it sufficient to consider the simplified Hamiltonian

$$H = \sum_k \omega_k Z_k + \sum_{j,k} Z_j \otimes Z_k + \sum_k g_k^x(t) X_k + g_k^y(t) Y_k, \tag{7.146}$$

in much of the following discussion. The treatment of the more general (7.145) follows the same ideas.

8.4.29 7.7.3 Quantum computation

Quantum information processing requires performing unitary transforms to a system prepared in a proper initial state. Three questions arise for the present system: First, how can arbitrary unitary transforms be implemented in a system of n coupled spins described by the Hamiltonian of (7.146)? And second, how can the thermal state (7.140) of an NMR system be used as a proper initial state for computation? Third, the quantum algorithms we have studied in the last three chapters ask for projective measurements to obtain output results, whereas with NMR, we can only easily perform ensemble average measurements. How can we deal with this ensemble readout problem? We answer these questions in this section.

Refocusing

Perhaps one of the most interesting techniques available to us in performing arbitrary unitary transforms using Hamiltonians of the sort of (7.146) is refocusing, as it is known in the art of NMR. Consider the simple two spin Hamiltonian $H = H^{\mathrm{sys}} + H^{\mathrm{RF}}$ where

$$H^{\mathrm{sys}} = aZ_1 + bZ_2 + cZ_1 Z_2 \tag{7.147}$$

As was shown in Section 7.7.2, when a large RF field is applied at the proper frequency, to a good approximation, we can approximate

$$e^{-iHt/\hbar} \approx e^{-iH^{\mathrm{RF}}t/\hbar} \tag{7.148}$$

This allows arbitrary single qubit operations to be performed with excellent fidelity. Let us define

$$R_{x1} = e^{-i\pi X_1/4} \tag{7.149}$$

as a 90° rotation about $\hat{x}$ on spin 1 , and similarly for spin 2 . The 180° rotation R_{x1}^2 has the special property that

$$R_{x1}^2 e^{-iaZ_1 t} R_{x1}^2 = e^{iaZ_1 t}, \tag{7.150}$$

as can be easily verified. This is known as refocusing, because of the way it reverses time evolution such that different frequency spins starting together at some point on the Bloch sphere come back to the same point on the Bloch sphere. 180° pulses applied in this manner are known as refocusing pulses. Note that in the above expression, a can be an operator as well as a constant (as long as it contains no operators which act on spin 1), and thus

$$e^{-iH^{\rm sys}t/\hbar} R_{x1}^2 e^{-iH^{\rm sys}t/\hbar} R_{x1}^2 = e^{-2ibZ_2 t/\hbar} \tag{7.151}$$

Using another set of refocusing pulses applied to spin 2 would remove even this remaining term. Refocusing is thus a useful technique for removing coupled evolution between spins, and for removing all evolution entirely.

Exercise 7.38: (Refocusing) Explicitly show that (7.150) is true (use the anti-commutativity of the Pauli matrices).

Exercise 7.39: (Three-dimensional refocusing) What set of pulses can be used to refocus evolution under any single spin Hamiltonian $H^{\rm sys} = \sum_k c_k \sigma_k$?

Exercise 7.40: (Refocusing dipolar interactions) Give a sequence of pulses which can be used to turn two spin dipolar coupling $H_{1,2}^{\rm D}$ into the much simpler form of (7.138).

Controlled-NOT gate

Realization of a controlled-NOT gate is simple using refocusing pulses and single qubit pulses. Let us show how this is done for a two spin system with the Hamiltonian of (7.147). From the construction of (7.46), we know that being able to realize the unitary transform

$$U_{CZ} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \tag{7.152}$$

is sufficient. Since $\sqrt{i} e^{iZ_1 Z_2 \pi/4} e^{-iZ_1 \pi/4} e^{-iZ_2 \pi/4} = U_{CZ}$, getting a controlled-NOT from one evolution period of time $\hbar\pi/4c$ together with several single qubit pulses is straightforward.

Exercise 7.41: (NMR controlled-NOT) Give an explicit sequence of single qubit rotations which realize a controlled-NOT between two spins evolving under the Hamiltonian of (7.147). You may start with (7.46), but the result can be simplified to reduce the number of single qubit rotations.

Temporal, spatial, and logical labeling

Being able to realize arbitrary unitary transforms on a spin system to good fidelity using RF pulses is one of the most attractive aspects of NMR for quantum computation. However, the major drawback is the fact that the initial state is usually the thermal state of (7.140). Despite the high entropy of this state, quantum computation can nevertheless be done, with some cost. Two techniques for achieving this are called temporal and logical labeling.

Temporal labeling, also sometimes called temporal averaging, is based on two important facts: quantum operations are linear, and the observables measured in NMR are traceless (see Section 2.2.5 for background on quantum measurements). Suppose a two spin system starts out with the density matrix

$$\rho_1 = \begin{bmatrix} a & 0 & 0 & 0 \\ 0 & b & 0 & 0 \\ 0 & 0 & c & 0 \\ 0 & 0 & 0 & d \end{bmatrix}, \tag{7.153}$$

where a, b, c, and d are arbitrary positive numbers satisfying $a+b+c+d = 1$. We can use a circuit P constructed from controlled-not gates to obtain a state with the permuted populations

$$\rho_2 = P\rho_1 P^\dagger = \begin{bmatrix} a & 0 & 0 & 0 \\ 0 & c & 0 & 0 \\ 0 & 0 & d & 0 \\ 0 & 0 & 0 & b \end{bmatrix}, \tag{7.154}$$

and similarly,

$$\rho_3 = P^\dagger \rho_1 P = \begin{bmatrix} a & 0 & 0 & 0 \\ 0 & d & 0 & 0 \\ 0 & 0 & b & 0 \\ 0 & 0 & 0 & c \end{bmatrix}. \tag{7.155}$$

A unitary quantum computation U is applied to each of these states, to obtain (in three separate experiments, which may be performed at different times) $C_k = U\rho_k U^\dagger$. By linearity,

$$\sum_{k=1,2,3} C_k = \sum_k U\rho_k U^\dagger \tag{7.156}$$

$$= U\left[\sum_k \rho_k\right] U^\dagger \tag{7.157}$$

$$= (4a-1)U \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} U^\dagger + (1-a) \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \tag{7.158}$$

In NMR, observables M (such as Pauli X and Y) for which $\mathrm{tr}(M) = 0$ are the only ones ever measured; thus,

$$\mathrm{tr}\left(\sum_k C_k M\right) = \sum_k \mathrm{tr}\left(C_k M\right) \tag{7.159}$$

$$= (4a-1)\,\mathrm{tr}\left(U \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} U^\dagger M\right) \tag{7.160}$$

$$= (4a-1)\,\mathrm{tr}\left(U|00\rangle\langle 00|U^\dagger\right). \tag{7.161}$$

We find that the sum of the measured signals from the three experiments gives us a result which is proportional to what we would have obtained had the original system been prepared in a pure state $|00\rangle\langle 00|$ instead of in the arbitrary state of (7.153). This is always possible to accomplish for arbitrarily prepared systems of any size, given enough experiments which are summed over, and sufficiently long coherence time for unitary operations to be performed before decoherence sets in. Note that the different C_k experiments can actually also be done

simultaneously with three different systems, or in different parts of a single system; this is experimentally feasible by applying gradient magnetic fields which vary systematically over a single sample, and that variant of this technique is called spatial labeling.

Exercise 7.42: (Permutations for temporal labeling) Give a quantum circuit to accomplish the permutations P and $P^\dagger$ necessary to transform ρ_1 of (7.153) to ρ_2 of (7.154).

Logical labeling is based on similar observations, but does not require multiple experiments to be performed. Suppose we have a system of three nearly identical spins in the state

$$\rho = \delta I + \alpha \begin{bmatrix} 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -6 \end{bmatrix} \tag{7.162}$$

$$\approx \left(\delta' I + \alpha' \begin{bmatrix} 2 & 0 \\ 0 & -2 \end{bmatrix} \right)^{\otimes 3}, \tag{7.163}$$

where δI refers to a background population which is unobservable (because of traceless measurement observables), and $\alpha \ll \delta$ is a small constant. We may then apply a unitary operation which performs a permutation P, giving

$$\rho' = P\rho P^\dagger = \delta I + \alpha \begin{bmatrix} 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -6 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \end{bmatrix}. \tag{7.164}$$

Note that the upper 4×4 block of this matrix has the form

$$\begin{bmatrix} 6 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 \\ 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & -2 \end{bmatrix} = 8|00\rangle\langle 00| - 2I, \tag{7.165}$$

where I here denotes the 4×4 identity matrix. Just as for temporal labeling, we find that if a computation is performed on such a state, in this case the $|000\rangle, |001\rangle, |010\rangle, |011\rangle$ manifold, then it produces a result which is proportional to what we would have obtained had the original system been prepared in a pure state $|00\rangle\langle 00|$! Experimentally, it is possible to perform $\tilde{P}$, and also to isolate the signal from just this manifold of states.

States which are of the form $\rho = 2^{-n}(1-\epsilon)I + \epsilon U|00\ldots0\rangle\langle 00\ldots0|U^\dagger$ (where U is any unitary operator), are called 'effective pure states', or 'pseudopure' states. n is the number of qubits, but the dimension of the Hilbert space need not be a power of two in general. There are many strategies for preparing such states, and in general they all incur some cost. We shall return to discuss this later, in Section 7.7.4. Effective pure states make it possible to observe zero temperature dynamics from a system which equilibrates to a high temperature state, as long as the coupling of the system to its high temperature environment is sufficiently small. This is the way it is used in NMR quantum computation.

Exercise 7.43: (Permutations for logical labeling) Give a quantum circuit to accomplish the permutations P necessary to transform ρ of (7.163) to ρ' of (7.165).

Exercise 7.44: (Logical labeling for n spins) Suppose we have a system of n nearly identical spins of Zeeman frequency $\hbar\omega$ in thermal equilibrium at temperature T with state ρ. What is the largest effective pure state that you can construct from ρ using logical labeling? (Hint: take advantage of states whose labels have Hamming weight of $n/2$.)

Ensemble readout of quantum algorithm results

We have seen how arbitrary unitary transforms can be performed on an n spin system with a Hamiltonian of (7.146), and we have learned how to prepare from a thermal state a well-defined input which behaves as a low-entropy ground state. However, to complete the requirements for quantum computation, we must have a way of performing measurements on the system to read out computational results. The difficulty is that the output of a typical quantum algorithm is a random number, whose distribution gives information which allows the problem to be solved. Unfortunately, the average value of the random variable does not necessarily give any relevant information. This would be the output if the quantum algorithm were executed without modification on an NMR quantum computer, since it is performed with a large ensemble of molecules, rather than with a single n spin molecule.

This difficulty is illustrated by the following example. The quantum factoring algorithm produces as its output a random rational number c/r, where c is an unknown integer, and r is the desired result (also an integer). Normally, a projective measurement is used to obtain c/r, then a classical continued fractions algorithm is performed to obtain c with high probability (Section 5.3.1). The answer is then checked by plugging in the
result to the original problem, and if it fails the entire algorithm is repeated. Unfortunately, however, if only the ensemble average is available, since c is nearly uniformly distributed the average value $\langle c/r \rangle$ gives no meaningful information.

A simple resolution to this problem, which works for all quantum algorithms based on the hidden subgroup problem (Chapter 5), is simply to append any required classical post-processing step to the quantum computation. This is always possible because quantum computation subsumes classical computation. In the example given above, we simply ask each individual quantum computer (each molecule) to perform a continued fractions algorithm. The result is then checked on each quantum computer, then only the computers which succeed in the verification give an output. The final ensemble average measurement thus gives $\langle r \rangle$.

8.4.30 7.7.4 Experiment

One of the most exciting aspects of the NMR approach is the ready experimental realization of small instances of quantum computation and quantum information tasks. In this concluding section on NMR, we briefly describe three experiments which have been performed, demonstrating state tomography, elementary logic gates, and the quantum search algorithm. We also summarize the drawbacks of this method.

State tomography

How does one debug a quantum computer? A classical computer is analyzed by measuring its internal state at different points in time. Analogously, for a quantum computer, an essential technique is the ability to measure its density matrix - this is called state tomography.

Recall that the density matrix of a single qubit can be expressed as

$$\rho = \frac{1}{2}\left[1 + \sum_k r_k \sigma_k\right], \tag{7.166}$$

where σ_k are the Pauli matrices and r_b is a real, three-component vector. Because of the trace orthogonality property of Pauli matrices,

$$\mathrm{tr}\,(\sigma_k \sigma_j) = 2\delta_{kj} \tag{7.167}$$

it follows that ρ can be reconstructed from the three measurement results

$$r_k = \langle \sigma_k \rangle = \mathrm{tr}\,(\rho \sigma_k) \tag{7.168}$$

Measurement of the usual observable in NMR, (7.143), preceded by the appropriate single qubit pulses, allows us to determine $\langle \sigma_k \rangle$, and thus obtain ρ. Similar results hold for larger numbers of spins. In practice, it is convenient to measure just the traceless deviation of ρ from the identity; this is called the deviation density matrix. Example results for two and three spin systems are shown in Figure 7.18.

Exercise 7.45: (State tomography with NMR) Let the voltage measurement $V_k(t) = V_0 \,\mathrm{tr}\left[e^{-iHt} M_k \rho M_k^\dagger e^{iHt}\,(iX_k + Y_k)\right]$ be the result of experiment k. Show that for two spins, nine experiments, with $M_0 = I, M_1 = R_{x1}, M_2 = R_{y1}$, $M_3 = R_{x2}, M_4 = R_{x2}R_{x1}, M_5 = R_{x2}R_{y1}$ etc. provide sufficient data from which ρ can be reconstructed.

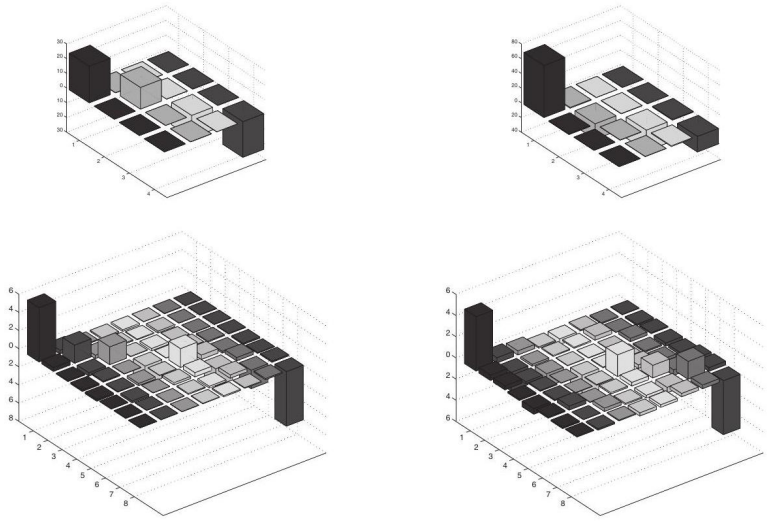


Figure 7.18. Experimentally measured deviation density matrices. Vertical scales are arbitrary, and only the real part is shown; the imaginary components are all relatively small. (top left) The two qubit thermal equilibrium state of the proton and the carbon nucleus in molecules of chloroform $\left({
ˆ{13} \mathrm{CHCl}_{3}\right)$ in a 11.78 tesla magnetic field. The 0.5 milliliter, 200 millimolar sample was diluted in acetone- d_6, degassed, and flame sealed in a thin walled, 5 mm glass tube. (top right) Two qubit effective pure state created using temporal labeling with the chloroform, as in Equation (7.161). (bottom left) The three qubit thermal equilibrium state of three fluorine nuclei in trifluoroethylene. (bottom right) An effective pure state created from the three spin system using logical labeling, as in Equation (7.164).}

Exercise 7.46: How many experiments are sufficient for three spins? Necessary?

Quantum logic gates

The two qubit proton-carbon system in chloroform presents an excellent system for demonstration of single qubit and two qubit gates, for many reasons. At ≈ 500 and ≈ 125 MHz in an ≈ 11.8 tesla field, the frequencies of the two spins are well separated and easily addressed. The 215 HzJ-coupling frequency of the two nuclei is also convenient; it is much slower than the time scale required for single qubit RF pulses, but much faster than the relaxation time scales. In typical experiments, the T_1 of the proton and carbon are approximately 18 and 25 seconds, respectively, while T_2 are 7 and 0.3 seconds. The carbon T_2 is short because of interactions with the three quadrupolar chlorine nuclei, but taking the product of the shortest T_2 lifetime and the J-coupling indicates that roughly 60 gates should still be realizable before quantum coherence is lost.

The Hamiltonian of the two spin system is very well approximated by the expression in (7.147), but it can be simplified significantly using an experimental trick. By tuning two oscillators to exactly the rotating frequencies of the proton and carbon, we obtain, in the rotating frame defined by the oscillators, the simplified Hamiltonian

$$H = 2\pi\hbar J Z_1 Z_2, \tag{7.169}$$

where $J = 215$ Hz. This Hamiltonian makes the realization of the controlled-not gate quite simple. A circuit which performs a CNOT transform equivalent up to single qubit phases is shown in Figure 7.19, as well as a circuit for creating a Bell state, and experimentally measured outputs.

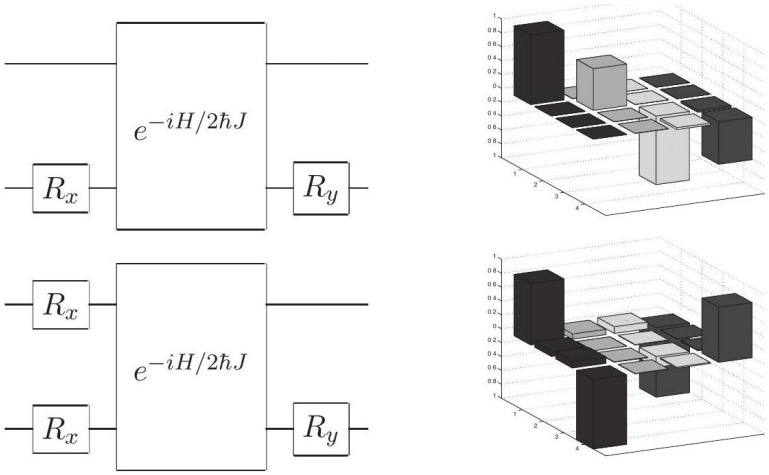


Figure 7.19. Quantum circuits implemented with NMR and the real part of the experimentally measured output deviation density matrices. In these circuits, $R_{x} and R_y denote single qubit gates which perform 90° rotations about $\hat{x}$ and $\hat{y}$, implemented with RF pulses about 10 microseconds long, and the two qubit box with $e^{-iH/2\hbar J}$ is a free evolution period of time $1/2J \approx 2.3$ milliseconds. (top) Controlled-not circuit, and the output measured for a thermal state input, showing the exchange of the $|10\rangle$ and $|11\rangle$ diagonal elements, as expected from the classical truth table for the CNOT gate. (bottom) Circuit for creating the Bell state $(|00\rangle - |11\rangle)/\sqrt{2}$, and its output, when a $|00\rangle$ effective pure state is prepared as an input.}

Exercise 7.47: (NMR controlled-NOT gate) Verify that the circuit shown in the top left of Figure 7.19 performs a controlled-NOT gate, up to single qubit phases; that is, it acts properly on classical input states, and furthermore can be turned into a proper controlled-NOT gate

by applying additional single qubit R_z rotations. Give another circuit using the same building blocks to realize a proper cNOT gate.

Exercise 7.48: Verify that the circuit shown in the bottom left of Figure 7.19 creates the Bell state $(|00\rangle - |11\rangle)/\sqrt{2}$ as advertised.

Exercise 7.49: (NMR swap gate) An important chemical application of NMR is measurement of connectivity of spins, i.e. what protons, carbons, and phosphorus atoms are nearest neighbors in a molecule. One pulse sequence to do this is known as INADEQUATE (incredible natural abundance double quantum transfer experiment - the art of NMR is full of wonderfully creative acronyms). In the language of quantum computation, it can be understood as simply trying to apply a CNOT between any two resonances; if the CNOT works, the two nuclei must be neighbors. Another building block which is used in sequences such as

TOCSY (total correlation spectroscopy) is a swap operation, but not quite in the perfect form we can describe simply with quantum gates! Construct a quantum circuit using only $e^{-iH/2\hbar J}$, R_x, and R_y operations to implement a swap gate (you may start from the circuit in Figure 1.7).

Quantum algorithms

Grover's quantum search algorithm provides another simple example for NMR quantum computation. For a problem size of four elements ($n = 2$ qubits), we are given the set $x = \{0, 1, 2, 3\}$ for which $f(x) = 0$ except at one value x_0, where $f(x_0) = 1$. The goal is to find x_0, which can be classically accomplished by evaluating $f(x)$ an average of 2.25 times. In comparison, the quantum algorithm finds x_0 by evaluating $f(x)$ only once (Chapter 6; see, in particular, Box 6.1).

Three operators are required: the oracle operator O (which performs a phase flip based on the function $f(x)$), the Hadamard operator on two qubits $H^{\otimes 2}$, and the conditional phase shift operator P. The oracle O flips the sign of the basis element corresponding to x_0; for $x_0 = 3$, this is

$$O = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \tag{7.170}$$

Denoting a $t = 1/2J$ (2.3 millisecond for the chloroform) period evolution $e^{-iH/2\hbar J}$ as τ, we find that $O = R_{y1}\bar{R}_{x1}\bar{R}_{y1}R_{y2}\bar{R}_{x2}\bar{R}_{y2}\tau$ (up to an irrelevant overall phase factor) for the $x_0 = 3$ case. $H^{\otimes 2}$ is just two single qubit Hadamard operations, $H_1 \otimes H_2$, where $H_k = R_{xk}^2\bar{R}_{yk}$. And the operator P,

$$P = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \tag{7.171}$$

is simply realized as $P = R_{y1}R_{x1}\bar{R}_{y1}R_{y2}R_{x2}\bar{R}_{y2}\tau$. From these, we construct the Grover iteration $G = H^{\otimes 2}PH^{\otimes 2}O$. This operator can be simplified straightforwardly by eliminating unnecessary operations which obviously cancel (see Exercise 7.51). Let $|\psi_k\rangle = G^k|00\rangle$ be the state after k applications of the Grover iteration to the initial state. We find that the amplitude $\langle x_0 \mid \psi_k\rangle \approx \sin((2k+1)\theta)$, where $\theta = \arcsin\left(1/\sqrt{2}\right)$; this periodicity is a fundamental property of the quantum search algorithm, and is a natural feature to test in an experiment. For the two qubit case, and $x_0 = 3$, we expect $|11\rangle = |\psi_1\rangle = -|\psi_4\rangle = |\psi_7\rangle = -|\psi_{10}\rangle$, a period of 3 if the overall sign is disregarded.

Exercise 7.50: Find quantum circuits using just single qubit rotations and $e^{-iH/2\hbar J}$ to implement the oracle O for $x_0 = 0, 1, 2$.

Exercise 7.51: Show that the Grover iteration can be simplified, by canceling adjacent single qubit rotations appropriately, to obtain

$$G = \begin{cases} \bar{R}_{x1}\bar{R}_{y1}\bar{R}_{x2}\bar{R}_{y2}\tau R_{x1}\bar{R}_{y1}R_{x2}\bar{R}_{y2}\tau & (x_0 = 3) \\ \bar{R}_{x1}\bar{R}_{y1}\bar{R}_{x2}\bar{R}_{y2}\tau R_{x1}\bar{R}_{y1}\bar{R}_{x2}\bar{R}_{y2}\tau & (x_0 = 2) \\ \bar{R}_{x1}\bar{R}_{y1}\bar{R}_{x2}\bar{R}_{y2}\tau \bar{R}_{x1}\bar{R}_{y1}R_{x2}\bar{R}_{y2}\tau & (x_0 = 1) \\ \bar{R}_{x1}\bar{R}_{y1}\bar{R}_{x2}\bar{R}_{y2}\tau \bar{R}_{x1}\bar{R}_{y1}\bar{R}_{x2}\bar{R}_{y2}\tau & (x_0 = 0) \end{cases} \tag{7.172}$$

for the four possible cases of x_0.

Figure 7.20 shows the theoretical and measured deviation density matrices $\rho_{\Delta n} = |\psi_n\rangle\langle\psi_n| - \mathrm{tr}\left(|\psi_n\rangle\langle\psi_n|\right)/4$ for the first seven iterations of U. As expected, $\rho_{\Delta 1}$ clearly reveals the $|11\rangle$ state corresponding to $x_0 = 3$. Analogous results were obtained for experiments repeated for the other possible values of x_0. Measuring each density matrix required $9 \times 3 = 27$ experimental repetitions, 9 for the tomographic reconstruction and 3 for the pure state preparation.

The longest computation, for $n = 7$, took less than 35 milliseconds, which was well within the coherence time. The periodicity of Grover's algorithm is clearly seen in Figure 7.20, with good agreement between theory and experiment. The large signal-to-noise (typically better than 10^4 to 1) was obtained with just single-shot measurements. Numerical simulations indicate that the $7 - 44\%$ errors are primarily due to inhomogeneity of the magnetic field, magnetization decay during the measurement, and imperfect calibration of the rotations (in order of importance).

Drawbacks

The bulk-ensemble NMR implementation of quantum computation has been successful in demonstrating quantum algorithms and quantum information tasks with systems up to seven qubits, which is quite impressive. However, there are important limitations which arise from the temporal, spatial, and logical labeling techniques which are at the heart of the method.

The essential objective of these labeling techniques is to isolate the signal from the subset of spins which happen to be in the $|00\ldots0\rangle$ component (or any other standard, high probability state) of the thermal equilibrium state. Temporal and spatial labeling do this by adding up signals to cancel all but the desired state; logical labeling trades off Hilbert space for purity. Irrespective of the method used, however, nothing can increase the probability of the $|00\ldots0\rangle$ component of the thermal state,

$$p_{00\ldots0} = \frac{1}{\mathcal{Z}}\langle 00\ldots0|e^{-\beta H}|00\ldots0\rangle \tag{7.173}$$

Taking $H = \sum_k \omega Z_k$, we find that $p_{00\ldots0}$ is proportional to $n2^{-n}$, for an n spin molecule. This means that the total signal decreases exponentially as the number of qubits 'distilled' into an effective pure state using labeling techniques, for constant initial state temperature.

Another limitation comes from using molecules as quantum computers. The structure of the molecule plays the role of the architecture of the computer, determining what pairs (or groups) of qubits interact with each other (analogously, the RF pulses serve as the software). Not all qubits are necessarily well connected! This is doubly important since interactions cannot be switched off, except by performing refocusing. Furthermore qubits are addressed by distinguishing them in frequency, but this rapidly becomes difficult as the number of nuclei is increased. A solution to this exists, which is to use a cellular automata style architecture, such as the one-dimensional chain $X - A - B - C - A -$

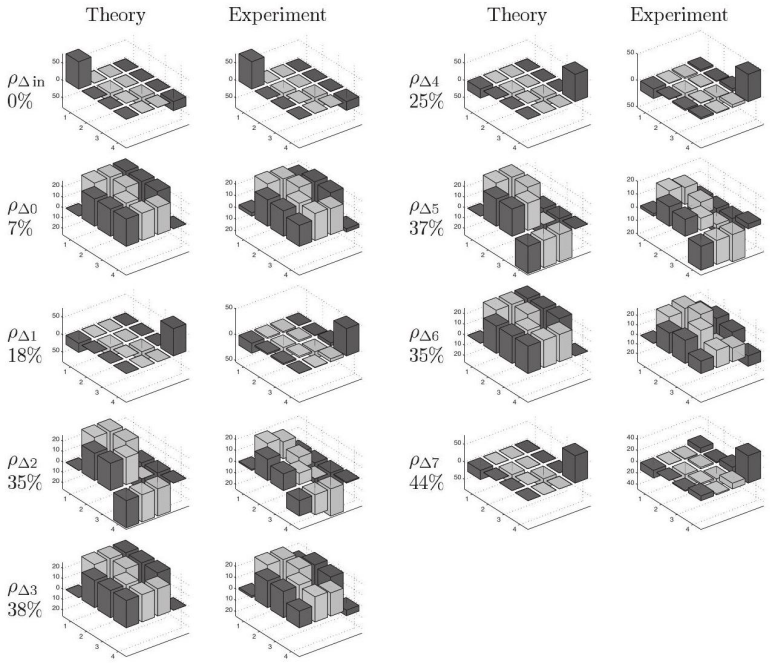


Figure 7.20. Theoretical and experimental deviation density matrices (in arbitrary units) for seven steps of Grover's algorithm performed on the hydrogen and carbon spins in chloroform. Three full cycles, with a periodicity of four iterations are clearly seen. Only the real component is plotted (the imaginary portion is theoretically zero and was found to contribute less than 12% to the experimental results). Relative errors $\left|\rho_{\text {theory }}-\rho_{expt}\right| /\left|\rho_{theory}\right|$ are shown.}

$B-C-\cdots-A-B-C-Y$, in which the ends are distinguished but the middle is composed of a repeating regular sequence. In this architecture, only distinct letters are addressable, and it might seem as if this is a highly restrictive model of computation. However, it has been shown that in fact it is universal, with only polynomial slowdown. The precise amount of slowdown required will of course be important when performing tasks such as the quantum search algorithm, which only has a square root speedup.

Methods for circumventing the limitations of labeling techniques also exist. One possibility is to polarize the nuclei through some physical mechanism; this has been done by using optical pumping (similar to how ions are cooled as shown in Figure 7.8) to polarize the electronic state of rubidium atoms, which then transfer their polarization to the nuclei of xenon atoms through formation of short-lived van der Waals molecules. This has also been done for helium. Doing similarly for molecules is conceivable, albeit technologically challenging. Another possibility is the use of a different labeling scheme; logical labeling is essentially a compression algorithm, which increases the relative probability of one state in an ensemble by discarding ensemble members. An improved version of this method has been developed which achieves the entropic limit, giving $nH(p)$ pure qubits from
n-spin molecules originally at temperature T such that $p = \left(1 - e^{-\Delta E/k_{\mathrm{B}}T}\right)/2$, where ΔE is the spin flip energy. This scheme does not have any exponential cost; the compression can be achieved using only a polynomial number of basic operations. However, it is inefficient unless p is relatively small, and today $p \approx 0.4999$ in good solenoid magnet systems.

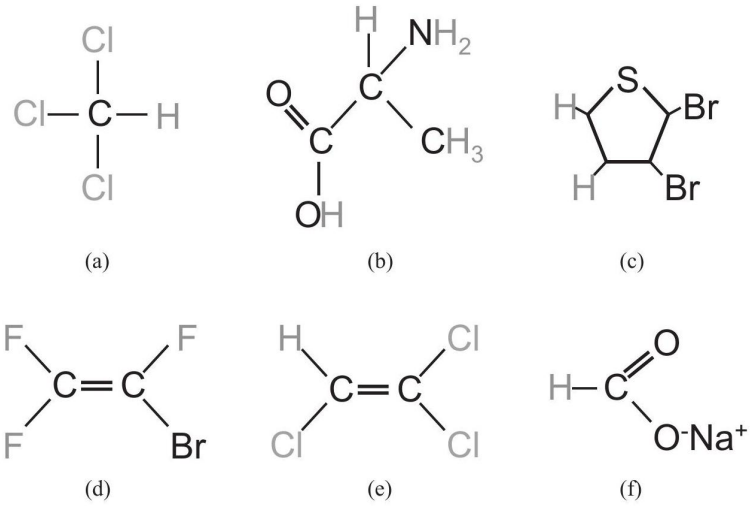


Figure 7.21. A selection of simple molecules which have been used to demonstrate various quantum computation and quantum information tasks with NMR. (a) Chloroform: two qubits, proton and carbon, have been used to implement the Deutsch-Jozsa algorithm, and a two qubit quantum search. (b) Alanine: three qubits, composed of the carbon backbone, have been used to demonstrate error-correction. Note how the three carbon nuclei have distinguishable frequencies because their surrounding chemical environments are different (for example, the electronegativity of the oxygen causes it to draw much of the nearby electrons away from the neighboring carbon). (c) 2,3-dibromothiophene: two qubits, composed of the two protons, have been used to simulate four levels of a truncated simple harmonic oscillator. Here, the two protons are at different distances from the sulphur atom, and thus have distinguishable frequencies. (d) Trifluorobromoethylene: three qubits, the three fluorines, have been used to demonstrate logical labeling and the creation of a $(|000\rangle+|111\rangle) / \sqrt{2 $ superposition state. (e) Trichloroethylene: three qubits, the proton and two carbons, were used to demonstrate teleportation, with the proton's state being teleported to the rightmost carbon. (f) Sodium formate: two qubits, proton and carbon, used to demonstrate the two qubit quantum error detection code. In this molecule, the sodium radical is used to tune the T_2 times of the two qubits to be nearly equal, by changing the ambient temperature to modify its exchange rate with the solvent.}

Despite these drawbacks, NMR provides a testbed for quantum algorithms and illustrates basic techniques which other realizations will have to implement to perform quantum computation. Some of the molecules which have been used to demonstrate quantum computation and quantum information tasks are shown in Figure 7.21. The NMR idea is also a very rich area for innovation, combining chemistry, physics, engineering, and mathematics, and undoubtedly continued innovation between fields will further this technique.

NMR quantum computer

- Qubit representation: Spin of an atomic nucleus.
- Unitary evolution: Arbitrary transforms are constructed from magnetic field pulses applied to spins in a strong magnetic field. Couplings between spins are provided by chemical bonds between neighboring atoms.
- Initial state preparation: Polarize the spins by placing them in a strong magnetic field, then use 'effective pure state' preparation techniques.

- Readout: Measure voltage signal induced by precessing magnetic moment.
- Drawbacks: Effective pure state preparation schemes reduce the signal exponentially in the number of qubits, unless the initial polarization is sufficiently high.

8.4.31 7.8 Other implementation schemes

In this chapter we have described but a fraction of the number of ideas people have considered for implementation of quantum computers. Our selection illustrates basic requirements and challenges common to all implementations: robust representation of quantum information, application of unitary transforms, preparation of a fiducial input state, and measurement of the output.

The simple harmonic oscillator example emphasizes how a digital representation is crucial: each unit (qubit, qutrit, qudit, or whatever) of quantum information should reside in physically separate degrees of freedom; otherwise, some resource (such as energy) is inefficiently utilized. That example also provides the mathematical basis for studying representations of qubits through the remainder of the chapter. Single photons are nearly ideal qubits, but the nonlinear optical materials required to get them to interact are difficult to realize without causing coherence loss. Cavity-QED techniques can address this problem by using single atoms to interact photons, but even more importantly, they introduce the notion of two-level atoms, and the idea of guarding qubit representations using selection rules imposed by physical symmetries such as dipole selection.

A natural extension of this idea is to represent qubits using spin- 1/2 particles, which inherently only have two states. This is the tack taken with trapped ions, which store qubits in electron and nuclear spins; the difficulty with this method, though, is that the center of mass oscillations - phonons - used to mediate interactions between spins have short coherence times. Molecules, in which nuclear spins can be strongly coupled by chemical bonds, can solve this difficulty, but the spin resonance signal from single molecules is too small to detect with present technology. NMR quantum computing solves this by creating 'effective pure states' with bulk ensembles of $O\left(10^{18}\right)$ molecules, thereby demonstrating simple quantum algorithms in the laboratory. But without providing initial polarization, this capability comes at the cost of signal strength, which decreases exponentially with the number of qubits.

As these examples demonstrate, coming up with a good physical realization for a quantum computer is tricky business, fraught with tradeoffs. All of the above schemes are unsatisfactory, in that none allow a large-scale quantum computer to be realized anytime in the near future. However, that does not preclude the possibility, and in fact
many other implementation schemes have been proposed, some of which we briefly touch upon in this final section here.

A good way to categorize realizations is in terms of the physical degree of freedom used to represent qubits. Recall Figure 7.1: just about anything which comes in quantum units could be a qubit, but, as we have seen, fundamental physical quanta such as photons and spin are particularly good choices.

Another fundamental quantum unit which could serve as a qubit representation is electric charge. Modern electronics provides excellent techniques to create, control, and measure charges, even at the level of single electrons. For example, quantum dots, fabricated from semiconductor materials, metals, or even small molecules, can serve as threedimensional boxes with electrostatic potentials which confine charge quanta. This is verified by observation of the Coulomb blockade effect, in which electrical conductance through dots of capacitance C is found to increase in discrete steps as a function of bias voltage across the dot, reflecting the $e^2/2C$ energy required to add each additional electron. Unlike photons, (net) charge cannot be destroyed; charges can only be moved around, and thus a charge state qubit would have to

use something like the dual-rail representation of Section 7.4.2, whereby the $|0\rangle$ and $|1\rangle$ states correspond to having charge located in either of two dots, or two states within a single dot.

Just as for single photons, single qubit operations on charge state qubits can be performed using electrostatic gates (the analogue of optical phase shifters) and either single mode waveguide couplers (the analogue of beamsplitters) for moving electrons, or tunnel junctions for quantum dots. Electrical charges experience long-range Coulomb interactions with other charges (the potential created by a single charge at distance r is $V(r) = e/4\pi\epsilon r$), and thus charges far away can modulate the phase of a local charge, much like the Kerr interaction between photons. Controlled Coulomb interactions can thus be used to perform two qubit operations. Finally, single electron charges are straightforward to measure; modern field effect transistors easily detect movements of single charges in their channels, and single electron transistors operating at ≈ 100 millikelvin temperatures can detect charge to better than $10^{-4}e/\sqrt{\text{Hz}}$ at frequencies over 200 MHz . Unfortunately, uncontrolled distant charge motion leads to dephasing; this, and other scattering mechanism such as those due to phonon interactions cause coherence times to be relatively short for charge states, on the order of hundreds of femtoseconds to hundreds of picoseconds.

Charge carriers in superconductors have also been suggested as qubit representations. At low temperatures in certain metals, two electrons can bind together through a phonon interaction to form a Cooper pair, which has charge $2e$. And just as electrons can be confined within quantum dots, Cooper pairs can be confined within an electrostatic box, such that the number of Cooper pairs in the box becomes a good quantum number, and can be used to represent quantum information. Single qubit operations can be realized by using electrostatic gates to modulate the box potential, and Josephson junctions between coupled boxes. These junctions can also be used to couple qubits, and their strength can be modulated using an external magnetic field by coupling appropriately to superconducting interferometric loops. Finally, qubits can be measured simply by measuring electric charge. This superconductor qubit representation is interesting because of the relative robustness of Cooper pairs; it is estimated that the main decoherence mechanism is spontaneous emission of electromagnetic photons, which may allow coherence times exceeding one microsecond, long compared with typical dynamical time scales of hundreds of picoseconds. Unfortunately, just as with the electronic charge representation, a fluctuating background of extraneous charges ('quasiparticles') is highly deleterious to qubit coherence. One means around this problem, using superconductor technology, is to choose instead a magnetic flux qubit representation, in which qubit states correspond to left and right hand orientations of flux localized through a superconducting loop device. Here, decoherence is caused by background magnetic fluctuations, which are expected to be much quieter than the electrostatic case.

The locality of magnetic interactions is a good feature for qubit representations, and thus we return to spin, for which schemes have also been proposed to take advantage of solid state technology. A fairly large quantum dot, even one containing many electrons, can behave as a spin- 1/2 object, where the spin is carried by a single excess electron. This spin state can be prepared by equilibrating in a strong magnetic field, at low temperatures, such that the spin flip energy ΔE is much larger than $k_B T$. Manipulating a single spin, as we have seen in Section 7.7, can be done by applying pulsed local magnetic fields, and coupled qubit operations can be realized with a controlled Heisenberg coupling,

$$H(t) = J(t)\vec{S}_1 \cdot \vec{S}_2 = \frac{1}{4}\left[X_1X_2 + Y_1Y_2 + Z_1Z_2\right] \tag{7.174}$$

where $\vec{S}$ are the spin operators (Pauli operators divided by two), and $J(t) = 4\tau_0^2(t)/u$, u being the charging energy of the dot, and $\tau_0(t)$ being the tunneling matrix element controlled by local electrostatic gates placed between dots. This interaction is universal, in the sense that

it is equivalent to the controlled-not gate (see exercise below). Spin states may, in theory, be measured by allowing the spin-carrying electron to tunnel to a readout paramagnetic dot, or to spin-dependently tunnel through a 'spin valve' to a readout electrometer. The challenge is to realize such measurements in practice; high fidelity single spin measurement in semiconductors has not been accomplished with present technology.

Exercise 7.52: (Universality of Heisenberg Hamiltonian) Show that a swap operation U can be implemented by turning on $J(t)$ for an appropriate amount of time in the Heisenberg coupling Hamiltonian of (7.174), to obtain $U = \exp\left(-i\pi \vec{S}_1 \cdot \vec{S}_2\right)$. The ' $\sqrt{\text{SWAP}}$ ' gate obtained by turning on the interaction for half this time is universal; compute this transform and show how to obtain a controlled-NOT gate by composing it with single qubit operations.

Eventually, with sufficiently advanced technology, it may be possible to place, control, and measure single nuclear spins in semiconductors, making possible the following vision. Imagine being able to precisely place single phosphorus atoms (nuclear spin-1/2) within a crystalline wafer of ^{28}Si (nuclear spin 0), positioned beneath lithographically patterned electrostatic gates. These gates allow manipulation of the electron cloud surrounding the ^{31}P dopants, to perform single qubit operations via modulation of the magnetic field seen by the ^{31}P nuclei. Additional gates located above the region separating the ^{31}P dopants can be used to artificially create electron distributions connecting adjacent ^{31}P, much like a chemical bond, thus allowing two qubit operations to be performed. Although fabrication constraints of such a scheme are extremely challenging - for example, the gates should be separated by 100Åor less, and the ^{31}P dopants must be registered precisely and in an ordered array - at least this vision articulates a possible venue for marrying quantum computing with more conventional computing technologies.

Of the schemes we have described for realizing quantum computers, the ones which have most captivated the attention of technologists are the ones based on solid state technologies. Of course, atomic, molecular, and optical quantum computing schemes continue to be proposed, using systems such as optical lattices (artificial crystals made from atoms confined by crossed beams of light) and Bose condensates which are at the forefront of those fields; someday, we may even see quantum computing proposals using mesons, quarks, and gluons, or even black holes. But the motivation to envision some kind of solid state quantum computer is enormous. It has been estimated that the world has invested over US $1 trillion in silicon technology since the invention of the transistor in the late 1940s. Condensed matter systems have also been rich in new physics, such as superconductivity, the quantum Hall effect, and the Coulomb blockade (a classical effect discovered long after it was widely thought that everything about classical physics was well known!).

This chapter has concentrated mainly on the implementation of quantum computing machines, but the basic components which were presented are also useful in many other quantum applications. Quantum cryptography and its experimental realization are described in Section 12.6. And pointers to experimental work on quantum teleportation and superdense coding are given in 'History and further reading' at the end of this chapter. The general interface between quantum communication and computation includes challenges such as distributed quantum computation; development of new algorithms and experimental implementations of such systems will certainly continue to be a rich area of research for the future.

Much of the allure of quantum computing and communication machines is certainly their potential economic ramifications, as novel information technologies. But as we have seen in this chapter, quantum computation and quantum information also motivate new questions about physical systems, and provide different ways to understand their properties. These new ideas embody a need to move away from traditional many-body, statistical, and thermodynamic studies of physical systems, all the way from atoms to condensed matter systems. They represent a new opportunity to focus instead on dynamical properties of physical systems at the single quantum level. Hopefully, by giving a flavor of the richness of this approach, this chapter will

motivate you to continue 'thinking algorithmically' about Physics.

Problem 7.1: (Efficient temporal labeling) Can you construct efficient circuits (which require only $O(\text{poly}(n))$ gates) to cyclically permute all diagonal elements in a $2^n \times 2^n$ diagonal density matrix except the $|0^n\rangle\langle 0^n|$ term?

Problem 7.2: (Computing with linear optics) In performing quantum computation with single photons, suppose that instead of the dual rail representation of Section 7.4.1 we use a unary representation of states, where $|00\ldots01\rangle$ is $0, |00\ldots010\rangle$ is $1, |00\ldots0100\rangle$ is 2 , and so on, up to $|10\ldots0\rangle$ being $2^n - 1$.

1. Show that an arbitrary unitary transformation on these states can be constructed completely from just beamsplitters and phase shifters (and no nonlinear media).

2. Construct a circuit of beamsplitters and phase shifters to perform the one qubit Deutsch-Jozsa algorithm.

3. Construct a circuit of beamsplitters and phase shifters to perform the two qubit quantum search algorithm.

4. Prove that an arbitrary unitary transform will, in general, require an exponential number (in n) of components to realize.

Problem 7.3: (Control via Jaynes-Cummings interactions) Robust and accurate control of small quantum systems - via an external classical degree of freedom is important to the ability to perform quantum computation. It is quite remarkable that atomic states can be controlled by applying optical pulses, without causing superpositions of atomic states to decohere very much! In this problem, we see what approximations are necessary for this to be the case. Let us begin with the Jaynes-Cummings Hamiltonian for a single atom coupled to a single mode of an electromagnetic field,

$$H = a^\dagger \sigma_- + a\sigma_+, \tag{7.175}$$

where $\sigma_\pm$act on the atom, and $a, a^\dagger$ act on the field.

1. For $U = e^{i\theta H}$, compute

$$A_n = \langle n|U|\alpha\rangle, \tag{7.176}$$

where $|\alpha\rangle$ and $|n\rangle$ are coherent states and number eigenstates of the field, respectively; A_n is an operator on atomic states, and you should obtain

$$A_n = e^{-|\alpha^2|}\frac{|\alpha|^2}{n!}\begin{bmatrix} \cos(\theta\sqrt{n}) & \frac{i\sqrt{n}}{\alpha}\sin(\theta\sqrt{n}) \\ \frac{i\alpha}{\sqrt{n+1}}\sin\bigl(\theta\sqrt{n+1}\bigr) & \cos\bigl(\theta\sqrt{n+1}\bigr) \end{bmatrix}. \tag{7.177}$$

The results of Exercise 7.17 may be helpful.

2. It is useful to make an approximation that α is large (without loss of generality, we may choose α real). Consider the probability distribution

$$p_n = e^{-x}\frac{x^n}{n!}, \tag{7.178}$$

which has mean $\langle n\rangle = x$, and standard deviation $\sqrt{\langle n^2\rangle - \langle n\rangle^2} = \sqrt{x}$. Now change variables to $n = x - L\sqrt{x}$, and use Stirling's approximation

$$n! \approx \sqrt{2\pi n}n^n e^{-n} \tag{7.179}$$

to obtain

$$p_L \approx \frac{e^{-L^2/2}}{\sqrt{2\pi}}. \tag{7.180}$$

3. The most important term is A_n for $n = |\alpha|^2$. Define $n = \alpha^2 + L\alpha$, and for

$$a = y\sqrt{\frac{1}{y^2} + \frac{L}{y}} \quad \text{and} \quad b = y\sqrt{\frac{1}{y^2} + \frac{L}{y} + 1}, \tag{7.181}$$

where $y = 1/\alpha$, show that

$$A_L \approx \frac{e^{-L^2/4}}{(2\pi)^{1/4}} \begin{bmatrix} \cos a\varphi & ia \sin a\varphi \\ (i/b)\sin b\varphi & \cos b\varphi \end{bmatrix}, \tag{7.182}$$

using $\theta = \varphi/\alpha$. Also verify that

$$\int_{-\infty}^{\infty} A_L^\dagger A_L dL = I \tag{7.183}$$

as expected.

4. The ideal unitary transform which occurs to the atom is

$$U = \begin{bmatrix} \cos\alpha\theta & i\sin\alpha\theta \\ i\sin\alpha\theta & \cos\alpha\theta \end{bmatrix} \tag{7.184}$$

How close is A_L to U ? See if you can estimate the fidelity

$$\mathcal{F} = \min_{|\psi\rangle} \int_{-\infty}^{\infty} \left| \langle\psi|U^\dagger A_L \right| \psi \Big\rangle \, |^2 \, dL \tag{7.185}$$

as a Taylor series in y.

Problem 7.4: (Ion trap logic with two-level atoms) The controlled-not gate described in Section 7.6.3 used a three-level atom for simplicity. It is possible to do without this third level, with some extra complication, as this problem demonstrates.

Let $\Upsilon_{\hat{n}}^{\text{blue},\,j}(\theta)$ denote the operation accomplished by pulsing light at the blue sideband frequency, $\omega = \Omega + \omega_z$, of the j th particle for time $\theta\sqrt{N}/\eta\Omega$, and similarly for the red sideband. $\hat{n}$ denotes the axis of the rotation in the $\hat{x} - \hat{y}$ plane, controlled by setting the phase of the incident light. The superscript j may be omitted when it is clear which ion is being addressed. Specifically,

$$\begin{aligned} \Upsilon_{\hat{n}}^{\text{blue}}(\theta) = \exp\Big[\big(&e^{i\varphi}|00\rangle\langle 11| + e^{-i\varphi}|11\rangle\langle 00| \\ &+ e^{i\varphi}\sqrt{2}|01\rangle\langle 12| + e^{-i\varphi}\sqrt{2}|12\rangle\langle 01| + \cdots\big)\,\frac{i\theta}{2}\Big] \end{aligned} \tag{7.186}$$

where $\hat{n} = \hat{x}\cos\varphi + \hat{y}\sin\varphi$, and the two labels in the ket represent the internal and the motional states, respectively, from left to right. The $\sqrt{2}$ factor comes from the fact that $a^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle$ for bosonic states.

(1) Show that $S^j = \Upsilon_{\hat{y}}^{\text{red},\,j}(\pi)$ performs a swap between the internal and motional states of ion j when the motional state is initially $|0\rangle$.

(2) Find a value of θ such that $\Upsilon_{\hat{n}}^{\text{blue}}(\theta)$ acting on any state in the computational subspace, spanned by $|00\rangle, |01\rangle, |10\rangle$, and $|11\rangle$, leaves it in that subspace. This should work for any axis $\hat{n}$.

(3) Show that if $\Upsilon_{\hat{n}}^{\text{blue}}(\varphi)$ stays within the computational subspace, then $U = \Upsilon_{\alpha}^{\text{blue}}(-\beta)\Upsilon_{\hat{n}}^{\text{blue}}(\theta)\Upsilon_{\alpha}^{\text{blue}}(\beta)$ also stays within the computational subspace, for any choice of rotation angle β and axis α.
(4) Find values of α and β such that U is diagonal. Specifically, it is useful to obtain an operator such as

$$\begin{bmatrix} e^{-i\pi/\sqrt{2}} & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\pi/\sqrt{2}} \end{bmatrix} \tag{7.187}$$

(5) Show that (7.187) describes a non-trivial gate, in that a controlled-NOT gate between the internal states of two ions can be constructed from it and single qubit operations. Can you come up with a composite pulse sequence for performing a CNOT without requiring the motional state to initially be $|0\rangle$?

8.4.32 Summary of Chapter 7: Quantum computers: physical realization

- There are four basic requirements for implementation of quantum computation: (1) Representation of qubits, (2) Controllable unitary evolution, (3) Preparation of initial qubit states, and (4) Measurement of final qubit states.
- Single photons can serve as good qubits, using $|01\rangle$ and $|10\rangle$ as logical 0 and 1 , but conventional nonlinear optical materials which are sufficiently strong to allow single photons to interact inevitably absorb or scatter the photons.
- Cavity-QED is a technique by which single atoms can be made to interact strongly with single photons. It provides a mechanism for using an atom to mediate interactions between single photons.
- Trapped ions can be cooled to the extent that their electronic and nuclear spin states can be controlled by applying laser pulses. By coupling spin states through center-of-mass phonons, logic gates between different ions can be performed.
- Nuclear spins are nearly ideal qubits, and single molecules would be nearly ideal quantum computers if their spin states could only be controlled and measured. Nuclear magnetic resonance makes this possible using large ensembles of molecules at room temperature, but at the expense of signal loss due to an inefficient preparation procedure.

History and further reading

For an excellent discussion of why building a quantum computer is difficult, see the article by DiVincenzo [DiV95], on which Figure 7.1 is based. DiVincenzo also presents five criteria for realizing a quantum computer, which are similar to those discussed in Section 7.2.

The quantum simple harmonic oscillator of Section 7.3 is a staple of quantum mechanics, and is treated in any standard textbook, such as [Sak95]. The general necessary and sufficient conditions for quantum computation given in Section 7.3.3 were discussed by Lloyd[Llo94].

The optical quantum computer of Section 7.4 uses as its main theoretical tools the formalism of quantum optics, which is described in many textbooks; two excellent ones are [Lou73, Gar91]. For more on basic optics and optical technology, such as polarizers, beamsplitters, photon detectors, and the like, see for example, the textbook [ST91]. The beamsplitter in the single

photon regime was studied by Campos, Saleh, and Tiech [CST89], and related to that context, the elegant connection between $SU(2)$ and two coupled harmonic oscillators was first described by Schwinger [*Sak*95]. The concept of a 'dual-rail' representation of a qubit was suggested by Yurke and used by Chuang and Yamamoto [CY95] to describe a complete quantum computer (using nonlinear Kerr media) to perform the

Deutsch-Jozsa algorithm (as in Exercise 7.13). The quantum-optical Fredkin gate was first described by Yamamoto, Kitagawa, and Igeta [YKI88] and Milburn [Mil89]. The single photon generation and detection technology required for an optical quantum computer has been discussed by Imamoglu and Yamamoto [IY94] and by Kwiat, Steinberg, Chiao, Eberhard, and Petroff [KSC +94]. An analogous mechanism using electron optics and the Coulomb interaction in place of the Kerr interaction has been discussed by Kitagawa and Ueda [KU91]. The fundamental limits of traditional, off-resonance nonlinear optical materials at single quanta levels have been studied by Watanabe and Yamamoto[WY90]. Cerf, Adami, and Kwiat have studied the simulation of quantum logic using (exponentially many) linear optical components [CAK98] . An influential earlier paper by Reck, Zeilinger, Bernstein and Bertani [RZBB94] described similar constructions, but did not make the explicit connection to quantum computation. Kwiat, Mitchell, Schwindt, and White have constructed an optical simulation of Grover's quantum search algorithm which uses linear optics, but appears to require exponential resources when scaling[KMSW99]. See Miller [Mil89 b] for a discussion of the energetics of optical communication over different distances.

Allen and Eberly [AE75] have written a beautiful treatise on two-level atoms and optical resonance. The experiment described in Section 7.5.4 was performed by Turchette, Hood, Lange, Mabuchi, and Kimble at Caltech in 1995[THL+95]. A detailed explanation is also given in Turchette's Ph.D. thesis [Tur97] . The single photons used in this experiment were called 'flying qubits'. A different approach, in which atomic states are used as qubits and the atoms travel through optical cavities, was proposed by Domokos, Raimond, Brune, and Haroche [DRBH95]. It is based on the idea of using a single atom to switch a coherent state into a cavity, as described by Davidovich, Maali, Brune, Raimond, and Haroche[DRBH87, DMB+93].

The idea of ion trap quantum compution was proposed by Cirac and Zoller [CZ95] . Our discussion of this idea in Section 7.6.1 benefited greatly from the articles by Steane [Ste97], and by Wineland, Monroe, Itano, Leibfried, King, and Meekof [WMI+98]. Earnshaw's theorem can be derived from Laplace's equation, as described in his original paper [Ear42] , or a modern electromagnetics textbook such as the one by Ramo, Whinnery, and van Duzer[RWvD84]. Figure 7.8 is drawn after Figure 6 in [Ste97]. Figure 7.7 is drawn after [WMI ${ }ˆ{+}$98]. The experiment described in Section 7.6.4 was performed by Monroe, Meekhof, King, Itano, and Wineland at the National Institute of Standards and Technology in Boulder, Colorado [MMK+95]. Figure 7.15 is reprinted courtesy of Wineland [WMI+98]. Brewer, DeVoe, and Kallenbach have envisioned using large arrays of planar ion microtraps [BDK92] as a scalable quantum computer; this is the kind of trap shown in Figure 7.12. James has extensively studied the theory of heating and other decoherence mechanisms in ion traps [Jam 98]. The impact of decoherence on ion trap quantum computation has also been studied in some depth by Plenio and Knight, who also consider effects such as the failure of the two-level approximation [PK96].

DiVincenzo first suggested the use of nuclear spins in quantum computation [DiV95b], and pointed out that the well known, and very old ENDOR (electron nucleon double resonance) pulse sequence is essentially an instance of the controlled-not gate. However, the problem of how to use an ensemble of nuclei at room temperature for quantum computation was not solved until Cory, Fahmy, and Havel[CFH97], and Gershenfeld and Chuang [GC97] realized that effective pure states could be prepared. It was also necessary to realize that quantum algorithms can be modified to allow ensemble
readout; a solution to this problem was provided in [GC97], and is presented in Section 7.7.3.

Excellent textbooks on NMR have been written by Ernst, Bodenhausen, and Wokaun [EBW87], and by Slichter [Sli96]. Warren has written a criticism of NMR quantum computation[War97]; interestingly, in the same paper he advocates using electron spin resonance (ESR) to do quantum computation. Temporal labeling was proposed by Knill, Chuang, and Laflamme[KCL98]. The NMR logic gates, and Bell state preparation circuit of Section 7.7.4 were discussed by Chuang, Gershenfeld, Kubinec, and Leung[CGKL98]. The realization of Grover's algorithm in Section 7.7.4 was by Chuang, Gershenfeld, and Kubinec [CGK98]; Figure 7.20 is taken from their paper. Linden, Kupce, and Freeman note that the swap gate may be a useful contribution of quantum computing to NMR, and provides a pulse sequence for it [LKF99]. The three spin data in Figure 7.18 showing logical labeling are from the article by Vandersypen, Yannoni, Sherwood and Chuang[VYSC99]. Yamaguchi and Yamamoto have creatively extended the NMR idea to use a crystal lattice [YY99]. The molecules shown in Figure 7.21 are attributed to (a) Chuang, Vandersypen, Zhou, Leung, and Lloyd [CVZ+98] (b) Cory, Mass, Price, Knill, Laflamme, Zurek, and Havel [CMP+98] (c) Somaroo, Tseng, Havel, Laflamme, and Cory [STH+99] (d) Vandersypen, Yannoni, Sherwood and Chuang [VYSC99] (e) Nielsen, Knill, and Laflamme[NKL98] (f) Leung, Vandersypen, Zhou, Sherwood, Yannoni, Kubinec and Chuang [LVZ+99]. Jones, Mosca, and Hansen have also realized various quantum algorithms on small molecules [*JM*98, *JMH*98]. The optimal labeling scheme which achieves the entropic limit was devised by Schulman and Vazirani[[*SV*99].

Various criticisms of the NMR approach to quantum information processing have been leveled. Perhaps the most comprehensive discussion is due to Schack and Caves [5*C*99], building on earlier work by Braunstein, Caves, Jozsa, Linden, Popescu and Schack [BCJ+99], whose main technical conclusions (though not the possible connection with NMR) were obtained by Vidal and Tarrach[Vid99] and also by Zyczkowski, Horodecki, Sanpera and Lewenstein [ZHSL99] . See also the discussion by Linden and Popescu[LP99].

There are far too many proposals for implementations of quantum computers to all be mentioned here, so only a few are given; references in the given citations should provide good leads to additional articles. Lloyd has envisioned many implementations of quantum computers, including polymer systems [Llo93] . Nakamura, Pashkin, and Tsai have demonstrated control of single Cooper-pair qubits and observation of their Rabi oscillations[NPT99]. Mooij, Orlando, Levitov, Tian, van der Waal, and Lloyd have studied the representation of a qubit using a superconducting flux representation [MOL+99]. Platzman and Dykman have creatively proposed the use of electrons bound to the surface of liquid helium as qubits [PD99]. The description of the spin based quantum dot qubit realization in Section 7.8 was proposed by Loss and DiVincenzo [LD98] ; Exercise 7.52 is due to them. An interesting entree into the literature on the coherence times of quantum dots is the article by Huibers, Switkes, Marcus, Campman, and Gossard [HSM+98]. Imamoglu, Awschalom, Burkard, DiVincenzo, Loss, Sherwin, and Small have proposed a quantum computer implementation using electron spins in quantum dots manipulated with cavity QED techniques [1AB+99]. The silicon-based nuclear spin quantum computer with ^{31}P dopants was proposed by Kane[Kan98], and Vrijen, Yablonovitch, Wang, Jiang, Balandin, Roychowdhury, Mor, and DiVincenzo [*VYW*+99] have extended this to use electron spins buried in a silicon-germanium heterostructure. Finally, Brennen, Caves, Jessen, and Deutsch [BCJD99] have proposed an implementation of quantum computation using neutral atoms trapped in a far off-resonance optical lattice.

Quantum teleportation has been experimentally realized using single photons and nuclear spins as qubits, as was described in 'History and further reading' at the end of Chapter 1. One of these implementations, by Furusawa, Sørensen, Braunstein, Fuchs, Kimble, and Polzik [FSB+98], is particularly of note in the context of this chapter, because it eschews the use of a finite Hilbert space representation of quantum information (such as qubits)! Instead, it

utilizes infinite dimensional Hilbert spaces, where continuous variables (such as position and momentum, as in Section 7.3.2) parameterize quantum states. This approach to teleportation was originally suggested by Vaidman [Vai94], then further developed by Braunstein and Kimble [BK98a]. The continuous variable representation has also been extended to superdense coding by Braunstein and Kimble [BK99]; to quantum error correction, independently by Braunstein [Bra98] and by Lloyd and Slotine [LS98]; and to computation, by Lloyd and Braunstein [LB99].

9 III Quantum information by Nielsen, Chang

9.1 8 Quantum noise and quantum operations

Until now we have dealt almost solely with the dynamics of closed quantum systems, that is, with quantum systems that do not suffer any unwanted interactions with the outside world. Although fascinating conclusions can be drawn about the information processing tasks which may be accomplished in principle in such ideal systems, these observations are tempered by the fact that in the real world there are no perfectly closed systems, except perhaps the universe as a whole. Real systems suffer from unwanted interactions with the outside world. These unwanted interactions show up as noise in quantum information processing systems. We need to understand and control such noise processes in order to build useful quantum information processing systems. This is a central topic of the third part of this book, which begins in this chapter with the description of the quantum operations formalism, a powerful set of tools enabling us to describe quantum noise and the behavior of open quantum systems.

What is the distinction between an open and a closed system? A swinging pendulum like that found in some mechanical clocks can be a nearly ideal closed system. A pendulum interacts only very slightly with the rest of the world - its environment - mainly through friction. However, to properly describe the full dynamics of the pendulum and why it eventually ceases to move one must take into account the damping effects of air friction and imperfections in the suspension mechanism of the pendulum. Similarly, no quantum systems are ever perfectly closed, and especially not quantum computers, which must be delicately programmed by an external system to perform some desired set of operations. For example, if the state of a qubit is represented by two positions of a electron, then that electron will interact with other charged particles, which act as a source of uncontrolled noise affecting the state of the qubit. An open system is nothing more than one which has interactions with some other environment system, whose dynamics we wish to neglect, or average over.

The mathematical formalism of quantum operations is the key tool for our description of the dynamics of open quantum systems. This tool is very powerful, in that it simultaneously addresses a wide range of physical scenarios. It can be used to describe not only nearly closed systems which are weakly coupled to their environments, but also systems which are strongly coupled to their environments, and closed systems that are opened suddenly and subject to measurement. Another advantage of quantum operations in applications to quantum computation and quantum information is that they are especially well adapted to describe discrete state changes, that is, transformations between an initial state ρ and final state ρ', without explicit reference to the passage of time. This discrete-time analysis is rather different to the tools traditionally used by physicists for the description of open quantum systems (such as 'master equations', 'Langevin equations', and 'stochastic differential equations'), which tend to be continuous-time descriptions.

The chapter is structured as follows. We begin in Section 8.1 with a discussion of how noise is described in classical systems. The intuition gained by understanding classical noise is invaluable in learning how to think about quantum operations and quantum noise. Section 8.2 introduces the quantum operations formalism from three different points of view, enabling

us to become thoroughly familiar with the basic theory of quantum operations. Section 8.3 illustrates several important examples of noise using quantum operations. These include such examples as depolarization, amplitude damping, and phase damping. A geometric approach to understanding quantum noise on single qubits is explained, using the Bloch sphere. Section 8.4 explains some miscellaneous applications of quantum operations: the connection between quantum operations and other tools conventionally used by physicists to describe quantum noise, such as master equations; how to experimentally determine the dynamics a quantum system undergoes using a procedure known as quantum process tomography; and an explanation of how quantum operations can be used to understand the fact that the world around us appears to obey the rules of classical physics, while it really follows quantum mechanical laws. The chapter concludes in Section 8.5 with a discussion of the limitations of the quantum operations formalism as a general approach to the description of noise in quantum systems.

9.1.1 8.1 Classical noise and Markov processes

To understand noise in quantum systems it is helpful to build some intuition by understanding noise in classical systems. How should we model noise in a classical system? Let's look at some simple examples to understand how this is done, and what it can teach us about noise in quantum systems.

Imagine a bit is being stored on a hard disk drive attached to an ordinary classical computer. The bit starts out in the state 0 or 1 , but after a long time it becomes likely that stray magnetic fields will cause the bit to become scrambled, possibly flipping its state. We can model this by a probability p for the bit to flip, and a probability $1 - p$ for the bit to remain the same. This process is illustrated in Figure 8.1.

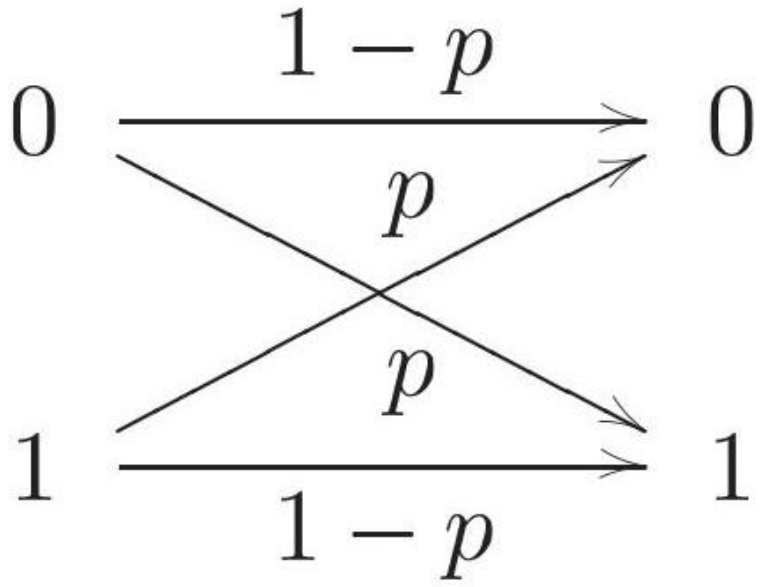


Figure 8.1. After a long time a bit on a hard disk drive may flip with probability p.

What is really going on, of course, is that the environment contains magnetic fields which can cause the bit to flip. To figure out the probability p for the bit to flip we need to understand two things. First, we need a model for the distribution of magnetic fields in the environment. Assuming that the user of the hard disk drive isn't doing anything silly like running a strong magnet near the disk drive, we can construct a realistic model by sampling the magnetic field in environments similar to the one in which the drive will be running. Second, we need a model

for how magnetic fields in the environment
will interact with bits on the disk. Fortunately, such a model is already well known to physicists, and goes by the name 'Maxwell's equations'. With these two elements in hand, we can in principle calculate the probability p that a bit flip will occur on the drive over some prescribed period of time.

This basic procedure - finding a model for the environment and for the systemenvironment interaction - is one we follow repeatedly in our study of noise, both classical and quantum. Interactions with the environment are the fundamental source of noise in both classical and quantum systems. It is often not easy to find exact models for the environment or the system-environment interaction; however, by being conservative in our modeling and closely studying the observed properties of a system to see if it obeys our model, it is possible to attain a high degree of accuracy in the modeling of noise in real physical systems.

The behavior of the bit on the hard disk can be succinctly summarized in a single equation. Suppose p_0 and p_1 are the initial probabilities that the bit is in the states 0 and 1 , respectively. Let q_0 and q_1 be the corresponding probabilities after the noise has occurred. Let X be the initial state of the bit, and Y the final state of the bit. Then the law of total probability (Appendix 1) states that

$$p(Y = y) = \sum_x p(Y = y \mid X = x)p(X = x). \tag{8.1}$$

The conditional probabilities $p(Y = y \mid X = x)$ are called transition probabilities, since they summarize the changes that may occur in the system. Writing these equations out explicitly for the bit on a hard disk we have

$$\begin{bmatrix} q_0 \\ q_1 \end{bmatrix} = \begin{bmatrix} 1-p & p \\ p & 1-p \end{bmatrix} \begin{bmatrix} p_0 \\ p_1 \end{bmatrix}. \tag{8.2}$$

Let's look at a slightly more complicated example of noise in a classical system. Imagine that we are trying to build a classical circuit to perform some computational task. Unfortunately, we've been given faulty components to build the circuit. Our rather artificial circuit consists of a single input bit, X, to which are applied two consecutive (faulty) not gates, producing an intermediate bit Y, and a final bit Z. It seems reasonable to assume that whether the second NOT gate works correctly is independent of whether the first not gate worked correctly. This assumption - that the consecutive noise processes act independently - is a physically reasonable assumption to make in many situations. It results in a stochastic process $X \to Y \to Z$ of a special type known as a Markov process. Physically, this assumption of Markovicity corresponds to assuming that the environment causing the noise in the first not gate acts independently of the environment causing the noise in the second not gate, a reasonable assumption given that the gates are likely to be located a considerable distance apart in space.

Summarizing, noise in classical systems can be described using the theory of stochastic processes. Often, in the analysis of multi-stage processes it is a good assumption to use Markov processes. For a single stage process the output probabilities $\vec{q}$ are related to the input probabilities $\vec{p}$ by the equation

$$\vec{q} = E\vec{p}, \tag{8.3}$$

where E is a matrix of transition probabilities which we shall refer to as the evolution matrix. Thus, the final state of the system is linearly related to the starting state. This
feature of linearity is echoed in the description of quantum noise, with density matrices replacing probability distributions.

What properties must the evolution matrix E possess? We require that if $\vec{p}$ is a valid probability distribution, then $E\vec{p}$ must also be a valid probability distribution. Satisfying this

condition turns out to be equivalent to two conditions on E. First, all the entries of E must be non-negative, a condition known as the positivity requirement. If they weren't, then it would be possible to obtain negative probabilities in $E\vec{p}$. Second, all the columns of E must sum to one, a condition known as the completeness requirement. Suppose this weren't true. Imagine, for example, that the first column didn't sum to one. Letting $\vec{p}$ contain a one in the first entry and zeroes everywhere else, we see that $E\vec{p}$ would not be a valid probability distribution in this case.

Summarizing, the key features of classical noise are as follows: there is a linear relationship between input and output probabilities, described by a transition matrix with non-negative entries (positivity) and columns summing to one (completeness). Classical noise processes involving multiple stages are described as Markov processes, provided the noise is caused by independent environments. Each of these key features has important analogues in the theory of quantum noise. Of course, there are also some surprising new features of quantum noise!

9.1.2 8.2 Quantum operations

9.1.3 8.2.1 Overview

The quantum operations formalism is a general tool for describing the evolution of quantum systems in a wide variety of circumstances, including stochastic changes to quantum states, much as Markov processes describe stochastic changes to classical states. Just as a classical state is described by a vector of probabilities, we shall describe quantum states in terms of the density operator (density matrix) ρ, whose properties you may wish to review by rereading Section 2.4, beginning on page 98, before continuing to read this chapter. And similar to how classical states transform as described by (8.3), quantum states transform as

$$\rho' = \mathcal{E}(\rho) \tag{8.4}$$

The map $\mathcal{E}$ in this equation is a quantum operation. Two simple examples of quantum operations which we have encountered previously, in Chapter 2, are unitary transformations and measurements, for which $\mathcal{E}(\rho) = U\rho U^\dagger$, and $\mathcal{E}_m(\rho) = M_m \rho M_m^\dagger$, respectively (see Exercises 8.1 and 8.2, below). The quantum operation captures the dynamic change to a state which occurs as the result of some physical process; ρ is the initial state before the process, and $\mathcal{E}(\rho)$ is the final state after the process occurs, possibly up to some normalization factor.

Over the next few sections, we develop a general theory of quantum operations incorporating unitary evolution, measurement, and even more general processes! We shall develop three separate ways of understanding quantum operations, illustrated in Figure 8.2, all of which turn out to be equivalent. The first method is based on the idea of studying dynamics as the result of an interaction between a system and an environment, much as classical noise was described in Section 8.1. This method is concrete and easy to relate to the real world. Unfortunately, it suffers from the drawback of not being mathematically convenient. Our second method of understanding quantum operations, completely equivalent to the first, overcomes this mathematical inconvenience by providing a powerful mathematical representation for quantum operations known as the operator-sum representation. This method is rather abstract, but is very useful for calculations and theoretical work. Our third approach to quantum operations, equivalent to the other two, is via a set of physically motivated axioms that we would expect a dynamical map in quantum mechanics to satisfy. The advantage of this approach is that it is exceedingly general - it shows that quantum dynamics will be described by quantum operations under an amazingly wide range of circumstances. However, it does not offer the calculational convenience of the second approach, nor the concrete nature of the first. Taken together, these three approaches

to quantum operations offer a powerful tool with which we can understand quantum noise and its effects.

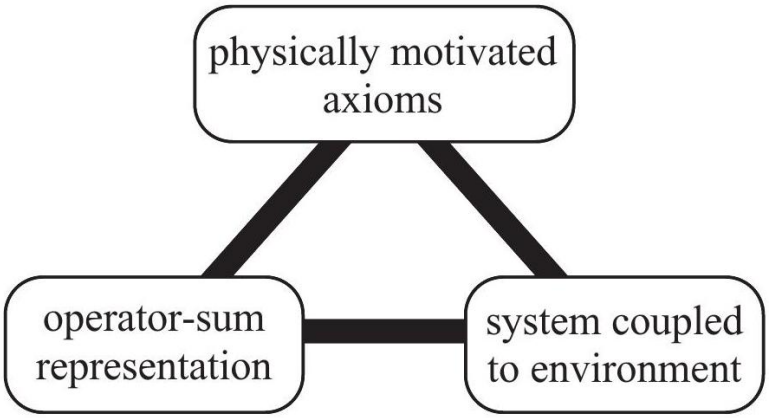


Figure 8.2. Three approaches to quantum operations which are equivalent, but offer different advantages depending upon the intended application.

Exercise 8.1: (Unitary evolution as a quantum operation) Pure states evolve under unitary transforms as $|\psi\rangle \rightarrow U|\psi\rangle$. Show that, equivalently, we may write $\rho \rightarrow \mathcal{E}(\rho) \equiv U\rho U^\dagger$, for $\rho = |\psi\rangle\langle\psi|$.

Exercise 8.2: (Measurement as a quantum operation) Recall from Section 2.2.3 (on page 84) that a quantum measurement with outcomes labeled by m is described by a set of measurement operators M_m such that $\sum_m M_m^\dagger M_m = I$. Let the state of the system immediately before the measurement be ρ. Show that for $\mathcal{E}_m(\rho) \equiv M_m \rho M_m^\dagger$, the state of the system immediately after the measurement is

$$\frac{\mathcal{E}_m(\rho)}{\mathrm{tr}\left(\mathcal{E}_m(\rho)\right)}. \tag{8.5}$$

Also show that the probability of obtaining this measurement result is $p(m) = \mathrm{tr}\left(\mathcal{E}_m(\rho)\right)$.

9.1.4 8.2.2 Environments and quantum operations

The dynamics of a closed quantum system are described by a unitary transform. Conceptually, we can think of the unitary transform as a box into which the input state enters and from which the output exits, as illustrated on the left hand side of Figure 8.3.

For our purposes, the interior workings of the box are not of concern to us; it could be implemented by a quantum circuit, or by some Hamiltonian system, or anything else.

A natural way to describe the dynamics of an open quantum system is to regard it as arising from an interaction between the system of interest, which we shall call the principal system, and an environment, which together form a closed quantum system, as illustrated on the right hand side of Figure 8.3. In other words, suppose we have a system in state ρ, which is sent into a box which is coupled to an environment. In general the final state of the system, $\mathcal{E}(\rho)$, may not be related by a unitary transformation to the initial state ρ. We assume (for now) that the system-environment input state is a product state, $\rho \otimes \rho_{\mathrm{env}}$. After the box's transformation U the system no longer interacts with the environment, and thus we perform a partial trace over the environment to obtain the reduced state of the system alone:

$$\mathcal{E}(\rho) = \mathrm{tr}\,\mathrm{env}\left[U\left(\rho \otimes \rho_{\mathrm{env}}\right)U^\dagger\right]. \tag{8.6}$$

Of course, if U does not involve any interaction with the environment, then $\mathcal{E}(\rho) = \tilde{U}\rho\tilde{U}^\dagger$, where $\tilde{U}$ is the part of U which acts on the system alone. Equation (8.6) is our first of three equivalent definitions of a quantum operation.

Figure 8.3. Models of closed (left) and open (right) quantum systems. An open quantum system consists of two parts, the principal system and an environment.

An important assumption is made in this definition - we assume that the system and the environment start in a product state. In general, of course, this is not true. Quantum systems interact constantly with their environments, building up correlations. One way this expresses itself is via the exchange of heat between the system and its environment. Left to itself a quantum system will relax to the same temperature as its environment, which causes correlations to exist between the two. However, in many cases of practical interest it is reasonable to assume that the system and its environment start out in a product state. When an experimentalist prepares a quantum system in a specified state they undo all the correlations between that system and the environment. Ideally, the correlations will be completely destroyed, leaving the system in a pure state. Even if this is not the case, we shall see later that the quantum operations formalism can even describe quantum dynamics when the system and environment do not start out in a product state.

Another issue one might raise is: how can U be specified if the environment has nearly infinite degrees of freedom? It turns out, very interestingly, that in order for this model to properly describe any possible transformation $\rho \rightarrow \mathcal{E}(\rho)$, if the principal system has a Hilbert space of d dimensions, then it suffices to model the environment as being in a Hilbert space of no more than d^2 dimensions. It also turns out not to be necessary for the environment to start out in a mixed state; a pure state will do. We shall return to these points in Section 8.2.3.

As an explicit example of the use of Equation (8.6), consider the two qubit quantum circuit shown in Figure 8.4, in which U is a controlled-NOT gate, with the principal system the control qubit, and the environment initially in the state $\rho_{\rm env} = |0\rangle\langle 0|$ as the target qubit. Inserting into Equation (8.6), it is easily seen that

$$\mathcal{E}(\rho) = P_0\rho P_0 + P_1\rho P_1, \tag{8.7}$$

where $P_0 = |0\rangle\langle 0|$ and $P_1 = |1\rangle\langle 1|$ are projection operators. Intuitively, this dynamics occurs because the environment stays in the $|0\rangle$ state only when the system is $|0\rangle$; otherwise the environment is flipped to the state $|1\rangle$. In the next section we give a derivation of this equation as an example of the operator-sum representation.

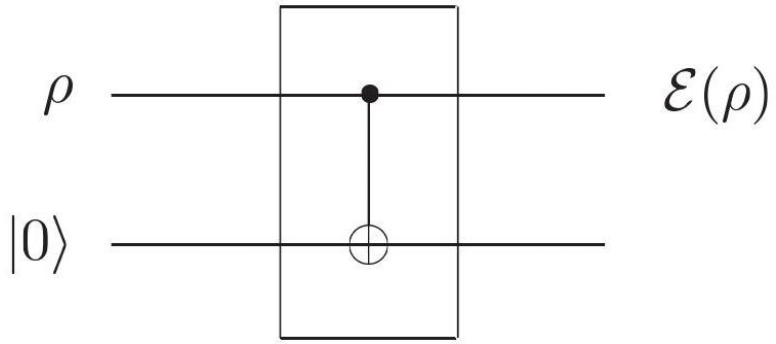


Figure 8.4. Controlled-NOT gate as an elementary example of a single qubit quantum operation.

We have described quantum operations as arising from the interaction of a principal system with an environment; however, it is convenient to generalize the definition somewhat to allow different input and output spaces. For example, imagine that a single qubit, which we label A, is prepared in an unknown state ρ. A three-level quantum system ('qutrit') labelled B is prepared in some standard state $|0\rangle$, and then interacts with system A via a unitary interaction U, causing the joint system to evolve into the state $U(\rho \otimes |0\rangle\langle 0|)U^\dagger$. We then discard system A, leaving system B in some final state ρ'. By definition, the quantum operation $\mathcal{E}$ describing this process is

$$\mathcal{E}(\rho) = \rho' = \mathrm{tr}_A \left(U(\rho \otimes |0\rangle\langle 0|)U^\dagger \right). \tag{8.8}$$

Notice that $\mathcal{E}$ maps density operators of the input system, A, to density operators of the output system, B. Most of our discussion of quantum operations below is concerned with quantum operations 'on' some system A, that is, they map density operators of system A to density operators of system A. However it is occasionally useful in applications to allow a more general definition. Such a definition is provided by defining quantum operations as the class of maps which arise as a result of the following processes: some initial system is prepared in an unknown quantum state ρ, and then brought into contact with other systems prepared in standard states, allowed to interact according to some unitary interaction, and then some part of the combined system is discarded, leaving just a final system in some state ρ'. The quantum operation $\mathcal{E}$ defining this process simply maps ρ to ρ'. We will see that this extension to allow different input and output spaces gels naturally with our treatment of quantum operations via the operator-sum representation, and also our axiomatic study. Nevertheless, for the most part it simplifies discussion if we assume that the input and output spaces of a quantum operation are the same, using the convenient distinction between 'principal system' and 'environment' which disappears
in the general case, and giving occasional exercises to indicate the necessary extensions when the input and output spaces are different.

9.1.5 8.2.3 Operator-sum representation

Quantum operations can be represented in an elegant form known as the operator-sum representation, which is essentially a re-statement of Equation (8.6) explicitly in terms of operators on the principal system's Hilbert space alone. The main result is motivated by the following simple calculation. Let $|e_k\rangle$ be an orthonormal basis for the (finite dimensional) state space of the environment, and let $\rho_{\mathrm{env}} = |e_0\rangle\langle e_0|$ be the initial state of the environment. There is no loss of generality in assuming that the environment starts in a pure state, since if it starts in a mixed state we are free to introduce an extra system purifying the environment (Section 2.5).

Although this extra system is 'fictitious', it makes no difference to the dynamics experienced by the principal system, and thus can be used as an intermediate step in calculations. Equation (8.6) can thus be rewritten as

$$\mathcal{E}(\rho) = \sum_k \langle e_k| U \left[\rho \otimes |e_0\rangle \langle e_0|\right] U^\dagger |e_k\rangle \tag{8.9}$$

$$= \sum_k E_k \rho E_k^\dagger \tag{8.10}$$

where $E_k \equiv \langle e_k| U |e_0\rangle$ is an operator on the state space of the principal system. Equation (8.10) is known as the operator-sum representation of $\mathcal{E}$. The operators $\{E_k\}$ are known as operation elements for the quantum operation $\mathcal{E}$. The operator-sum representation is important; it will be used repeatedly for the remainder of the book.

The operation elements satisfy an important constraint known as the completeness relation, analogous to the completeness relation for evolution matrices in the description of classical noise. In the classical case, the completeness relation arose from the requirement that probability distributions be normalized to one. In the quantum case the completeness relation arises from the analogous requirement that the trace of $\mathcal{E}(\rho)$ be equal to one,

$$1 = \mathrm{tr}(\mathcal{E}(\rho)) \tag{8.11}$$

$$= \mathrm{tr}\left(\sum_k E_k \rho E_k^\dagger\right) \tag{8.12}$$

$$= \mathrm{tr}\left(\sum_k E_k^\dagger E_k \rho\right). \tag{8.13}$$

Since this relationship is true for all ρ it follows that we must have

$$\sum_k E_k^\dagger E_k = I \tag{8.14}$$

This equation is satisfied by quantum operations which are trace-preserving. There are also non-trace-preserving quantum operations, for which $\sum_k E_k^\dagger E_k \leq I$, but they describe processes in which extra information about what occurred in the process is obtained by measurement, as we explain in more detail shortly. Maps $\mathcal{E}$ of the form of (8.10) for which $\sum_k E_k^\dagger E_k \leq I$ provide our second definition of a quantum operation. We show below that this definition is essentially equivalent to the first, Equation (8.6), and in fact is slightly more general, since it allows for non-trace-preserving operations. We
will often have occasion to move backwards and forwards between these two definitions; it should be clear from context which definition we are working from at any given moment.

Exercise 8.3: Our derivation of the operator-sum representation implicitly assumed that the input and output spaces for the operation were the same. Suppose a composite system AB initially in an unknown quantum state ρ is brought into contact with a composite system CD initially in some standard state $|0\rangle$, and the two systems interact according to a unitary interaction U. After the interaction we discard systems A and D, leaving a state ρ' of system BC. Show that the map $\mathcal{E}(\rho) = \rho'$ satisfies

$$\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger \tag{8.15}$$

for some set of linear operators E_k from the state space of system AB to the state space of system BC, and such that $\sum_k E_k^\dagger E_k = I$.

The operator-sum representation is important because it gives us an intrinsic means of characterizing the dynamics of the principal system. The operator-sum representation describes the dynamics of the principal system without having to explicitly consider properties of the environment; all that we need to know is bundled up into the operators E_k, which act on the principal system alone. This simplifies calculations and often provides considerable theoretical insight. Furthermore, many different environmental interactions may give rise to the same dynamics on the principal system. If it is only the dynamics of the principal system which are of interest then it makes sense to choose a representation of the dynamics which does not include unimportant information about other systems.

In the remainder of this section, we explore the properties of the operator-sum representation, and in particular, three features. First, we give it a physical interpretation, in terms of the operation elements E_k. A natural question which arises from this is how an operator-sum representation can be determined for any open quantum system (given, for example, the system-environment interaction or other specification). This is answered in the second topic addressed below, and the converse, how to construct a model open quantum system for any operator-sum representation, concludes.

Exercise 8.4: (Measurement) Suppose we have a single qubit principal system, interacting with a single qubit environment through the transform

$$U = P_0 \otimes I + P_1 \otimes X \tag{8.16}$$

where X is the usual Pauli matrix (acting on the environment), and $P_0 \equiv |0\rangle\langle 0|, P_1 \equiv |1\rangle\langle 1|$ are projectors (acting on the system). Give the quantum operation for this process, in the operator-sum representation, assuming the environment starts in the state $|0\rangle$.

Exercise 8.5: (Spin flips) Just as in the previous exercise, but now let

$$U = \frac{X}{\sqrt{2}} \otimes I + \frac{Y}{\sqrt{2}} \otimes X, \tag{8.17}$$

Give the quantum operation for this process, in the operator-sum representation.

Exercise 8.6: (Composition of quantum operations) Suppose $\mathcal{E}$ and $\mathcal{F}$ are quantum operations on the same quantum system. Show that the composition $\mathcal{F} \circ \mathcal{E}$ is a quantum operation, in the sense that it has an operator-sum representation. State and prove an extension of this result to the case where $\mathcal{E}$ and $\mathcal{F}$ do not necessarily have the same input and output spaces.

Physical interpretation of the operator-sum representation

There is a nice interpretation that can be given to the operator-sum representation. Imagine that a measurement of the environment is performed in the basis $|e_k\rangle$ after the unitary transformation U has been applied. Applying the principle of implicit measurement, we see that such a measurement affects only the state of the environment, and does not change the state of the principal system. Let ρ_k be the state of the principal system given that outcome k occurs, so

$$\rho_k \propto \mathrm{tr}_E \left(|e_k\rangle \langle e_k| U \left(\rho \otimes |e_0\rangle \langle e_0| \right) U^\dagger |e_k\rangle \langle e_k| \right) = \langle e_k| U \left(\rho \otimes |e_0\rangle \langle e_0| \right) U^\dagger |e_k\rangle \tag{8.18}$$

$$= E_k \rho E_k^\dagger \tag{8.19}$$

Normalizing ρ_k,

$$\rho_k = \frac{E_k \rho E_k^\dagger}{\mathrm{tr}\left(E_k \rho E_k^\dagger\right)}, \tag{8.20}$$

we find the probability of outcome k is given by

$$p(k) = \mathrm{tr}\left(|e_k\rangle\langle e_k| U \left(\rho \otimes |e_0\rangle\langle e_0|\right) U^\dagger |e_k\rangle\langle e_k|\right) \tag{8.21}$$

$$= \mathrm{tr}\left(E_k \rho E_k^\dagger\right) \tag{8.22}$$

Thus

$$\mathcal{E}(\rho) = \sum_k p(k)\rho_k = \sum_k E_k \rho E_k^\dagger \tag{8.23}$$

This gives us a beautiful physical interpretation of what is going on in a quantum operation with operation elements $\{E_k\}$. The action of the quantum operation is equivalent to taking the state ρ and randomly replacing it by $E_k \rho E_k^\dagger / \mathrm{tr}\left(E_k \rho E_k^\dagger\right)$, with probability $\mathrm{tr}\left(E_k \rho E_k^\dagger\right)$. In this sense, it is very similar to the concept of noisy communication channels used in classical information theory; in this vein, we shall sometimes refer to certain quantum operations which describe quantum noise processes as being noisy quantum channels.

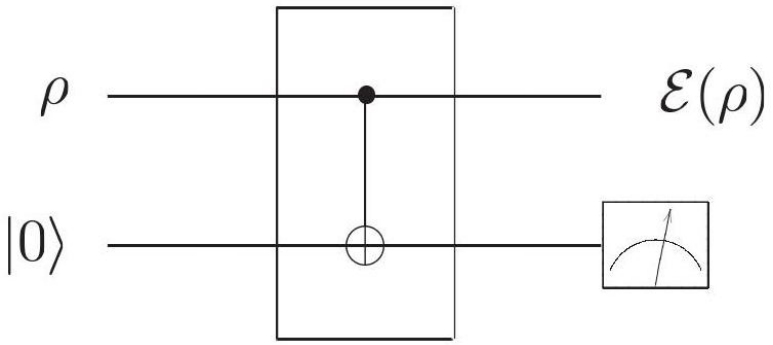


Figure 8.5. Controlled-not gate as an elementary model of single qubit measurement.

A simple example, based on Figure 8.4, illustrates this interpretation of the operatorsum representation. Suppose we choose the states $|e_k\rangle = |0_E\rangle$ and $|1_E\rangle$, where we include the E subscript to make it clear that the state is a state of the environment. This can be interpreted as doing a measurement in the computational basis of the environment qubit, as shown in Figure 8.5. Doing such a measurement does not, of course, change the state of the principal system. Using subscripts P to denote the principal system, the controlled-NOT may be expanded as

$$U = |0_P 0_E\rangle\langle 0_P 0_E| + |0_P 1_E\rangle\langle 0_P 1_E| + |1_P 1_E\rangle\langle 1_P 0_E| + |1_P 0_E\rangle\langle 1_P 1_E|. \tag{8.24}$$

Thus

$$E_0 = \langle 0_E| U |0_E\rangle = |0_P\rangle\langle 0_P| \tag{8.25}$$

$$E_1 = \langle 1_E| U |0_E\rangle = |1_P\rangle\langle 1_P|, \tag{8.26}$$

and therefore

$$\mathcal{E}(\rho) = E_0 \rho E_0 + E_1 \rho E_1, \tag{8.27}$$

in agreement with Equation (8.7).

Measurements and the operator-sum representation

Given a description of an open quantum system, how do we determine an operator-sum representation for its dynamics? We have already found one answer: given the unitary system-environment transformation operation U, and a basis of states $|e_k\rangle$ for the environment, the operation elements are

$$E_k \equiv \langle e_k | U | e_0 \rangle . \tag{8.28}$$

It is possible to extend this result even further by allowing the possibility that a measurement is performed on the combined system-environment after the unitary interaction, allowing the acquisition of information about the quantum state. It turns out that this physical possibility is naturally connected to non-trace-preserving quantum operations, that is, maps $\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger$ such that $\sum_k E_k^\dagger E_k \leq I$.

Suppose the principal system is initially in a state ρ. For convenience we denote the principal system by the letter Q. Adjoined to Q is an environment system E. We suppose that Q and E are initially independent systems, and that E starts in some standard state, σ. The joint state of the system is thus initially

$$\rho^{QE} = \rho \otimes \sigma. \tag{8.29}$$

We suppose that the systems interact according to some unitary interaction U. After the unitary interaction a projective measurement is performed on the joint system, described by projectors P_m. The case where no measurement is made corresponds to the special case where there is only a single measurement outcome, $m = 0$, which corresponds to the projector $P_0 \equiv I$.

The situation is summarized in Figure 8.6. Our aim is to determine the final state of Q as a function of the initial state, ρ. The final state of QE is given by

$$\frac{P_m U(\rho \otimes \sigma) U^\dagger P_m}{\mathrm{tr}\left(P_m U(\rho \otimes \sigma) U^\dagger P_m\right)}, \tag{8.30}$$

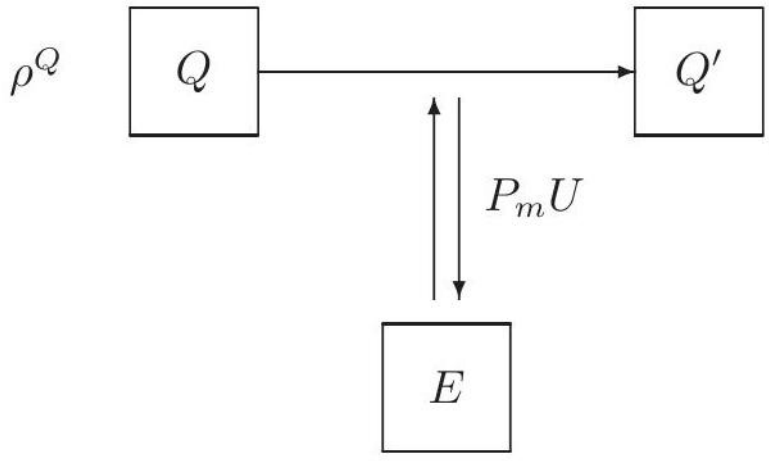


Figure 8.6. Environmental model for a quantum operation.

given that measurement outcome m occurred. Tracing out E we see that the final state of Q alone is

$$\frac{\mathrm{tr}_E\left(P_m U(\rho \otimes \sigma) U^\dagger P_m\right)}{\mathrm{tr}\left(P_m U(\rho \otimes \sigma) U^\dagger P_m\right)}. \tag{8.31}$$

This representation of the final state involves the initial state σ of the environment, the interaction U and the measurement operators P_m. Define a map

$$\mathcal{E}_m(\rho) \equiv \mathrm{tr}_E \left(P_m U(\rho \otimes \sigma) U^\dagger P_m \right), \tag{8.32}$$

so the final state of Q alone is $\mathcal{E}_m(\rho)/\mathrm{tr}\left(\mathcal{E}_m(\rho)\right)$. Note that $\mathrm{tr}\left[\mathcal{E}_m(\rho)\right]$ is the probability of outcome m of the measurement occurring. Let $\sigma = \sum_j q_j |j\rangle\langle j|$ be an ensemble decomposition for σ. Introduce an orthonormal basis $|e_k\rangle$ for the system E. Note that

$$\mathcal{E}_m(\rho) = \sum_{jk} q_j \, \mathrm{tr}_E \left(|e_k\rangle \langle e_k| \, P_m U(\rho \otimes |j\rangle\langle j|) U^\dagger P_m \, |e_k\rangle \langle e_k| \right) \tag{8.33}$$

$$= \sum_{jk} E_{jk} \rho E_{jk}^\dagger \tag{8.34}$$

where

$$E_{jk} \equiv \sqrt{q_j} \, \langle e_k| \, P_m U |j\rangle. \tag{8.35}$$

This equation is a generalization of Equation (8.10), and gives an explicit means for calculating the operators appearing in an operator-sum representation for $\mathcal{E}_m$, given that the initial state σ of E is known, and the dynamics between Q and E are known. The quantum operations $\mathcal{E}_m$ can be thought of as defining a kind of measurement process generalizing the description of measurements given in Chapter 2.

Exercise 8.7: Suppose that instead of doing a projective measurement on the combined principal system and environment we had performed a general measurement described by measurement operators $\{M_m\}$. Find operator-sum representations for the corresponding quantum operations $\mathcal{E}_m$ on the principal system, and show that the respective measurement probabilities are $\mathrm{tr}[\mathcal{E}(\rho)]$.

System-environment models for any operator-sum representation

We have shown that interacting quantum systems give rise in a natural way to an operator-sum representation for quantum operations. What about the converse problem? Given a set of operators $\{E_k\}$ is there some reasonable model environmental system and dynamics which give rise to a quantum operation with those operation elements? By 'reasonable' we mean that the dynamics must be either a unitary evolution or a projective measurement. Here, we show how to construct such a model. We will only show how to do this for quantum operations mapping the input space to the same output space, although it is mainly a matter of notation to generalize the construction to the more general case. In particular, we show that for any trace-preserving or non-trace-preserving quantum operation, $\mathcal{E}$, with operation elements $\{E_k\}$, there exists a model environment, E, starting in a pure state $|e_0\rangle$, and model dynamics specified by a unitary operator U and projector P onto E such that

$$\mathcal{E}(\rho) = \mathrm{tr}_E \left(PU \left(\rho \otimes |e_0\rangle \langle e_0| \right) U^\dagger P \right). \tag{8.36}$$

To see this, suppose first that $\mathcal{E}$ is a trace-preserving quantum operation, with operator-sum representation generated by operation elements $\{E_k\}$ satisfying the completeness relation $\sum_k E_k^\dagger E_k = I$, so we are only attempting to find an appropriate unitary operator U to model the dynamics. Let $|e_k\rangle$ be an orthonormal basis set for E, in one-to-one correspondence with the index k for the operators E_k. Note that by definition E has such a basis; we are trying to find a model environment giving rise to a dynamics described by the operation elements $\{E_k\}$. Define an operator U which has the following action on states of the form $|\psi\rangle \, |e_0\rangle$,

$$U|\psi\rangle\,|e_0\rangle \equiv \sum_k E_k|\psi\rangle\,|e_k\rangle\,, \tag{8.37}$$

where $|e_0\rangle$ is just some standard state of the model environment. Note that for arbitrary states $|\psi\rangle$ and $|\varphi\rangle$ of the principal system,

$$\langle\psi|\,\langle e_0|\,U^\dagger U|\varphi\rangle\,|e_0\rangle = \sum_k \langle\psi|E_k^\dagger E_k|\varphi\rangle = \langle\psi\mid\varphi\rangle, \tag{8.38}$$

by the completeness relation. Thus the operator U can be extended to a unitary operator acting on the entire state space of the joint system. It is easy to verify that

$$\mathrm{tr}_E\left(U\left(\rho\otimes|e_0\rangle\,\langle e_0|\right)U^\dagger\right) = \sum_k E_k\rho E_k^\dagger, \tag{8.39}$$

so this model provides a realization of the quantum operation $\mathcal{E}$ with operation elements $\{E_k\}$. This result is illustrated in Box 8.1.

Non-trace-preserving quantum operations can easily be modeled using a construction along the same lines (Exercise 8.8). A more interesting generalization of this construction is the case of a set of quantum operations $\{\mathcal{E}_m\}$ corresponding to possible outcomes from a measurement, so the quantum operation $\sum_m \mathcal{E}_m$ is trace-preserving, since the probabilities of the distinct outcomes sum to one, $1 = \sum_m p(m) = \mathrm{tr}\left[\left(\sum_m \mathcal{E}_m\right)(\rho)\right]$ for all possible inputs ρ. See Exercise 8.9, below.

Exercise 8.8: (Non-trace-preserving quantum operations) Explain how to construct a unitary operator for a system-environment model of a
non-trace-preserving quantum operation, by introducing an extra operator, E_∞, into the set of operation elements E_k, chosen so that when summing over the complete set of k, including $k=\infty$, one obtains $\sum_k E_k^\dagger E_k = I$.

Exercise 8.9: (Measurement model) If we are given a set of quantum operations $\{\mathcal{E}_m\}$ such that $\sum_m \mathcal{E}_m$ is trace-preserving, then it is possible to construct a measurement model giving rise to this set of quantum operations. For each m, let E_{mk} be a set of operation elements for $\mathcal{E}_m$. Introduce an environmental system, E, with an orthonormal basis $|m,k\rangle$ in one-to-one correspondence with the set of indices for the operation elements. Analogously to the earlier construction, define an operator U such that

$$U|\psi\rangle\,|e_0\rangle = \sum_{mk} E_{mk}|\psi\rangle|m,k\rangle. \tag{8.40}$$

Next, define projectors $P_m \equiv \sum_k |m,k\rangle\langle m,k|$ on the environmental system, E. Show that performing U on $\rho\otimes|e_0\rangle\,\langle e_0|$, then measuring P_m gives m with probability $\mathrm{tr}\left(\mathcal{E}_m(\rho)\right)$, and the corresponding post-measurement state of the principal system is $\mathcal{E}_m(\rho)/\,\mathrm{tr}\left(\mathcal{E}_m(\rho)\right)$.

Box 8.1: Mocking up a quantum operation

Given a trace-preserving quantum operation expressed in the operator-sum representation, $\mathcal{E}(\rho) = \sum_k E_k\rho E_k^\dagger$, we can construct a physical model for it in the following way. From (8.10), we want U to satisfy

$$E_k = \langle e_k|\,U\,|e_0\rangle \tag{8.41}$$

where U is some unitary operator, and $|e_k\rangle$ are orthonormal basis vectors for the environment system. Such a U is conveniently represented as the block matrix

$$U = \begin{bmatrix} [E_1] & \cdot & \cdot & \cdot \\ [E_2] & \cdot & \cdot & \cdots \\ [E_3] & \cdot & \cdot & \cdots \\ [E_4] & \cdot & \cdot & \cdots \\ \vdots & \vdots & \vdots & \vdots \end{bmatrix} \tag{8.42}$$

in the basis $|e_k\rangle$. Note that the operation elements E_k only determine the first block column of this matrix (unlike elsewhere, here it is convenient to have the first label of the states be the environment, and the second, the principal system). Determination of the rest of the matrix is left up to us; we simply choose the entries such that U is unitary. Note that by the results of Chapter 4, U can be implemented by a quantum circuit.

9.1.6 8.2.4 Axiomatic approach to quantum operations

Until now the main motivation for our study of quantum operations has been that they provide an elegant way of studying systems which are interacting with an environment. We're going to switch to a different viewpoint now, where we try to write down physically motivated axioms which we expect quantum operations to obey. This viewpoint is more abstract than our earlier approach, based on explicit system-environment models, but it is also extremely powerful because of that abstraction.

The way we're going to proceed is as follows. First, we're going to forget everything we've learned about quantum operations, and start over by defining quantum operations according to a set of axioms, which we'll justify on physical grounds. That done, we'll prove that a map $\mathcal{E}$ satisfies these axioms if and only if it has an operator-sum representation, thus providing the missing link between the abstract axiomatic formulation, and our earlier discussion.

We define a quantum operation $\mathcal{E}$ as a map from the set of density operators of the input space Q_1 to the set of density operators for the output space Q_2, with the following three axiomatic properties: (note that for notational simplicity in the proofs we take $Q_1 = Q_2 = Q$)

- A1: First, $\mathrm{tr}[\mathcal{E}(\rho)]$ is the probability that the process represented by $\mathcal{E}$ occurs, when ρ is the initial state. Thus, $0 \leq \mathrm{tr}[\mathcal{E}(\rho)] \leq 1$ for any state ρ.
- A2: Second, $\mathcal{E}$ is a convex-linear map on the set of density matrices, that is, for probabilities $\{p_i\}$,

$$\mathcal{E}\left(\sum_i p_i \rho_i\right) = \sum_i p_i \mathcal{E}\left(\rho_i\right). \tag{8.43}$$

- A3: Third, $\mathcal{E}$ is a completely positive map. That is, if $\mathcal{E}$ maps density operators of system Q_1 to density operators of system Q_2, then $\mathcal{E}(A)$ must be positive for any positive operator A. Furthermore, if we introduce an extra system R of arbitrary dimensionality, it must be true that $(\mathcal{I} \otimes \mathcal{E})(A)$ is positive for any positive operator A on the combined system RQ_1, where $\mathcal{I}$ denotes the identity map on system R.

The first property is one of mathematical convenience. To cope with the case of measurements, it turns out that it is extremely convenient to make the convention that $\mathcal{E}$ does not necessarily preserve the trace property of density matrices, that $\mathrm{tr}(\rho) = 1$. Rather, we make the convention that $\mathcal{E}$ is to be defined in such a way that $\mathrm{tr}[\mathcal{E}(\rho)]$ is equal to the probability of the measurement outcome described by $\mathcal{E}$ occurring. For example, suppose that we

are doing a projective measurement in the computational basis of a single qubit. Then two quantum operations are used to describe this process, defined by $\mathcal{E}_0(\rho) \equiv |0\rangle\langle 0|\rho|0\rangle\langle 0|$ and $\mathcal{E}_1(\rho) \equiv |1\rangle\langle 1|\rho|1\rangle\langle 1|$. Notice that the probabilities of the respective outcomes are correctly given by $\mathrm{tr}\left[\mathcal{E}_0(\rho)\right]$ and $\mathrm{tr}\left[\mathcal{E}_1(\rho)\right]$. With this convention the correctly normalized final quantum state is therefore

$$\frac{\mathcal{E}(\rho)}{\mathrm{tr}[\mathcal{E}(\rho)]} \tag{8.44}$$

In the case where the process is deterministic, that is, no measurement is taking place, this reduces to the requirement that $\mathrm{tr}[\mathcal{E}(\rho)] = 1 = \mathrm{tr}(\rho)$, for all ρ. As previously discussed, in this case, we say that the quantum operation is a trace-preserving quantum operation, since on its own $\mathcal{E}$ provides a complete description of the quantum process. On the other hand, if there is a ρ such that $\mathrm{tr}[\mathcal{E}(\rho)] < 1$, then the quantum operation is non-tracepreserving, since on its own $\mathcal{E}$ does not provide a complete description of the processes that may occur in the system. (That is, other measurement outcomes may occur, with
some probability.) A physical quantum operation is one that satisfies the requirement that probabilities never exceed $1, \mathrm{tr}[\mathcal{E}(\rho)] \leq 1$.

The second property stems from a physical requirement on quantum operations. Suppose the input ρ to the quantum operation is obtained by randomly selecting the state from an ensemble $\{p_i, \rho_i\}$ of quantum states, that is, $\rho = \sum_i p_i \rho_i$. Then we would expect that the resulting state, $\mathcal{E}(\rho)/\,\mathrm{tr}[\mathcal{E}(\rho)] = \mathcal{E}(\rho)/p(\mathcal{E})$ corresponds to a random selection from the ensemble $\{p(i \mid \mathcal{E}), \mathcal{E}\left(\rho_i\right)/\,\mathrm{tr}\left[\mathcal{E}\left(\rho_i\right)\right]\}$, where $p(i \mid \mathcal{E})$ is the probability that the state prepared was ρ_i, given that the process represented by $\mathcal{E}$ occurred. Thus, we demand that

$$\mathcal{E}(\rho) = p(\mathcal{E}) \sum_i p(i \mid \mathcal{E}) \frac{\mathcal{E}\left(\rho_i\right)}{\mathrm{tr}\left[\mathcal{E}\left(\rho_i\right)\right]} \tag{8.45}$$

where $p(\mathcal{E}) = \mathrm{tr}[\mathcal{E}(\rho)]$ is the probability that the process described by $\mathcal{E}$ occurs on input of ρ. By Bayes' rule (Appendix 1),

$$p(i \mid \mathcal{E}) = p(\mathcal{E} \mid i) \frac{p_i}{p(\mathcal{E})} = \frac{\mathrm{tr}\left[\mathcal{E}\left(\rho_i\right)\right] p_i}{p(\mathcal{E})} \tag{8.46}$$

so (8.45) reduces to (8.43).
The third property also originates from an important physical requirement, that not only must $\mathcal{E}(\rho)$ be a valid density matrix (up to normalization) so long as ρ is valid, but furthermore, if $\rho = \rho_{RQ}$ is the density matrix of some joint system of R and Q, if $\mathcal{E}$ acts only on Q, then $\mathcal{E}\left(\rho_{RQ}\right)$ must still result in a valid density matrix (up to normalization) of the joint system. An example is given in Box 8.2. Formally, suppose we introduce a second (finite dimensional) system R. Let $\mathcal{I}$ denote the identity map on system R. Then the map $\mathcal{I} \otimes \mathcal{E}$ must take positive operators to positive operators.

It is perhaps surprising that these three axioms are sufficient to define quantum operations. However, the following theorem shows that they are equivalent to the earlier system-environment models and the definition in terms of an operator-sum representation:

Theorem 8.1: The map $\mathcal{E}$ satisfies axioms **A1**, A2 and A3 if and only if

$$\mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger \tag{8.50}$$

for some set of operators $\{E_i\}$ which map the input Hilbert space to the output Hilbert space, and $\sum_i E_i^\dagger E_i \leq I$.

Proof

Suppose $\mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger \cdot \mathcal{E}$ is obviously linear, so to check that $\mathcal{E}$ is a quantum operation we need only prove that it is completely positive. Let A be any positive operator acting on the state space of an extended system, RQ, and let $|\psi\rangle$ be some state of RQ. Defining $|\varphi_i\rangle \equiv \left(I_R \otimes E_i^\dagger\right)|\psi\rangle$, we have

$$\langle\psi|\left(I_R \otimes E_i\right) A \left(I_R \otimes E_i^\dagger\right)|\psi\rangle = \langle\varphi_i| A |\varphi_i\rangle \tag{8.51}$$

$$\geq 0, \tag{8.52}$$

by the positivity of the operator A. It follows that

$$\langle\psi|(\mathcal{I} \otimes \mathcal{E})(A)|\psi\rangle = \sum_i \langle\varphi_i| A |\varphi_i\rangle \geq 0 \tag{8.53}$$

Box 8.2: Complete positivity versus positivity

The transpose operation on a single qubit provides an example of why complete positivity is an important requirement for quantum operations. By definition, this map transposes the density operator in the computational basis:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \stackrel{T}{\rightarrow} \begin{bmatrix} a & c \\ b & d \end{bmatrix}. \tag{8.47}$$

This map preserves positivity of a single qubit. However, suppose that qubit is part of a two qubit system initially in the entangled state

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}, \tag{8.48}$$

and the transpose operation is applied to the first of these two qubits, while the second qubit is subject to trivial dynamics. Then the density operator of the system after the dynamics has been applied is

$$\frac{1}{2}\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \tag{8.49}$$

A calculation shows that this operator has eigenvalues $1/2, 1/2, 1/2$ and $-1/2$, so this is not a valid density operator. Thus, the transpose operation is an example of a positive map which is not completely positive, that is, it preserves the positivity of operators on the principal system, but does not continue to preserve positivity when applied to systems which contain the principal system as a subsystem.

and thus for any positive operator A, the operator $(\mathcal{I} \otimes \mathcal{E})(A)$ is also positive, as required. The requirement $\sum_i E_i^\dagger E_i \leq I$ ensures that probabilities are less than or equal to 1. This completes the first part of the proof.

Suppose next that $\mathcal{E}$ satisfies axioms A1, A2 and A3. Our aim will be to find an operator-sum representation for $\mathcal{E}$. Suppose we introduce a system, R, with the same dimension as the original quantum system, Q. Let $|i_R\rangle$ and $|i_Q\rangle$ be orthonormal bases for R and Q. It will be convenient to use the same index, i, for these two bases, and this can certainly be done as R and Q have the same dimensionality. Define a joint state $|\alpha\rangle$ of RQ by

$$|\alpha\rangle \equiv \sum_i |i_R\rangle\, |i_Q\rangle\,. \tag{8.54}$$

The state $|\alpha\rangle$ is, up to a normalization factor, a maximally entangled state of the systems R and Q. This interpretation of $|\alpha\rangle$ as a maximally entangled state may help in understanding the following construction. Next, we define an operator σ on the state space of RQ by

$$\sigma \equiv (\mathcal{I}_R \otimes \mathcal{E})\,(|\alpha\rangle\langle\alpha|). \tag{8.55}$$

We may think of this as the result of applying the quantum operation $\mathcal{E}$ to one half of a maximally entangled state of the system RQ. It is a truly remarkable fact, which we will now demonstrate, that the operator σ completely specifies the quantum operation $\mathcal{E}$. That is, to know how $\mathcal{E}$ acts on an arbitrary state of Q, it is sufficient to know how it acts on a single maximally entangled state of Q with another system!

The trick which allows us to recover $\mathcal{E}$ from σ is as follows. Let $|\psi\rangle = \sum_j \psi_j\, |j_Q\rangle$ be any state of system Q. Define a corresponding state $|\tilde{\psi}\rangle$ of system R by the equation

$$|\tilde{\psi}\rangle \equiv \sum_j \psi_j^*\, |j_R\rangle \tag{8.56}$$

Notice that

$$\langle\tilde{\psi}|\sigma|\tilde{\psi}\rangle = \langle\tilde{\psi}| \left(\sum_{ij} |i_R\rangle\, \langle j_R| \otimes \mathcal{E}\,(|i_Q\rangle\, \langle j_Q|) \right) |\tilde{\psi}\rangle \tag{8.57}$$

$$= \sum_{ij} \psi_i \psi_j^* \mathcal{E}\,(|i_Q\rangle\, \langle j_Q|) \tag{8.58}$$

$$= \mathcal{E}(|\psi\rangle\langle\psi|) \tag{8.59}$$

Let $\sigma = \sum_i |s_i\rangle\, \langle s_i|$ be some decomposition of σ, where the vectors $|s_i\rangle$ need not be normalized. Define a map

$$E_i(|\psi\rangle) \equiv \left\langle \tilde{\psi} \mid s_i \right\rangle \tag{8.60}$$

A little thought shows that this map is a linear map, so E_i is a linear operator on the state space of Q. Furthermore, we have

$$\sum_i E_i|\psi\rangle\langle\psi|E_i^\dagger = \sum_i \left\langle \tilde{\psi} \mid s_i \right\rangle \left\langle s_i \mid \tilde{\psi} \right\rangle \tag{8.61}$$

$$= \langle\tilde{\psi}|\sigma|\tilde{\psi}\rangle \tag{8.62}$$

$$= \mathcal{E}(|\psi\rangle\langle\psi|). \tag{8.63}$$

Thus

$$\mathcal{E}(|\psi\rangle\langle\psi|) = \sum_i E_i|\psi\rangle\langle\psi|E_i^\dagger \tag{8.64}$$

for all pure states, $|\psi\rangle$, of Q. By convex-linearity it follows that

$$\mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger \tag{8.65}$$

in general. The condition $\sum_i E_i^\dagger E_i \leq I$ follows immediately from axiom A1 identifying the trace of $\mathcal{E}(\rho)$ with a probability.

Freedom in the operator-sum representation

We have seen that the operator-sum representation provides a very general description of the dynamics of an open quantum system. Is it a unique description?

Consider quantum operations $\mathcal{E}$ and $\mathcal{F}$ acting on a single qubit with the operatorsum representations $\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger$ and $\mathcal{F}(\rho) = \sum_k F_k \rho F_k^\dagger$, where the operation elements for $\mathcal{E}$ and $\mathcal{F}$ are defined by

$$E_1 = \frac{I}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad E_2 = \frac{Z}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{8.66}$$

and

$$F_1 = |0\rangle\langle 0| = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \quad F_2 = |1\rangle\langle 1| = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}. \tag{8.67}$$

These appear to be very different quantum operations. What is interesting is that $\mathcal{E}$ and $\mathcal{F}$ are actually the same quantum operation. To see this, note that $F_1 = (E_1 + E_2)/\sqrt{2}$ and $F_2 = (E_1 - E_2)/\sqrt{2}$. Thus,

$$\mathcal{F}(\rho) = \frac{(E_1 + E_2)\,\rho\left(E_1^\dagger + E_2^\dagger\right) + (E_1 - E_2)\,\rho\left(E_1^\dagger - E_2^\dagger\right)}{2} \tag{8.68}$$

$$= E_1 \rho E_1^\dagger + E_2 \rho E_2^\dagger \tag{8.69}$$

$$= \mathcal{E}(\rho). \tag{8.70}$$

This example shows that the operation elements appearing in an operator-sum representation for a quantum operation are not unique.

The freedom in the representation is very interesting. Suppose we flipped a fair coin, and, depending on the outcome of the coin toss, applied either the unitary operator I or Z to the quantum system. This process corresponds to the first operator-sum representation for $\mathcal{E}$. The second operator-sum representation for $\mathcal{E}$ (labeled $\mathcal{F}$ above) corresponds to performing a projective measurement in the $\{|0\rangle, |1\rangle\}$ basis, with the outcome of the measurement unknown. These two apparently very different physical processes give rise to exactly the same dynamics for the principal system.

When do two sets of operation elements give rise to the same quantum operation? Understanding this question is important for at least two reasons. First, from a physical point of view, understanding the freedom in the representation gives us more insight into how different physical processes can give rise to the same system dynamics. Second, understanding the freedom in operator-sum representation is crucial to a good understanding of quantum error-correction.

Intuitively, it is clear that there must be a great deal of freedom in an operatorsum representation. Consider a trace-preserving quantum operation $\mathcal{E}$ which describes the dynamics of some system such as that shown in Figure 8.3. We have shown that the operation elements $E_k = \langle e_k | U | e_0 \rangle$ for $\mathcal{E}$ may be associated with an orthonormal basis $|e_k\rangle$ for the environment. Suppose that we supplement the interaction U with an additional unitary action U' on the environment alone, as shown in Figure 8.7. Clearly this does not change the state of the principal system. What are the corresponding operation elements to this new process, $(I \otimes U')\,U$? We obtain:

$$F_k = \langle e_k | (I \otimes U') U | e_0 \rangle \tag{8.71}$$
$$= \sum_j [I \otimes \langle e_k | U' | e_j \rangle] \langle e_j | U | e_0 \rangle \tag{8.72}$$
$$= \sum_j U'_{kj} E_j, \tag{8.73}$$

where we have used the fact that $\sum_j |e_j\rangle \langle e_j| = I$, and U'_{kj} are the matrix elements of U' with respect to the basis $|e_k\rangle$. It turns out that the freedom in the operator-sum representation yielded by this physically motivated picture captures the essence of the complete freedom available in the operator-sum representation, as proved in the following theorem.

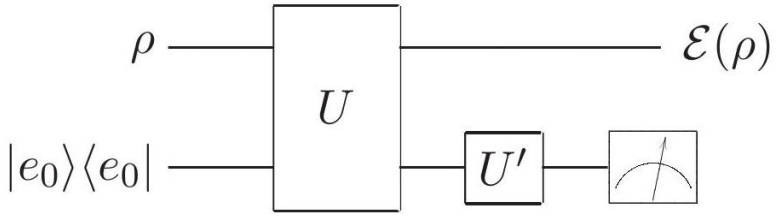


Figure 8.7. Origin of the unitary freedom in the operator-sum representation.

Theorem 8.2: (Unitary freedom in the operator-sum representation) Suppose $\{E_1, \ldots, E_m\}$ and $\{F_1, \ldots, F_n\}$ are operation elements giving rise to quantum operations $\mathcal{E}$ and $\mathcal{F}$, respectively. By appending zero operators to the shorter list of operation elements we may ensure that $m = n$. Then $\mathcal{E} = \mathcal{F}$ if and only if there exist complex numbers u_{ij} such that $E_i = \sum_j u_{ij} F_j$, and u_{ij} is an m by m unitary matrix.

Proof

The key to the proof is Theorem 2.6, on page 103. Recall that this result tells us that two sets of vectors $|\psi_i\rangle$ and $|\varphi_j\rangle$ generate the same operator if and only if

$$|\psi_i\rangle = \sum_j u_{ij} |\varphi_j\rangle , \tag{8.74}$$

where u_{ij} is a unitary matrix of complex numbers, and we 'pad' whichever set of states $|\psi_i\rangle$ or $|\varphi_j\rangle$ is smaller with additional states 0 so that the two sets have the same number of elements. This result allows us to characterize the freedom in operator-sum representations. Suppose $\{E_i\}$ and $\{F_j\}$ are two sets of operation elements for the same quantum operation, $\sum_i E_i \rho E_i^\dagger = \sum_j F_j \rho F_j^\dagger$ for all ρ. Define

$$|e_i\rangle \equiv \sum_k |k_R\rangle (E_i |k_Q\rangle) \tag{8.75}$$
$$|f_j\rangle \equiv \sum_k |k_R\rangle (F_j |k_Q\rangle) . \tag{8.76}$$

Recall the definition of σ in Equation (8.55), from which it follows that $\sigma = \sum_i |e_i\rangle \langle e_i| = \sum_j |f_j\rangle \langle f_j|$, and thus there exists unitary u_{ij} such that

$$|e_i\rangle = \sum_j u_{ij} |f_j\rangle . \tag{8.77}$$

But for arbitrary $|\psi\rangle$ we have

$$E_i|\psi\rangle = \left\langle \tilde{\psi} \mid e_i \right\rangle \tag{8.78}$$

$$= \sum_j u_{ij} \left\langle \tilde{\psi} \mid f_j \right\rangle \tag{8.79}$$

$$= \sum_k u_{ij} F_j |\psi\rangle. \tag{8.80}$$

Thus

$$E_i = \sum_j u_{ij} F_j. \tag{8.81}$$

Conversely, supposing E_i and F_j are related by a unitary transformation of the form $E_i = \sum_{ij} u_{ij} F_j$, simple algebra shows that the quantum operation with operation elements $\{E_i\}$ is the same as the quantum operation with operation elements $\{F_j\}$. □

Theorem 8.2 can be used to answer another interesting question: what is the maximum size of an environment that would be needed to mock up a given quantum operation?

Theorem 8.3: All quantum operations $\mathcal{E}$ on a system of Hilbert space dimension d can be generated by an operator-sum representation containing at most d^2 elements,

$$\mathcal{E}(\rho) = \sum_{k=1}^{M} E_k \rho E_k^\dagger, \tag{8.82}$$

where $1 \leq M \leq d^2$.

The proof of this theorem is simple and is left as an exercise for you.

Exercise 8.10: Give a proof of Theorem 8.3 based on the freedom in the operator-sum representation, as follows. Let $\{E_j\}$ be a set of operation elements for $\mathcal{E}$. Define a matrix $W_{jk} \equiv \mathrm{tr}\left(E_j^\dagger E_k\right)$. Show that the matrix W is Hermitian and of rank at most d^2, and thus there is unitary matrix u such that $uWu^\dagger$ is diagonal with at most d^2 non-zero entries. Use u to define a new set of at most d^2 non-zero operation elements $\{F_j\}$ for $\mathcal{E}$.

Exercise 8.11: Suppose $\mathcal{E}$ is a quantum operation mapping a d-dimensional input space to a d'-dimensional output space. Show that $\mathcal{E}$ can be described using a set of at most dd' operation elements $\{E_k\}$.

The freedom in the operator-sum representation is surprisingly useful. We use it, for example, in our study of quantum error-correction in Chapter 10. In that chapter we will see that certain sets of operators in the operator-sum representation give more useful information about the quantum error-correction process, and it behooves us to study quantum error-correction from that point of view. As usual, having multiple ways of understanding a process gives us much more insight into what is going on.

9.1.7 8.3 Examples of quantum noise and quantum operations

In this section we examine some concrete examples of quantum noise and quantum operations. These models illustrate the power of the quantum operations formalism we have been developing. They are also important in understanding the practical effects of noise on quantum systems, and how noise can be controlled by techniques such as error-correction.

We begin in Section 8.3.1 by considering how measurement can be described as a quantum operation, and in particular we consider the trace and partial trace operations. After that, we turn to noise processes, beginning in Section 8.3.2 with the presentation of a graphical

method for understanding quantum operations on a single qubit. This method is used in the remainder of the section to illustrate elementary bit and phase flip error processes (in Section 8.3.3), the depolarizing channel (in Section 8.3.4), amplitude damping (in Section 8.3.5), and phase damping (in Section 8.3.6). Amplitude and phase
damping are ideal models of noise that capture many of the most important features of the noise occurring in quantum mechanical systems, and we not only consider their abstract mathematical formulation, but also how the processes arise in real-world quantum systems.

9.1.8 8.3.1 Trace and partial trace

One of the main uses of the quantum operations formalism is to describe the effects of measurement. Quantum operations can be used to describe both the probability of getting a particular outcome from a measurement on a quantum system, and also the state change in the system effected by the measurement.

The simplest operation related to measurement is the trace map $\rho \rightarrow \mathrm{tr}(\rho)-$ which we can show is indeed a quantum operation, in the following way. Let H_Q be any input Hilbert space, spanned by an orthonormal basis $|1\rangle \ldots |d\rangle$, and let H'_Q be a onedimensional output space, spanned by the state $|0\rangle$. Define

$$\mathcal{E}(\rho) \equiv \sum_{i=1}^{d} |0\rangle\langle i|\rho|i\rangle\langle 0|, \tag{8.83}$$

so that $\mathcal{E}$ is a quantum operation, by Theorem 8.1. Note that $\mathcal{E}(\rho) = \mathrm{tr}(\rho)|0\rangle\langle 0|$, so that, up to the unimportant $|0\rangle\langle 0|$ multiplier, this quantum operation is identical to the trace function.

An even more useful result is the observation that the partial trace is a quantum operation. Suppose we have a joint system QR, and wish to trace out system R. Let $|j\rangle$ be a basis for system R. Define a linear operator $E_i : H_{QR} \rightarrow H_Q$ by

$$E_i \left(\sum_j \lambda_j |q_j\rangle |j\rangle \right) \equiv \lambda_i |q_i\rangle \tag{8.84}$$

where λ_j are complex numbers, and $|q_j\rangle$ are arbitrary states of system Q. Define $\mathcal{E}$ to be the quantum operation with operation elements $\{E_i\}$, that is,

$$\mathcal{E}(\rho) \equiv \sum_i E_i \rho E_i^\dagger \tag{8.85}$$

By Theorem 8.1, this is a quantum operation from system QR to system Q. Notice that

$$\mathcal{E}\left(\rho \otimes |j\rangle \langle j'|\right) = \rho \delta_{j,j'} = \mathrm{tr}_R\left(\rho \otimes |j\rangle \langle j'|\right), \tag{8.86}$$

where ρ is any Hermitian operator on the state space of system Q, and $|j\rangle$ and $|j'\rangle$ are members of the orthonormal basis for system R. By linearity of $\mathcal{E}$ and tr_R, it follows that $\mathcal{E} = \mathrm{tr}_R$.

9.1.9 8.3.2 Geometric picture of single qubit quantum operations

There is an elegant geometric method for picturing quantum operations on a single qubit. This method allows one to get an intuitive feel for the behavior of quantum operations in terms of their action on the Bloch sphere. Recall from Exercise 2.72 on page 105 that the state of a single qubit can always be written in the Bloch representation,

$$\rho = \frac{I + \vec{r} \cdot \vec{\sigma}}{2}, \tag{8.87}$$

where $\vec{r}$ is a three component real vector. Explicitly, this gives us

$$\rho = \frac{1}{2} \begin{bmatrix} 1 + r_z & r_x - i r_y \\ r_x + i r_y & 1 - r_z \end{bmatrix}. \tag{8.88}$$

In this representation, it turns out that an arbitrary trace-preserving quantum operation is equivalent to a map of the form

$$\vec{r} \xrightarrow{\mathcal{E}} \vec{r}' = M\vec{r} + \vec{c}, \tag{8.89}$$

where M is a 3×3 real matrix, and $\vec{c}$ is a constant vector. This is an affine map, mapping the Bloch sphere into itself. To see this, suppose the operators E_i generating the operator-sum representation for $\mathcal{E}$ are written in the form

$$E_i = \alpha_i I + \sum_{k=1}^{3} a_{ik} \sigma_k. \tag{8.90}$$

Then it is not difficult to check that

$$\begin{aligned} M_{jk} &= \sum_l \left[a_{lj} a_{lk}^* + a_{lj}^* a_{lk} + \left(|\alpha_l|^2 - \sum_p a_{lp} a_{lp}^* \right) \delta_{jk} + i \sum_p \epsilon_{jkp} \left(\alpha_l a_{lp}^* - \alpha_l^* a_{lp} \right) \right] \\ c_k &= 2i \sum_l \sum_{jp} \epsilon_{jpk} a_{lj} a_{lp}^* \end{aligned} \tag{8.91}$$

where we have made use of the completeness relation $\sum_i E_i^\dagger E_i = I$ to simplify the expression for $\vec{c}$.

The meaning of the affine map, Equation (8.89), is made clearer by considering the polar decomposition of the matrix $M, M = U|M|$, where U is unitary. Because M is real, it follows that $|M|$ is real and Hermitian, that is, $|M|$ is a symmetric matrix. Furthermore, because M is real we may assume that U is real, and is thus an orthogonal matrix, that is, $U^T U = I$, where T is the transpose operation. Thus we may write

$$M = OS, \tag{8.93}$$

where O is a real orthogonal matrix with determinant 1 , representing a proper rotation, and S is a real symmetric matrix. Viewed this way, Equation (8.89) is just a deformation of the Bloch sphere along principal axes determined by S, followed by a proper rotation due to O, followed by a displacement due to $\vec{c}$.

Exercise 8.12: Why can we assume that O has determinant 1 in the decomposition (8.93)?

Exercise 8.13: Show that unitary transformations correspond to rotations of the Bloch sphere.

Exercise 8.14: Show that $\det(S)$ need not be positive.

9.1.10 8.3.3 Bit flip and phase flip channels

The geometric picture described above can be used to visualize some important quantum operations on single qubits, which will later be used in the theory of error-correction. The bit flip channel flips the state of a qubit from $|0\rangle$ to $|1\rangle$ (and vice versa) with probability $1 - p$. It has operation elements

$$E_0 = \sqrt{p} I = \sqrt{p} \left[\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right] \quad E_1 = \sqrt{1-p} X = \sqrt{1-p} \left[\begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array} \right]. \tag{8.94}$$

The effect of the bit flip channel is illustrated in Figure 8.8.

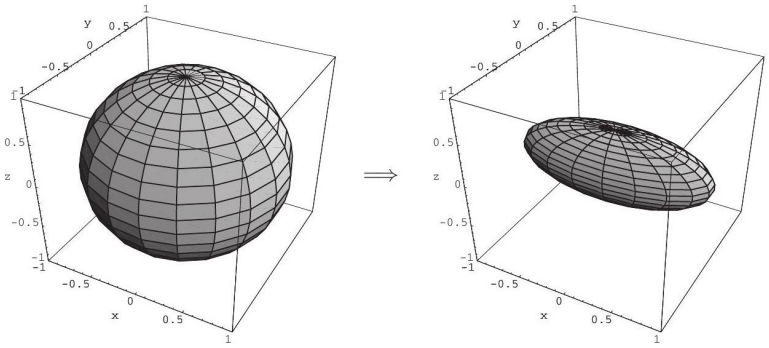


Figure 8.8. The effect of the bit flip channel on the Bloch sphere, for $p = 0.3$. The sphere on the left represents the set of all pure states, and the deformed sphere on the right represents the states after going through the channel. Note that the states on the $\hat{x}$ axis are left alone, while the $\hat{y} - \hat{z}$ plane is uniformly contracted by a factor of $1 - 2p$.

This geometric picture makes it very easy to verify certain facts about this quantum operation. For example, it is easy to verify that the quantity $\mathrm{tr}\left(\rho^2\right)$ for a single qubit is equal to $\left(1 + |r|^2\right)/2$, where $|r|$ is the norm of the Bloch vector. The contraction of the Bloch sphere illustrated in Figure 8.8 cannot increase the norm of the Bloch vector, and therefore we can immediately conclude that $\mathrm{tr}\left(\rho^2\right)$ can only ever decrease for the bit flip channel. This is but one example of the use of the geometric picture; once it becomes sufficiently familiar it becomes a great source of insight about the properties of quantum operations on a single qubit.

The phase flip channel has operation elements

$$E_0 = \sqrt{p} I = \sqrt{p} \left[\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right] \quad E_1 = \sqrt{1-p} Z = \sqrt{1-p} \left[\begin{array}{cc} 1 & 0 \\ 0 & -1 \end{array} \right]. \tag{8.95}$$

The effect of the phase flip channel is illustrated in Figure 8.9. As a special case of the phase flip channel, consider the quantum operation which arises when we choose $p = 1/2$. Using the freedom in the operator-sum representation this operation may be written

$$\rho \rightarrow \mathcal{E}(\rho) = P_0 \rho P_0 + P_1 \rho P_1, \tag{8.96}$$

where $P_0 = |0\rangle\langle 0|, P_1 = |1\rangle\langle 1|$, which corresponds to a measurement of the qubit in the $|0\rangle, |1\rangle$ basis, with the result of the measurement unknown. Using the above prescription it is easy to see that the corresponding map on the Bloch sphere is given by

$$(r_x, r_y, r_z) \rightarrow (0, 0, r_z). \tag{8.97}$$

Geometrically, the Bloch vector is projected along the z axis, and the x and y components of the Bloch vector are lost.

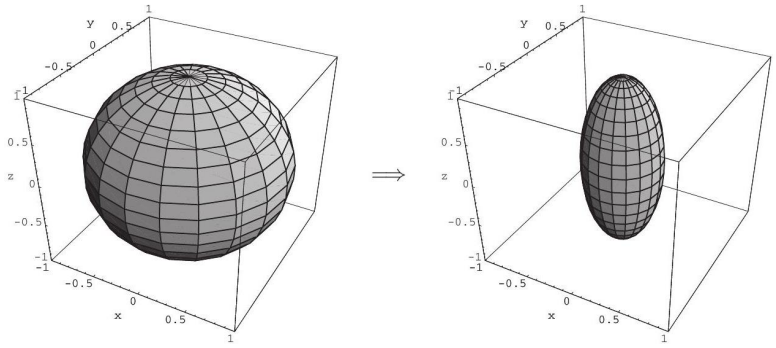


Figure 8.9. The effect of the phase flip channel on the Bloch sphere, for $p = 0.3$. Note that the states on the $\hat{z}$ axis are left alone, while the $\hat{x} - \hat{y}$ plane is uniformly contracted by a factor of $1 - 2p$.}

The bit-phase flip channel has operation elements

$$E_0 = \sqrt{p} I = \sqrt{p} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad E_1 = \sqrt{1-p} Y = \sqrt{1-p} \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}. \tag{8.98}$$

As the name indicates, this is a combination of a phase flip and a bit flip, since $Y = iXZ$. The action of the bit-phase flip channel is illustrated in Figure 8.10.

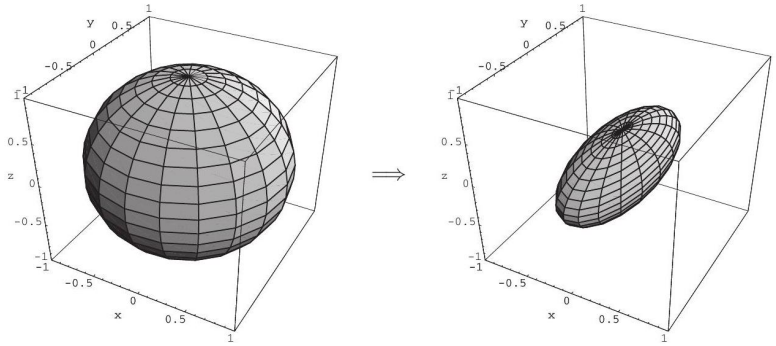


Figure 8.10. The effect of the bit-phase flip channel on the Bloch sphere, for $p = 0.3$. Note that the states on the $\hat{y}$ axis are left alone, while the $\hat{x} - \hat{z}$ plane is uniformly contracted by a factor of $1 - 2p$.}

Exercise 8.15: Suppose a projective measurement is performed on a single qubit in the basis $|+\rangle, |-\rangle$, where $|\pm\rangle \equiv (|0\rangle \pm |1\rangle)/\sqrt{2}$. In the event that we are ignorant of the result of the measurement, the density matrix evolves according to the equation

$$\rho \rightarrow \mathcal{E}(\rho) = |+\rangle\langle+|\rho|+\rangle\langle+| + |-\rangle\langle-|\rho|-\rangle\langle-|. \tag{8.99}$$

Illustrate this transformation on the Bloch sphere.

Exercise 8.16: The graphical method for understanding single qubit quantum operations was derived for trace-preserving quantum operations. Find an explicit example of a non-trace-preserving quantum operation which cannot be described as a deformation of the Bloch sphere, followed by a rotation and a displacement.

9.1.11 8.3.4 Depolarizing channel

The depolarizing channel is an important type of quantum noise. Imagine we take a single qubit, and with probability p that qubit is depolarized. That is, it is replaced by the completely

mixed state, $I/2$. With probability $1-p$ the qubit is left untouched. The state of the quantum system after this noise is

$$\mathcal{E}(\rho) = \frac{pI}{2} + (1-p)\rho. \tag{8.100}$$

The effect of the depolarizing channel on the Bloch sphere is illustrated in Figure 8.11.

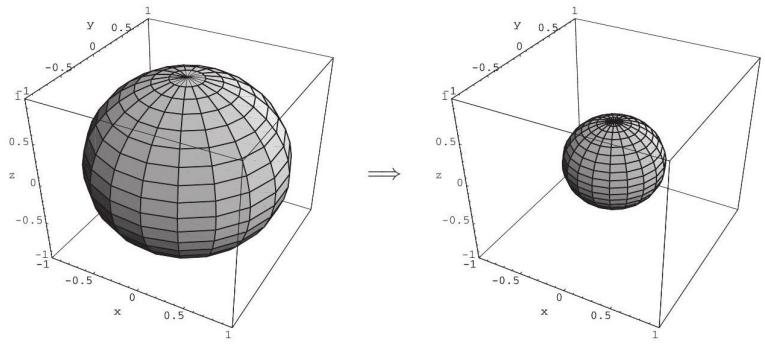


Figure 8.11. The effect of the depolarizing channel on the Bloch sphere, for $p = 0.5$. Note how the entire sphere contracts uniformly as a function of p.

A quantum circuit simulating the depolarizing channel is illustrated in Figure 8.12. The top line of the circuit is the input to the depolarizing channel, while the bottom two lines are an 'environment' to simulate the channel. We have used an environment with two mixed state inputs. The idea is that the third qubit, initially a mixture of the state $|0\rangle$ with probability $1-p$ and state $|1\rangle$ with probability p acts as a control for whether or not the completely mixed state $I/2$ stored in the second qubit is swapped into the first qubit.

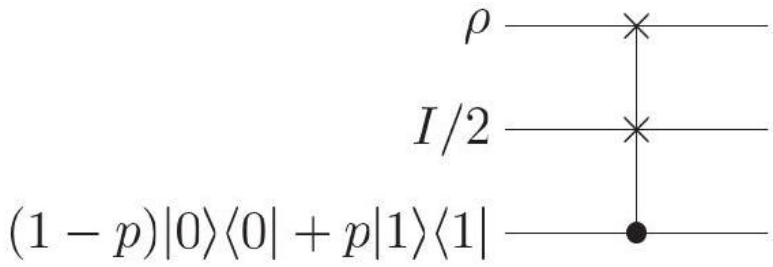


Figure 8.12. Circuit implementation of the depolarizing channel.

The form (8.100) is not in the operator-sum representation. However, if we observe that for arbitrary ρ,

$$\frac{I}{2} = \frac{\rho + X\rho X + Y\rho Y + Z\rho Z}{4} \tag{8.101}$$

and then substitute for $I/2$ into (8.100) we arrive at the equation

$$\mathcal{E}(\rho) = \left(1 - \frac{3p}{4}\right)\rho + \frac{p}{4}(X\rho X + Y\rho Y + Z\rho Z), \tag{8.102}$$

showing that the depolarizing channel has operation elements $\{\sqrt{1-3p/4}I, \sqrt{p}X/2, \sqrt{p}Y/2, \sqrt{p}Z/2\}$. Note, incidentally, that it is frequently convenient to parametrize the depolarizing channel in different ways, such as

$$\mathcal{E}(\rho) = (1-p)\rho + \frac{p}{3}(X\rho X + Y\rho Y + Z\rho Z), \tag{8.103}$$

which has the interpretation that the state ρ is left alone with probability $1-p$, and the operators X, Y and Z applied each with probability $p/3$.

Exercise 8.17: Verify (8.101) as follows. Define

$$\mathcal{E}(A) \equiv \frac{A + XAX + YAY + ZAZ}{4}, \tag{8.104}$$

and show that

$$\mathcal{E}(I) = I; \quad \mathcal{E}(X) = \mathcal{E}(Y) = \mathcal{E}(Z) = 0. \tag{8.105}$$

Now use the Bloch sphere representation for single qubit density matrices to verify (8.101).

The depolarizing channel can, of course, be generalized to quantum systems of dimension more than two. For a d-dimensional quantum system the depolarizing channel again replaces the quantum system with the completely mixed state I/d with probability p, and leaves the state untouched otherwise. The corresponding quantum operation is

$$\mathcal{E}(\rho) = \frac{pI}{d} + (1-p)\rho. \tag{8.106}$$

Exercise 8.18: For $k \geq 1$ show that $\mathrm{tr}\left(\rho^k\right)$ is never increased by the action of the depolarizing channel.

Exercise 8.19: Find an operator-sum representation for a generalized depolarizing channel acting on a d-dimensional Hilbert space.

9.1.12 8.3.5 Amplitude damping

An important application of quantum operations is the description of energy dissipation - effects due to loss of energy from a quantum system. What are the dynamics of an atom which is spontaneously emitting a photon? How does a spin system at high temperature approach equilibrium with its environment? What is the state of a photon in an interferometer or cavity when it is subject to scattering and attenuation?

Each of these processes has its own unique features, but the general behavior of all of them is well characterized by a quantum operation known as amplitude damping, which we can derive by considering the following scenario. Suppose we have a single optical mode containing the quantum state $a|0\rangle + b|1\rangle$, a superposition of zero or one photons. The scattering of a photon from this mode can be modeled by thinking of inserting a partially silvered mirror, a beamsplitter, in the path of the photon. As we saw in Section 7.4.2, this beamsplitter allows the photon to couple to another single optical mode (representing the environment), according to the unitary transformation $B = \exp\left[\theta\left(a^\dagger b - a b^\dagger\right)\right]$, where $a, a^\dagger$ and $b, b^\dagger$ are annihilation and creation operators for photons in the two modes. The output after the beamsplitter, assuming the environment starts out with no photons, is simply $B|0\rangle(a|0\rangle + b|1\rangle) = a|00\rangle + b(\cos\theta|01\rangle + \sin\theta|10\rangle)$, using Equation (7.34). Tracing over the environment gives us the quantum operation

$$\mathcal{E}_{\mathrm{AD}}(\rho) = E_0 \rho E_0^\dagger + E_1 \rho E_1^\dagger, \tag{8.107}$$

where $E_k = \langle k|B|0\rangle$ are

$$E_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix}$$
$$E_1 = \begin{bmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{bmatrix}, \tag{8.108}$$

the operation elements for amplitude damping. $\gamma = \sin^2\theta$ can be thought of as the probability of losing a photon.

Observe that no linear combination can be made of E_0 and E_1 to give an operation element proportional to the identity (though compare with Exercise 8.23). The E_1 operation changes a $|1\rangle$ state into a $|0\rangle$ state, corresponding to the physical process of losing a quantum of energy to the environment. E_0 leaves $|0\rangle$ unchanged, but reduces the amplitude of a $|1\rangle$ state; physically, this happens because a quantum of energy was not lost to the environment, and thus the environment now perceives it to be more likely that the system is in the $|0\rangle$ state, rather than the $|1\rangle$ state.

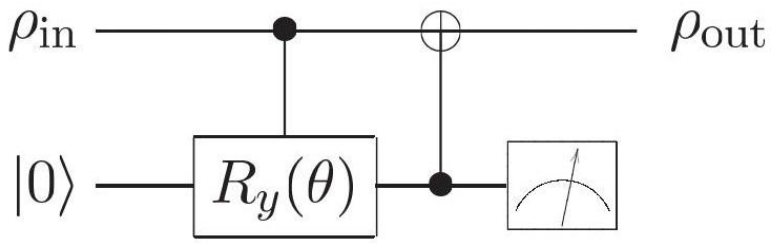


Figure 8.13. Circuit model for amplitude damping

Exercise 8.20: (Circuit model for amplitude damping) Show that the circuit in
Figure 8.13 models the amplitude damping quantum operation, with $\sin^2(\theta/2) = \gamma$.

Exercise 8.21: (Amplitude damping of a harmonic oscillator) Suppose that our principal system, a harmonic oscillator, interacts with an environment, modeled as another harmonic oscillator, through the Hamiltonian

$$H = \chi\left(a^\dagger b + b^\dagger a\right) \tag{8.109}$$

where a and b are the annihilation operators for the respective harmonic oscillators, as defined in Section 7.3.

(1) Using $U = \exp(-iH\Delta t)$, denoting the eigenstates of $b^\dagger b$ as $|k_b\rangle$, and selecting the vacuum state $|0_b\rangle$ as the initial state of the environment, show that the operation elements $E_k = \langle k_b| U |0_b\rangle$ are found to be

$$E_k = \sum_n \sqrt{\binom{n}{k}} \sqrt{(1-\gamma)^{n-k}\gamma^k}|n-k\rangle\langle n|, \tag{8.110}$$

where $\gamma = 1 - \cos^2(\chi\Delta t)$ is the probability of loosing a single quantum of energy, and states such as $|n\rangle$ are eigenstates of $a^\dagger a$.

(2) Show that the operation elements E_k define a trace-preserving quantum operation.

Exercise 8.22: (Amplitude damping of single qubit density matrix) For the general single qubit state

$$\rho = \begin{bmatrix} a & b \\ b^* & c \end{bmatrix} \tag{8.111}$$

show that amplitude damping leads to

$$\mathcal{E}_{\rm AD}(\rho) = \left[\begin{array}{cc} 1-(1-\gamma)(1-a) & b\sqrt{1-\gamma} \\ b^*\sqrt{1-\gamma} & c(1-\gamma) \end{array} \right]. \tag{8.112}$$

Exercise 8.23: (Amplitude damping of dual-rail qubits) Suppose that a single qubit state is represented by using two qubits, as

$$|\psi\rangle = a|01\rangle + b|10\rangle. \tag{8.113}$$

Show that $\mathcal{E}_{\rm AD} \otimes \mathcal{E}_{\rm AD}$ applied to this state gives a process which can be described by the operation elements

$$E_0^{\rm dr} = \sqrt{1-\gamma} I \tag{8.114}$$

$$E_1^{\rm dr} = \sqrt{\gamma}[|00\rangle\langle 01| + |00\rangle\langle 10|] \tag{8.115}$$

that is, either nothing ($E_0^{\rm dr}$) happens to the qubit, or the qubit is transformed ($E_1^{\rm dr}$) into the state $|00\rangle$, which is orthogonal to $|\psi\rangle$. This is a simple error-detection code, and is also the basis for the robustness of the 'dual-rail' qubit discussed in Section 7.4.

Exercise 8.24: (Spontaneous emission is amplitude damping) A single atom coupled to a single mode of electromagnetic radiation undergoes spontaneous emission, as was described in Section 7.6.1. To see that this process is just
amplitude damping, take the unitary operation resulting from the Jaynes-Cummings interaction, Equation (7.77), with detuning $\delta = 0$, and give the quantum operation resulting from tracing over the field.

A general characteristic of a quantum operation is the set of states that are left invariant under the operation. For example, we have seen how the phase flip channel leaves the $\hat{z}$ axis of the Bloch sphere unchanged; this corresponds to states of the form $p|0\rangle\langle 0| + (1-p)|1\rangle\langle 1|$ for arbitrary probability p. In the case of amplitude damping, only the ground state $|0\rangle$ is left invariant. That is a natural consequence of our modeling the environment as starting in the $|0\rangle$ state, as if it were at zero temperature.

What quantum operation describes the effect of dissipation to an environment at finite temperature? This process, $\mathcal{E}_{\rm GAD}$, called generalized amplitude damping, is defined for single qubits by the operation elements

$$E_0 = \sqrt{p} \left[\begin{array}{cc} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{array} \right] \tag{8.116}$$

$$E_1 = \sqrt{p} \left[\begin{array}{cc} 0 & \sqrt{\gamma} \\ 0 & 0 \end{array} \right] \tag{8.117}$$

$$E_2 = \sqrt{1-p} \left[\begin{array}{cc} \sqrt{1-\gamma} & 0 \\ 0 & 1 \end{array} \right] \tag{8.118}$$

$$E_3 = \sqrt{1-p} \left[\begin{array}{cc} 0 & 0 \\ \sqrt{\gamma} & 0 \end{array} \right] \tag{8.119}$$

where the stationary state

$$\rho_\infty = \left[\begin{array}{cc} p & 0 \\ 0 & 1-p \end{array} \right] \tag{8.120}$$

satisfies $\mathcal{E}_{\rm GAD}(\rho_\infty) = \rho_\infty$. Generalized amplitude damping describes the ' T_1 ' relaxation processes due to coupling of spins to their surrounding lattice, a large system which is in thermal

equilibrium at a temperature often much higher than the spin temperature. This is the case relevant to NMR quantum computation, where some of the properties of $\mathcal{E}_{\rm GAD}$ described in Box 8.3 become important.

Exercise 8.25: If we define the temperature T of a qubit by assuming that in equilibrium the probabilities of being in the $|0\rangle$ and $|1\rangle$ states satisfy a Boltzmann distribution, that is $p_0 = e^{-E_0/k_{\rm B}T}/\mathcal{Z}$ and $p_1 = e^{-E_1/k_{\rm B}T}/\mathcal{Z}$, where E_0 is the energy of the state $|0\rangle, E_1$ the energy of the state $|1\rangle$, and $\mathcal{Z} = e^{-E_0/k_{\rm B}T} + e^{-E_1/k_{\rm B}T}$, what temperature describes the state ρ_∞ ?

We can visualize the effect of amplitude damping in the Bloch representation as the Bloch vector transformation

$$(r_x, r_y, r_z) \rightarrow \left(r_x\sqrt{1-\gamma}, r_y\sqrt{1-\gamma}, \gamma + r_z(1-\gamma)\right) \tag{8.122}$$

When γ is replaced with a time-varying function like $1 - e^{-t/T_1}$ (t is time, and T_1 just some constant characterizing the speed of the process), as is often the case for real physical processes, we can visualize the effects of amplitude damping as a flow on the Bloch sphere, which moves every point in the unit ball towards a fixed point at the north pole, where $|0\rangle$ is located. This is shown in Figure 8.14.

Box 8.3: Generalized amplitude damping and effective pure states

The notion of 'effective pure states' introduced in Section 7.7 was found to be useful in NMR implementations of quantum computers. These states behave like pure states under unitary evolution and measurement of traceless observables. How do they behave under quantum operations? In general, non-unitary quantum operations ruin the effectiveness of these states, but surprisingly, they can behave properly under generalized amplitude damping.
Consider a single qubit effective pure state $\rho = (1-p)I + (2p-1)|0\rangle\langle 0|$. Clearly, traceless measurement observables acting on $U\rho U^\dagger$ produce results which are proportional to those on the pure state $U|0\rangle\langle 0|U^\dagger$. Suppose ρ is the stationary state of $\mathcal{E}_{\rm GAD}$. Interestingly, in this case,

$$\mathcal{E}_{\rm GAD}\left(U\rho U^\dagger\right) = (1-p)I + (2p-1)\mathcal{E}_{\rm AD}\left(U\rho U^\dagger\right). \tag{8.121}$$

That is, under generalized amplitude damping, an effective pure state can remain such, and moreover, the 'pure' component of ρ behaves as if it were undergoing amplitude damping to a reservoir at zero temperature!

Similarly, generalized amplitude damping performs the transformation

$$(r_x, r_y, r_z) \rightarrow \left(r_x\sqrt{1-\gamma}, r_y\sqrt{1-\gamma}, \gamma(2p-1) + r_z(1-\gamma)\right). \tag{8.123}$$

Comparing (8.122) and (8.123), it is clear that amplitude damping and generalized amplitude damping differ only in the location of the fixed point of the flow; the final state is along the $\hat{z}$ axis, at the point ($2p-1$), which is a mixed state.

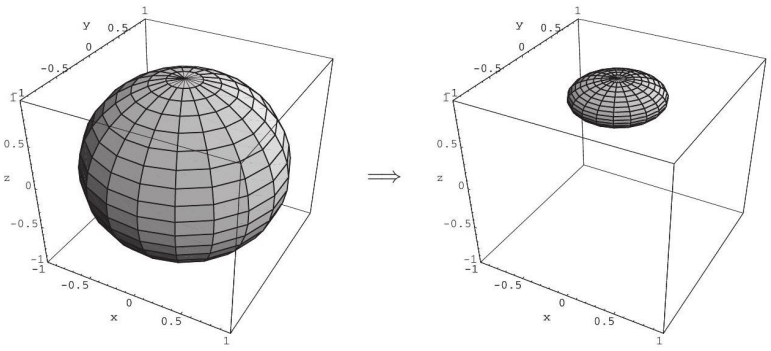


Figure 8.14. The effect of the amplitude damping channel on the Bloch sphere, for $p = 0.8$. Note how the entire sphere shrinks towards the north pole, the $|0\rangle$ state.

9.1.13 8.3.6 Phase damping

A noise process that is uniquely quantum mechanical, which describes the loss of quantum information without loss of energy, is phase damping. Physically it describes, for example, what happens when a photon scatters randomly as it travels through a waveguide, or how electronic states in an atom are perturbed upon interacting with distant electrical charges. The energy eigenstates of a quantum system do not change as a function of time, but do accumulate a phase which is proportional to the eigenvalue. When a system evolves for an amount of time which is not precisely known, partial information about this quantum phase - the relative phases between the energy eigenstates - is lost.

A very simple model for this kind of quantum noise is the following. Suppose that we have a qubit $|\psi\rangle = a|0\rangle + b|1\rangle$ upon which the rotation operation $R_z(\theta)$ is applied, where the angle of rotation θ is random. The randomness could originate, for example, from a deterministic interaction with an environment, which never again interacts with the system and thus is implicitly measured (see Section 4.4). We shall call this random R_z operation a phase kick. Let us assume that the phase kick angle θ is well represented as a random variable which has a Gaussian distribution with mean 0 and variance 2λ.

The output state from this process is given by the density matrix obtained from averaging over θ,

$$\rho = \frac{1}{\sqrt{4\pi\lambda}} \int_{-\infty}^{\infty} R_z(\theta)|\psi\rangle\langle\psi|R_z^\dagger(\theta) e^{-\theta^2/4\lambda} d\theta \tag{8.124}$$

$$= \begin{bmatrix} |a|^2 & ab^* e^{-\lambda} \\ a^* b e^{-\lambda} & |b|^2 \end{bmatrix} \tag{8.125}$$

The random phase kicking causes the expected value of the off-diagonal elements of the density matrix to decay exponentially to zero with time. That is a characteristic result of phase damping.

Another way to derive the phase damping quantum operation is to consider an interaction between two harmonic oscillators, in a manner similar to how amplitude damping was derived in the last section, but this time with the interaction Hamiltonian

$$H = \chi a^\dagger a \left(b + b^\dagger\right) \tag{8.126}$$

Letting $U = \exp(-iH\Delta t)$, considering only the $|0\rangle$ and $|1\rangle$ states of the a oscillator as our system, and taking the environment oscillator to initially be $|0\rangle$, we find that tracing over the environment gives the operation elements $E_k = \langle k_b| U |0_b\rangle$, which are

$$E_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\lambda} \end{bmatrix} \tag{8.127}$$

$$E_1 = \begin{bmatrix} 0 & 0 \\ 0 & \sqrt{\lambda} \end{bmatrix}, \tag{8.128}$$

where $\lambda = 1 - \cos^2(\chi \Delta t)$ can be interpreted as the probability that a photon from the system has been scattered (without loss of energy). As was the case for amplitude damping, E_0 leaves $|0\rangle$ unchanged, but reduces the amplitude of a $|1\rangle$ state; unlike amplitude damping, however, the E_1 operation destroys $|0\rangle$ and reduces the amplitude of the $|1\rangle$ state, and does not change it into a $|0\rangle$.

By applying Theorem 8.2, the unitary freedom of quantum operations, we find that a unitary recombination of E_0 and E_1 gives a new set of operation elements for phase damping,

$$\tilde{E}_0 = \sqrt{\alpha} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{8.129}$$

$$\tilde{E}_1 = \sqrt{1-\alpha} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \tag{8.130}$$

where $\alpha = (1+\sqrt{1-\lambda})/2$. Thus the phase damping quantum operation is exactly the same as the phase flip channel which we encountered in Section 8.3.3!

Since phase damping is the same as the phase flip channel, we have already seen how it is visualized on the Bloch sphere, in Figure 8.9. This corresponds to the Bloch vector transformation

$$(r_x, r_y, r_z) \rightarrow \left(r_x \sqrt{1-\lambda}, r_y \sqrt{1-\lambda}, r_z \right) \tag{8.131}$$

which has the effect of shrinking the sphere into ellipsoids. Phase damping is often referred to as a ' T_2 ' (or 'spin-spin') relaxation process, for historical reasons, where $e^{-t/2T_2} = \sqrt{1-\lambda}$. As a function of time, the amount of damping increases, corresponding to an inwards flow of all points in the unit ball towards the $\hat{z}$ axis. Note that states along the $\hat{z}$ axis remain invariant.

Historically, phase damping was a process that was almost always thought of, physically, as resulting from a random phase kick or scattering process. It was not until the connection to the phase flip channel was discovered that quantum error-correction was developed, since it was thought that phase errors were continuous and couldn't be described as a discrete process! In fact, single qubit phase errors can always be thought of as resulting from a process in which either nothing happens to a qubit, with probability α, or with probability $1-\alpha$, the qubit is flipped by the Z Pauli operation. Although this might not be the actual microscopic physical process happening, from the standpoint of the transformation occurring to a qubit over a discrete time interval large compared to the underlying random process, there is no difference at all.

Phase damping is one of the most subtle and important processes in the study of quantum computation and quantum information. It has been the subject of an immense amount of study and speculation, particularly with regard to why the world around us appears to be so classical, with superposition states not a part of our everyday experience! Perhaps it is phase damping that is responsible for this absence of superposition states from the everyday (Exercise 8.31)? The pioneering quantum physicist Schrödinger was perhaps the first to pose this problem, and he did this in a particularly stark form, as discussed in Box 8.4.

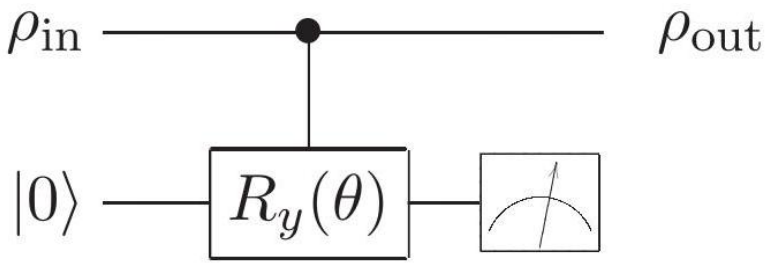


Figure 8.15. Circuit model for phase damping. The upper wire carries the input qubit with an unknown state, and the lower wire is an ancilla qubit used to model the environment.

Exercise 8.26: (Circuit model for phase damping) Show that the circuit in Figure 8.15 can be used to model the phase damping quantum operation, provided θ is chosen appropriately.

Exercise 8.27: (Phase damping = phase flip channel) Give the unitary transformation which relates the operation elements of (8.127)-(8.128) to those of (8.129)-(8.130); that is, find u such that $\tilde{E}_k = \sum_j u_{kj} E_j$.

Exercise 8.28: (One CNOT phase damping model circuit) Show that a single controlled-NOT gate can be used as a model for phase damping, if we let the initial state of the environment be a mixed state, where the amount of damping is determined by the probability of the states in the mixture.

Exercise 8.29: (Unitality) A quantum process $\mathcal{E}$ is unital if $\mathcal{E}(I) = I$. Show that the depolarizing and phase damping channels are unital, while amplitude damping is not.

Exercise 8.30: ($T_2 \leq T_1/2$) The T_2 phase coherence relaxation rate is just the exponential decay rate of the off-diagonal elements in the qubit density matrix, while T_1 is the decay rate of the diagonal elements (see Equation (7.144)). Amplitude damping has both nonzero T_1 and T_2 rates; show that for amplitude damping $T_2 = T_1/2$. Also show that if amplitude and phase damping are both applied then $T_2 \leq T_1/2$.

Exercise 8.31: (Exponential sensitivity to phase damping) Using (8.126), show that the element $\rho_{nm} = \langle n|\rho|m\rangle$ in the density matrix of a harmonic oscillator decays exponentially as $e^{-\lambda(n-m)^2}$ under the effect of phase damping, for some constant λ.

9.1.14 8.4 Applications of quantum operations

As befits a powerful tool, the quantum operations formalism has numerous applications. In this section we describe two of these applications. Section 8.4.1 describes the theory of master equations, a picture of quantum noise complementary to the quantum operations formalism. The master equation approach describes quantum noise in continuous time using differential equations, and is the approach to quantum noise most often used by physicists. In Section 8.4.2 we describe quantum process tomography, a procedure to experimentally determine the dynamics of a quantum system.

9.1.15 8.4.1 Master equations

Open quantum systems occur in a wide range of disciplines, and many tools other than quantum operations can be employed in their study. In this section, we briefly describe one such tool, the approach of master equations.

The dynamics of open quantum systems have been studied extensively in the field of quantum optics. The main objective in this context is to describe the time evolution of an open system with a differential equation which properly describes non-unitary behavior. This descrip-

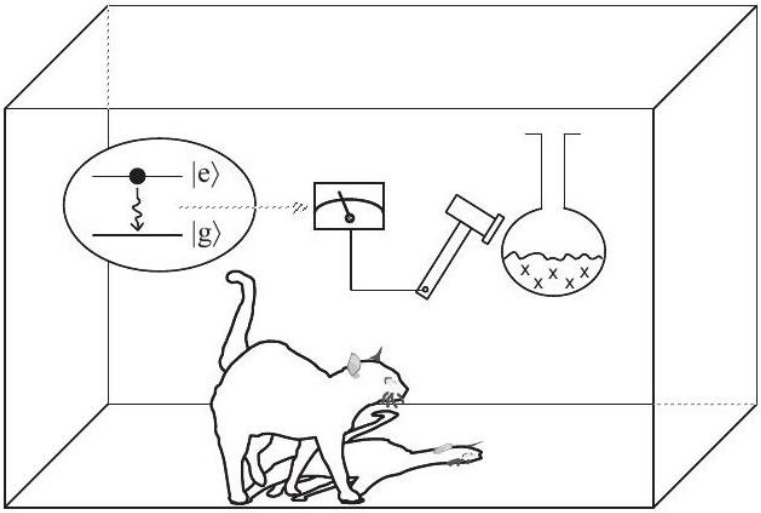
tion is provided by the master equation, which can be written most generally in the Lindblad form as

$$\frac{d\rho}{dt} = -\frac{i}{\hbar}[H,\rho] + \sum_j \left[2L_j\rho L_j^\dagger - \left\{L_j^\dagger L_j, \rho\right\}\right] \tag{8.134}$$

where $\{x, y\} = xy + yx$ denotes an anticommutator, H is the system Hamiltonian, a Hermitian operator representing the coherent part of the dynamics, and L_j are the Lindblad

Box 8.4: Schrödinger's cat

When I hear about Schrödinger's cat, I reach for my gun. - Stephen Hawking Schrödinger's infamous cat faces life or death contingent upon an automatic device which breaks a vial of poison and kills the cat if an excited atomic state is observed to decay, as illustrated here:



Schrödinger asked what happens when the atom is in a superposition state? Is the cat alive or dead? Why do superposition states such as this apparently not occur in the everyday world? This conundrum is resolved by realizing that it is very unlikely to occur in real life, because of extreme sensitivity of macroscopic superposition states to decoherence. Let the atom represent a single qubit. The joint system has the initial state $\mid \text{alive} \rangle|1\rangle$. Suppose that after one half-life of the atom, the state is the equal superposition $\mid \text{alive} \rangle(|0\rangle + |1\rangle)/\sqrt{2}$ (this represents a simplification of the actual physics, which are too involved to go into here). The apparatus kills the cat if the atom is in the $|0\rangle$ state; otherwise, the cat lives. This gives the state $|\psi\rangle = [\mid \text{dead} \rangle|0\rangle + \mid \text{alive} \rangle|1\rangle]/\sqrt{2}$, in which the cat's state has become entangled with that of the atom. This would seem to indicate the cat is simultaneously alive and dead, but suppose we consider the density matrix of this state,

$$\rho = |\psi\rangle\langle\psi| \tag{8.132}$$

$$= \frac{1}{2}[\mid \text{alive}, 1\rangle\langle \text{alive}, 1\mid + \mid \text{dead}, 0\Big\rangle \langle \text{dead}, 0\mid + \mid \text{alive}, 1\rangle\langle \text{dead}, 0\mid + \mid \text{dead}, 0\rangle\langle \text{alive}, 1\mid]. \tag{8.133}$$

Now, in practice it is impossible to perfectly isolate the cat and the atom in their box, and thus information about this superposition state will leak into the external world. For example, heat from the cat's body could permeate the wall and give some indication of its state to the outside. Such effects may be modeled as phase damping, which exponentially damps out the final two (off-diagonal) terms in ρ. To a first approximation, we may model the cat-atom system as a simple harmonic oscillator. An important result about the decoherence of such a

system is that coherence between states of high energy difference decays faster than between states with a lower energy difference (Exercise 8.31). Thus ρ will quickly be transformed into a nearly diagonal state, which represents an ensemble of cat-atom states which correspond to either dead or alive, and are not in a superposition of the two states.
operators, representing the coupling of the system to its environment. The differential equation takes on the above form in order that the process be completely positive in a sense similar to that described earlier for quantum operations. It is also generally assumed that the system and environment begin in a product state. Furthermore, in order to derive a master equation for a process, one usually begins with a system-environment model Hamiltonian, and then makes the Born and Markov approximations in order to determine L_j. Note that in the master equation approach, $\mathrm{tr}[\rho(t)] = 1$ at all times.

As an example of a Lindblad equation, consider a two-level atom coupled to the vacuum, undergoing spontaneous emission. The coherent part of the atom's evolution is described by the Hamiltonian $H = -\hbar\omega\sigma_z/2$. $\hbar\omega$ is the energy difference of the atomic levels. Spontaneous emission causes an atom in the excited ($|1\rangle$) state to drop down into the ground ($|0\rangle$) state, emitting a photon in the process. This emission is described by the Lindblad operator $\sqrt{\gamma}\sigma_-$, where $\sigma_- \equiv |0\rangle\langle 1|$ is the atomic lowering operator, and γ is the rate of spontaneous emission. The master equation describing this process is

$$\frac{d\rho}{dt} = -\frac{i}{\hbar}[H, \rho] + \gamma\left[2\sigma_-\rho\sigma_+ - \sigma_+\sigma_-\rho - \rho\sigma_+\sigma_-\right] \tag{8.135}$$

where $\sigma_+ \equiv \sigma_-^\dagger$ is the atomic raising operator.
To solve the equation it is helpful to move to the interaction picture, that is, make the change of variables

$$\tilde{\rho}(t) \equiv e^{iHt}\rho(t)e^{-iHt} \tag{8.136}$$

The equation of motion for $\tilde{\rho}$ is easily found to be

$$\frac{d\tilde{\rho}}{dt} = \gamma\left[2\tilde{\sigma}_-\tilde{\rho}\tilde{\sigma}_+ - \tilde{\sigma}_+\tilde{\sigma}_-\tilde{\rho} - \tilde{\rho}\tilde{\sigma}_+\tilde{\sigma}_-\right] \tag{8.137}$$

where

$$\tilde{\sigma}_- \equiv e^{iHt}\sigma_- e^{-iHt} = e^{-i\omega t}\sigma_- \tag{8.138}$$

$$\tilde{\sigma}_+ \equiv e^{iHt}\sigma_+ e^{-iHt} = e^{i\omega t}\sigma_+. \tag{8.139}$$

Our final equation of motion is thus

$$\frac{d\tilde{\rho}}{dt} = \gamma\left[2\sigma_-\tilde{\rho}\sigma_+ - \sigma_+\sigma_-\tilde{\rho} - \tilde{\rho}\sigma_+\sigma_-\right] \tag{8.140}$$

This equation of motion is easily solved using a Bloch vector representation for $\tilde{\rho}$. The solution is

$$\lambda_x = \lambda_x(0)e^{-\gamma t} \tag{8.141}$$

$$\lambda_y = \lambda_y(0)e^{-\gamma t} \tag{8.142}$$

$$\lambda_z = \lambda_z(0)e^{-2\gamma t} + 1 - e^{-2\gamma t} \tag{8.143}$$

Defining $\gamma' = 1 - \exp(-2t\gamma)$ we can easily check that this evolution is equivalent to

$$\tilde{\rho}(t) = \mathcal{E}(\tilde{\rho}(0)) \equiv E_0\tilde{\rho}(0)E_0^\dagger + E_1\tilde{\rho}(0)E_1^\dagger, \tag{8.144}$$

where

$$E_0 \equiv \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma'} \end{bmatrix} \tag{8.145}$$

$$E_1 \equiv \begin{bmatrix} 0 & \sqrt{\gamma'} \\ 0 & 0 \end{bmatrix} \tag{8.146}$$

are the operation elements defining the quantum operation $\mathcal{E}$. Note that the effect of $\mathcal{E}$ is amplitude damping; compare with Equation (8.108). The example we have considered is an instance of the spin-boson model, in which a small, finite dimensional quantum system interacts with a bath of simple harmonic oscillators. Physically, it is important in describing the interaction of atoms with electromagnetic radiation, as in cavity QED, or atom and ion traps.

The master equation approach is less general than the quantum operations formalism. Solving a master equation allows one to determine the time dependence of a density matrix. Knowing this, in turn, means that the result can be expressed as a quantum operation in the operator-sum representation,

$$\rho(t) = \sum_k E_k(t)\rho(0)E_k^\dagger(t), \tag{8.147}$$

where $E_k(t)$ are time dependent operation elements, determined from the solution to the master equation. However, a quantum process described in terms of an operator-sum representation cannot necessarily be written down as a master equation. For example, quantum operations can describe non-Markovian dynamics, simply because they describe only state changes, not continuous time evolution. Nevertheless, each approach has its own place. In fact, even quantum operations do not provide the most general description; we consider in Section 8.5 some processes which are not described by quantum operations.

9.1.16 8.4.2 Quantum process tomography

Quantum operations provide a wonderful mathematical model for open quantum systems, and are conveniently visualized (at least for qubits) - but how do they relate to experimentally measurable quantities? What measurements should an experimentalist do if they wish to characterize the dynamics of a quantum system? For classical systems, this elementary task is known as system identification. Here, we show how its analogue, known as quantum process tomography, can be performed for finite dimensional quantum systems.

To understand process tomography we first need to understand another procedure called quantum state tomography. State tomography is the procedure of experimentally determining an unknown quantum state. Suppose we are given an unknown state, ρ, of a single qubit. How can we experimentally determine what the state of ρ is?

If we are given just a single copy of ρ then it turns out to be impossible to characterize ρ. The basic problem is that there is no quantum measurement which can distinguish non-orthogonal quantum states like $|0\rangle$ and $(|0\rangle + |1\rangle)/\sqrt{2}$ with certainty. However, it is possible to estimate ρ if we have a large number of copies of ρ. For instance, if ρ is the quantum state produced by some experiment, then we simply repeat the experiment many times to produce many copies of the state ρ.

Suppose we have many copies of a single qubit density matrix, ρ. The set $I/\sqrt{2}$, $X/\sqrt{2}, Y/\sqrt{2}, Z/\sqrt{2}$ forms an orthonormal set of matrices with respect to the HilbertSchmidt inner product, so ρ may be expanded as

$$\rho = \frac{\mathrm{tr}(\rho) I + \mathrm{tr}(X\rho) X + \mathrm{tr}(Y\rho) Y + \mathrm{tr}(Z\rho) Z}{2}. \tag{8.148}$$

Recall, however, that expressions like $\mathrm{tr}(A\rho)$ have an interpretation as the average value of observables. For example, to estimate $\mathrm{tr}(Z\rho)$ we measure the observable Z a large number of times, m, obtaining outcomes $z_1, z_2, \ldots, z_m$, all equal to $+1$ or -1 . The empirical average of these quantities, $\sum_i z_i/m$, is an estimate for the true value of $\mathrm{tr}(Z\rho)$. We can use the central limit theorem to determine how well this estimate behaves for large m, where it becomes approximately Gaussian with mean equal to $\mathrm{tr}(Z\rho)$ and with standard deviation $\Delta(Z)/\sqrt{m}$, where $\Delta(Z)$ is the standard deviation for a single measurement of Z, which is upper bounded by 1 , so the standard deviation in our estimate $\sum_i z_i/m$ is at most $1/\sqrt{m}$.

In a similar way we can estimate the quantities $\mathrm{tr}(X\rho)$ and $\mathrm{tr}(Y\rho)$ with a high degree of confidence in the limit of a large sample size, and thus obtain a good estimate for ρ. Generalizing this procedure to the case of more than one qubit is not difficult, at least in principle! Similar to the single qubit case, an arbitrary density matrix on n qubits can be expanded as

$$\rho = \sum_{\vec{v}} \frac{\mathrm{tr}\left(\sigma_{v_1} \otimes \sigma_{v_2} \otimes \cdots \otimes \sigma_{v_n} \rho\right) \sigma_{v_1} \otimes \sigma_{v_2} \otimes \cdots \otimes \sigma_{v_n}}{2^n}, \tag{8.149}$$

where the sum is over vectors $\vec{v} = (v_1, \ldots, v_n)$ with entries v_i chosen from the set $0, 1, 2, 3$. By performing measurements of observables which are products of Pauli matrices we can estimate each term in this sum, and thus obtain an estimate for ρ.

We've described how to do state tomography for systems comprised of qubits. What if non-qubit systems are involved? Not surprisingly, it is easy to generalize the above prescription to such systems. We won't explicitly do so here, but instead refer you to the end of chapter 'History and further reading' for references.

Now that we know how to do quantum state tomography, how can we use it to do quantum process tomography? The experimental procedure may be outlined as follows. Suppose the state space of the system has d dimensions; for example, $d = 2$ for a single qubit. We choose d^2 pure quantum states $|\psi_1\rangle, \ldots, |\psi_{d^2}\rangle$, chosen so that the corresponding density matrices $|\psi_1\rangle\langle\psi_1|, \ldots, |\psi_{d^2}\rangle\langle\psi_{d^2}|$ form a basis set for the space of matrices. We explain in more detail how to choose such a set below. For each state $|\psi_j\rangle$ we prepare the quantum system in that state and then subject it to the process which we wish to characterize. After the process has run to completion we use quantum state tomography to determine the state $\mathcal{E}(|\psi_j\rangle\langle\psi_j|)$ output from the process. From a purist's point of view we are now done, since in principle the quantum operation $\mathcal{E}$ is now determined by a linear extension of $\mathcal{E}$ to all states.

In practice, of course, we would like to have a way of determining a useful representation of $\mathcal{E}$ from experimentally available data. We will explain a general procedure for doing so, worked out explicitly for the case of a single qubit. Our goal is to determine a set of operation elements $\{E_i\}$ for $\mathcal{E}$,

$$\mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger \tag{8.150}$$

However, experimental results involve numbers, not operators, which are a theoretical concept. To determine the E_i from measurable parameters, it is convenient to consider an equivalent description of $\mathcal{E}$ using a fixed set of operators $\tilde{E}_i$, which form a basis for the set of operators on the state space, so that

$$E_i = \sum_m e_{im} \tilde{E}_m \tag{8.151}$$

for some set of complex numbers e_{im}. Equation (8.150) may thus be rewritten as

$$\mathcal{E}(\rho) = \sum_{mn} \tilde{E}_m \rho \tilde{E}_n^\dagger \chi_{mn} \tag{8.152}$$

where $\chi_{mn} \equiv \sum_i e_{im} e_{in}^*$ are the entries of a matrix which is positive Hermitian by definition. This expression, known as the chi matrix representation, shows that $\mathcal{E}$ can be completely described by a complex number matrix, χ, once the set of operators E_i has been fixed.

In general, χ will contain $d^4 - d^2$ independent real parameters, because a general linear map of d by d complex matrices to d by d matrices is described by d^4 independent parameters, but there are d^2 additional constraints due to the fact that ρ remains Hermitian with trace one; that is, the completeness relation

$$\sum_i E_i^\dagger E_i = I, \tag{8.153}$$

is satisfied, giving d^2 real constraints. We will show how to determine χ experimentally, and then show how an operator-sum representation of the form (8.150) can be recovered once the χ matrix is known.

Let $\rho_j, 1 \leq j \leq d^2$ be a fixed, linearly independent basis for the space of $d \times d$ matrices; that is, any $d \times d$ matrix can be written as a unique linear combination of the ρ_j. A convenient choice is the set of operators $|n\rangle\langle m|$. Experimentally, the output state $\mathcal{E}(|n\rangle\langle m|)$ may be obtained by preparing the input states $|n\rangle, |m\rangle, |+\rangle = (|n\rangle + |m\rangle)/\sqrt{2}$, and $|-\rangle = (|n\rangle + i|m\rangle)/\sqrt{2}$ and forming linear combinations of $\mathcal{E}(|n\rangle\langle n|), \mathcal{E}(|m\rangle\langle m|)$, $\mathcal{E}(|+\rangle\langle +|)$, and $\mathcal{E}(|-\rangle\langle -|)$, as follows:

$$\mathcal{E}(|n\rangle\langle m|) = \mathcal{E}(|+\rangle\langle +|) + i\mathcal{E}(|-\rangle\langle -|) - \frac{1+i}{2}\mathcal{E}(|n\rangle\langle n|) - \frac{1+i}{2}\mathcal{E}(|m\rangle\langle m|) \tag{8.154}$$

Thus, it is possible to determine $\mathcal{E}(\rho_j)$ by state tomography, for each ρ_j.
Furthermore, each $\mathcal{E}(\rho_j)$ may be expressed as a linear combination of the basis states,

$$\mathcal{E}(\rho_j) = \sum_k \lambda_{jk} \rho_k, \tag{8.155}$$

and since $\mathcal{E}(\rho_j)$ is known from the state tomography, λ_{jk} can be determined by standard linear algebraic algorithms. To proceed, we may write

$$\tilde{E}_m \rho_j \tilde{E}_n^\dagger = \sum_k \beta_{jk}^{mn} \rho_k, \tag{8.156}$$

where β_{jk}^{mn} are complex numbers which can be determined by standard algorithms from linear algebra given the $\tilde{E}_m$ operators and the ρ_j operators. Combining the last two expressions and (8.152) we have

$$\sum_k \sum_{mn} \chi_{mn} \beta_{jk}^{mn} \rho_k = \sum_k \lambda_{jk} \rho_k. \tag{8.157}$$

From the linear independence of the ρ_k it follows that for each k,

$$\sum_{mn} \beta_{jk}^{mn} \chi_{mn} = \lambda_{jk}. \tag{8.158}$$

This relation is a necessary and sufficient condition for the matrix χ to give the correct quantum operation $\mathcal{E}$. One may think of χ and λ as vectors, and β as a $d^4 \times d^4$ matrix with columns indexed by mn, and rows by jk. To show how χ may be obtained, let κ be the generalized inverse for the matrix β, satisfying the relation

$$\beta_{jk}^{mn} = \sum_{st,xy} \beta_{jk}^{st} \kappa_{st}^{xy} \beta_{xy}^{mn} \tag{8.159}$$

Most computer packages for matrix manipulation are capable of finding such generalized inverses. We now prove that χ defined by

$$\chi_{mn} \equiv \sum_{jk} \kappa_{jk}^{mn} \lambda_{jk} \tag{8.160}$$

satisfies the relation (8.158).
The difficulty in verifying that χ defined by (8.160) satisfies (8.158) is that, in general, χ is not uniquely determined by Equation (8.158). For convenience we rewrite these equations in matrix form as

$$\beta \vec{\chi} = \vec{\lambda} \tag{8.161}$$

$$\vec{\chi} \equiv \kappa \vec{\lambda} \tag{8.162}$$

From the construction that led to Equation (8.152) we know there exists at least one solution to Equation (8.161), which we shall call $\vec{\chi}'$. Thus $\vec{\lambda} = \beta \vec{\chi}'$. The generalized inverse satisfies $\beta\kappa\beta = \beta$. Premultiplying the definition of $\vec{\chi}$ by β gives

$$\beta \vec{\chi} = \beta\kappa\vec{\lambda} \tag{8.163}$$

$$= \beta\kappa\beta\vec{\chi}' \tag{8.164}$$

$$= \beta\vec{\chi}' \tag{8.165}$$

$$= \vec{\lambda} \tag{8.166}$$

Thus χ defined by (8.162) satisfies the Equation (8.161), as we wanted to show.
Having determined χ one immediately obtains the operator-sum representation for $\mathcal{E}$ in the following manner. Let the unitary matrix $U^\dagger$ diagonalize χ,

$$\chi_{mn} = \sum_{xy} U_{mx} d_x \delta_{xy} U_{ny}^* \tag{8.167}$$

From this it can easily be verified that

$$E_i = \sqrt{d_i} \sum_j U_{ji} E_j \tag{8.168}$$

are operation elements for $\mathcal{E}$. Our algorithm may thus be summarized as follows: λ is experimentally determined using state tomography, which in turn determines χ via the equation $\vec{\chi} = \kappa\lambda$, which gives us a complete description of $\mathcal{E}$, including a set of operation elements E_i.

In the case of a single qubit quantum process, only 12 parameters must be determined (Box 8.5). The dynamics of a two qubit quantum black box $\mathcal{E}_2$ pose an even greater challenge for our understanding. In this case there are 240 parameters which need to be determined in order to completely specify the quantum operation acting on the quantum system! Determining these would obviously be quite a considerable undertaking. However, as for the single qubit case, it is relatively straightforward to implement a numerical routine which will automate the calculation, provided experimental state tomography and state preparation procedures are available in the laboratory.

Box 8.5: Process tomography for a single qubit

The general method of process tomography can be simplified in the case of a one qubit operation to provide explicit formulas which may be useful in experimental contexts. This simplification is made possible by choosing the fixed operators $\tilde{E}_i$ to have commutation properties which conveniently allow the χ matrix to be determined by straightforward matrix multiplication. In the one qubit case, we use:

$$E_0 = I \tag{8.169}$$
$$\tilde{E}_1 = X \tag{8.170}$$
$$\tilde{E}_2 = -iY \tag{8.171}$$
$$\tilde{E}_3 = Z. \tag{8.172}$$

There are 12 parameters, specified by χ, which determine an arbitrary single qubit quantum operation $\mathcal{E}$.
These parameters may be measured using four sets of experiments. As a specific example, suppose the input states $|0\rangle, |1\rangle, |+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|-\rangle = (|0\rangle + i|1\rangle)/\sqrt{2}$ are prepared, and the four matrices

$$\rho'_1 = \mathcal{E}(|0\rangle\langle 0|) \tag{8.173}$$
$$\rho'_4 = \mathcal{E}(|1\rangle\langle 1|) \tag{8.174}$$
$$\rho'_2 = \mathcal{E}(|+\rangle\langle +|) - i\mathcal{E}(|-\rangle\langle -|) - (1-i)\left(\rho'_1 + \rho'_4\right)/2 \tag{8.175}$$
$$\rho'_3 = \mathcal{E}(|+\rangle\langle +|) + i\mathcal{E}(|-\rangle\langle -|) - (1+i)\left(\rho'_1 + \rho'_4\right)/2 \tag{8.176}$$

are determined using state tomography. These correspond to $\rho'_j = \mathcal{E}(\rho_j)$, where

$$\rho_1 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \tag{8.177}$$

$\rho_2 = \rho_1 X, \rho_3 = X\rho_1$, and $\rho_4 = X\rho_1 X$. From (8.156) and Equations (8.169)-(8.172) we may determine β, and similarly ρ'_j determines λ. However, due to the particular choice of basis, and the Pauli matrix representation of $\tilde{E}_i$, we may express the β matrix as the Kronecker product $\beta = \Lambda \otimes \Lambda$, where

$$\Lambda = \frac{1}{2}\begin{bmatrix} I & X \\ X & -I \end{bmatrix}, \tag{8.178}$$

so that χ may be expressed conveniently as

$$\chi = \Lambda \begin{bmatrix} \rho'_1 & \rho'_2 \\ \rho'_3 & \rho'_4 \end{bmatrix} \Lambda, \tag{8.179}$$

in terms of block matrices.

We have shown how a useful representation for the dynamics of a quantum system may be experimentally determined using a systematic procedure. This procedure of quantum process tomography is analogous to the system identification step performed in classical control theory, and plays a similar role in understanding and controlling noisy quantum systems.

Exercise 8.32: Explain how to extend quantum process tomography to the case of non-trace-preserving quantum operations, such as arise in the study of measurement.

Exercise 8.33: (Specifying a quantum process) Suppose that one wished to completely specify an arbitrary single qubit operation $\mathcal{E}$ by describing how a set of points on the Bloch sphere $\{\vec{r}_k\}$ transform under $\mathcal{E}$. Prove that the set must contain at least four points.

Exercise 8.34: (Process tomography for two qubits) Show that the χ_2 describing the black box operations on two qubits can be expressed as

$$\chi_2 = \Lambda_2 \bar{\rho}' \Lambda_2 \tag{8.180}$$

where $\Lambda_2 = \Lambda \otimes \Lambda, \Lambda$ is as defined in Box 8.5, and $\bar{\rho}'$ is a block matrix of 16 measured density matrices,

$$\bar{\rho}' = P^T \begin{bmatrix} \rho'_{11} & \rho'_{12} & \rho'_{13} & \rho'_{14} \\ \rho'_{21} & \rho'_{22} & \rho'_{23} & \rho'_{24} \\ \rho'_{31} & \rho'_{32} & \rho'_{33} & \rho'_{34} \\ \rho'_{41} & \rho'_{42} & \rho'_{43} & \rho'_{44} \end{bmatrix} P \tag{8.181}$$

where $\rho'_{nm} = \mathcal{E}(\rho_{nm}), \rho_{nm} = T_n|00\rangle\langle 00|T_m, T_1 = I \otimes I, T_2 = I \otimes X, T_3 = X \otimes I, T_4 = X \otimes X$, and $P = I \otimes [(\rho_{00} + \rho_{12} + \rho_{21} + \rho_{33}) \otimes I]$ is a permutation matrix.

Exercise 8.35: (Process tomography example) Consider a one qubit black box of unknown dynamics $\mathcal{E}_1$. Suppose that the following four density matrices are obtained from experimental measurements, performed according to Equations (8.173)-(8.176):

$$\rho'_1 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \tag{8.182}$$

$$\rho'_2 = \begin{bmatrix} 0 & \sqrt{1-\gamma} \\ 0 & 0 \end{bmatrix} \tag{8.183}$$

$$\rho'_3 = \begin{bmatrix} 0 & 0 \\ \sqrt{1-\gamma} & 0 \end{bmatrix} \tag{8.184}$$

$$\rho'_4 = \begin{bmatrix} \gamma & 0 \\ 0 & 1-\gamma \end{bmatrix}, \tag{8.185}$$

where γ is a numerical parameter. From an independent study of each of these input-output relations, one could make several important observations: the ground state $|0\rangle$ is left invariant by $\mathcal{E}_1$, the excited state $|1\rangle$ partially decays to the ground state, and superposition states are damped. Determine the χ matrix for this process.

9.1.17 8.5 Limitations of the quantum operations formalism

Are there interesting quantum systems whose dynamics are not described by quantum operations? In this section we will construct an artificial example of a system whose evolution is not described by a quantum operation, and try to understand the circumstances under which this is likely to occur.

Suppose a single qubit is prepared in some unknown quantum state, which we denote ρ. The preparation of this qubit involves certain procedures to be carried out in the laboratory in which the qubit is prepared. Suppose that among the laboratory degrees of freedom is a single qubit which, as a side effect of the state preparation procedure, is left in the state $|0\rangle$ if ρ is a state on the bottom half of the Bloch sphere, and is left in the state $|1\rangle$ if ρ is a state on the top half of the Bloch sphere. That is, the state of the system after preparation is

$$\rho \otimes |0\rangle\langle 0| \otimes \text{ other degrees of freedom} \tag{8.186}$$

if ρ is a state on the bottom half of the Bloch sphere, and

$$\rho \otimes |1\rangle\langle 1| \otimes \text{ other degrees of freedom} \tag{8.187}$$

if ρ is a state on the top half of the Bloch sphere.
Once the state preparation is done, the system begins to interact with the environment, in this case all the laboratory degrees of freedom. Suppose the interaction is such that a controlled-NOT is performed between the principal system and the extra qubit in the laboratory system. Thus, if the system's Bloch vector was initially in the bottom half of the Bloch sphere it is left invariant by the process, while if it was initially in the top half of the Bloch sphere it is rotated into the bottom half of the Bloch sphere.

Obviously, this process is not an affine map acting on the Bloch sphere, and therefore, by the results of Section 8.3.2, it cannot be a quantum operation. The lesson to be learned from this discussion is that a quantum system which interacts with the degrees of freedom used to prepare that system after the preparation is complete will in general suffer a dynamics which is not adequately described within the quantum operations formalism. This is an important conclusion to have reached, as it indicates that there are physically reasonable circumstances under which the quantum operations formalism may not adequately describe the processes taking place in a quantum system. This should be kept in mind, for example, in applications of the quantum process tomography procedure discussed in the previous section.

For the remainder of this book we will, however, work within the quantum operations formalism. It provides a powerful, and reasonably general tool for describing the dynamics experienced by quantum systems. Most of all, it provides a means by which concrete progress can be made on problems related to quantum information processing. It is an interesting problem for further research to study quantum information processing beyond the quantum operations formalism.

Problem 8.1: (Lindblad form to quantum operation) In the notation of Section 8.4.1, explicitly work through the steps to solve the differential equation

$$\dot{\rho} = -\frac{\lambda}{2}\left(\sigma_+\sigma_-\rho + \rho\sigma_+\sigma_- - 2\sigma_-\rho\sigma_+\right) \tag{8.188}$$

for $\rho(t)$. Express the map $\rho(0) \rightarrow \rho(t)$ as $\rho(t) = \sum_k E_k(t)\rho(0)E_k^\dagger(t)$.
Problem 8.2: (Teleportation as a quantum operation) Suppose Alice is in possession of a single qubit, denoted as system 1, which she wishes to teleport to

Bob. Unfortunately, she and Bob only share an imperfectly entangled pair of qubits. Alice's half of this pair is denoted system 2, and Bob's half is denoted system 3. Suppose Alice performs a measurement described by a set of quantum operations $\mathcal{E}_m$ with result m on systems 1 and 2 . Show that this induces an operation $\tilde{\mathcal{E}}_m$ relating the initial state of system 1 to the final state of system 3, and that teleportation is accomplished if Bob can reverse this operation using a trace-preserving quantum operation $\mathcal{R}_m$, to obtain

$$\mathcal{R}_m\left(\frac{\tilde{\mathcal{E}}_m(\rho)}{\text{tr}\left[\tilde{\mathcal{E}}_m(\rho)\right]}\right) = \rho \tag{8.189}$$

where ρ is the initial state of system 1 .
Problem 8.3: (Random unitary channels) It is tempting to believe that all unital channels, that is, those for which $\mathcal{E}(I) = I$, result from averaging over random unitary operations, that is, $\mathcal{E}(\rho) = \sum_k p_k U_k \rho U_k^\dagger$, where U_k are unitary operators and the p_k form a probability distribution. Show that while this is true for single qubits, it is untrue for larger systems.

9.1.18 Summary of Chapter 8: Quantum noise and quantum operations

- The operator-sum representation: The behavior of an open quantum system can be modeled as

$$\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger, \tag{8.190}$$

where E_k are operation elements, satisfying $\sum_k E_k^\dagger E_k = I$ if the quantum operation is trace-preserving.

- Environmental models for quantum operations: A trace-preserving quantum operation can always be regarded as arising from the unitary interaction of a system with an initially uncorrelated environment, and vice versa. Non-tracepreserving quantum operations may be treated similarly, except an additional projective measurement is performed on the composite of system and environment, with the different outcomes corresponding to different non-trace-preserving quantum operations.

- Quantum process tomography: A quantum operation on a d-dimensional quantum system can be completely determined by experimentally measuring the output density matrices produced from d^2 pure state inputs.

- Operation elements for important single qubit quantum operations:

depolarizing channel	$\sqrt{1-\frac{3p}{4}}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $\sqrt{\frac{p}{4}}\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$,	$\sqrt{\frac{p}{4}}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $\sqrt{\frac{p}{4}}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
amplitude damping	$\begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix}$,	$\begin{bmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{bmatrix}$
phase damping	$\begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix}$,	$\begin{bmatrix} 0 & 0 \\ 0 & \sqrt{\gamma} \end{bmatrix}$
phase flip	$\sqrt{p}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$,	$\sqrt{1-p}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
bit flip	$\sqrt{p}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$,	$\sqrt{1-p}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
bit-phase flip	$\sqrt{p}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$,	$\sqrt{1-p}\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$

History and further reading

Quantum noise is an important topic in several fields, and there is an enormous literature on the subject. We will necessarily be restricted to citing only a small sample of the resources available on the topic. An early treatise on quantum noise from a rather mathematical perspective is due to Davies [Dav76]. Caldeira and Leggett [CL83] did some of the first and most complete studies of an important model known as the spin-boson model, using an approach based upon the Feynman path integral. Gardiner [Gar 91] studied quantum noise from the perspective of quantum optics. More recently, the quantum optics community has developed what is known as the quantum trajectories approach to quantum noise. Reviews of this

subject may be found in the articles by Zoller and Gardiner [ZG97] , and Plenio and Knight [PK98] .

A large literature exists on the subject of quantum operations. We mention just a few key references, primarily the book by Kraus [Kra8], which contains references to much earlier work on the subject. Influential early papers on the subject include those by Hellwig and Kraus [HK69,HK70], and by Choi [Cho75]. Lindblad [Lin76] connected the quantum operations formalism to the theory of continuous time quantum evolution, introducing what is now known as the Lindblad form. Schumacher [*Sch*96 b] and Caves [Cav99] have written excellent summaries of the quantum operations formalism from the point of view of quantum error-correction.

Quantum state tomography was suggested by Vogel and Risken [VR 89]. Leonhardt [Leo97] has written a recent review containing references to other work. The need for quantum process tomography was pointed out in a paper by Turchette, Hood, Lange, Mabuchi, and Kimble [THL+95]. The theory was developed independently by Chuang and Nielsen [CN97], and by Poyatos, Cirac and Zoller [PCZ97] . Jones [Jon94] had earlier sketched out the main ideas of quantum process tomography.

An unfortunate confusion of terms has arisen with the word 'decoherence'. Historically, it has been used to refer just to a phase damping process, particularly by Zurek[Zur91]. Zurek and other researchers recognized that phase damping has a unique role in the transition from quantum to classical physics; for certain environmental couplings, it occurs on a time scale which is much faster than any amplitude damping process, and can therefore be much more important in determining the loss of quantum coherence. The major point of these studies has been this emergence of classicality due to environmental interactions. However, by and large, the usage of decoherence in quantum computation and quantum information is to refer to any noise process in quantum processing. In this book, we prefer the more generic term 'quantum noise' and tend towards its usage, although occasionally decoherence finds a proper place in the context.

A more detailed discussion of some of the limitations of the quantum operations formalism (and in particular, the assumption of a system and environment initially in a product state) is provided by Royer [Roy 96].

Problem 8.2 is due to Nielsen and Caves [NC97]. Problem 8.3 is due to Landau and Streater [*LS*93] as part of an in-depth study of the extremal points of the convex set of doubly stochastic quantum operations.

9.2 9 Distance measures for quantum information

What does it mean to say that two items of information are similar? What does it mean to say that information is preserved by some process? These questions are central to a theory of quantum information processing, and the purpose of this chapter is the development of distance measures giving quantitative answers to these questions. Motivated by our two questions we will be concerned with two broad classes of distance measures, static measures and dynamic measures. Static measures quantify how close two quantum states are, while dynamic measures quantify how well information has been preserved during a dynamic process. The strategy we take is to begin by developing good static measures of distance, and then to use those static measures as the basis for the development of dynamic measures of distance.

There is a certain arbitrariness in the way distance measures are defined, both classically and quantum mechanically, and the community of people studying quantum computation and quantum information has found it convenient to use a variety of distance measures over the years. Two of those measures, the trace distance and the fidelity, have particularly wide currency today, and we discuss both these measures in detail in this chapter. For the most part the properties of both are quite similar, however for certain applications one may be easier to deal

with than the other. It is for this reason and because both are widely used within the quantum computation and quantum information community that we discuss both measures.

9.2.1 9.1 Distance measures for classical information

> The idea of distinguishing probability distributions is slippery business. - Christopher Fuchs

Let's start out in an arena where we can easily apply our intuition - distance measures for classical information. What are the objects to be compared in classical information theory? We might consider comparing strings of bits like 00010 and 10011 . One way of quantifying the distance between these is the Hamming distance, defined to be the number of places at which two bit strings are not equal. For example, the bit strings 00010 and 10011 differ in the first and last place, so the Hamming distance between them is two. Unfortunately, the Hamming distance between two objects is simply a matter of labeling, and a priori there aren't any labels in the Hilbert space arena of quantum mechanics!

A much better place to launch the study of distance measures for quantum information is with the comparison of classical probability distributions. In fact, in classical information theory an information source is usually modeled as a random variable, that is, as a probability distribution over some source alphabet. For example, an unknown source of English text may be modeled as a sequence of random variables over the Roman alphabet.

Before the text is read we can make a fair guess at the relative frequency of the letters that appear in the text, and certain correlations among them, such as the fact that occurrences of the pair of letters 'th' are much more common than the pair 'zx' in English text. This characterization of information sources as probability distributions over some alphabet encourages us to concentrate on the comparison of probability distributions in our search for measures of distance.

What does it mean to say that two probability distributions $\{p_x\}$ and $\{q_x\}$ over the same index set, x, are similar to one another? It is difficult to give an answer to this question which is obviously the unique 'correct' answer, so instead we propose two different answers, each of which is widely used by the quantum computation and quantum information community. The first measure is the trace distance, defined by the equation:

$$D\left(p_x, q_x\right) \equiv \frac{1}{2} \sum_x |p_x - q_x| \tag{9.1}$$

This quantity is sometimes known as the L_1 distance or Kolmogorov distance. We prefer the term trace distance because it anticipates the later quantum mechanical analogue of this quantity, which is defined using the trace function. The trace distance turns out to be a metric on probability distributions, (a metric $D(x, y)$ must be symmetric, $D(x, y) = D(y, x)$, and satisfy the triangle inequality, $D(x, z) \leq D(x, y) + D(y, z)$) so the use of the term 'distance' is justified.

Exercise 9.1: What is the trace distance between the probability distribution (1,0) and the probability distribution $(1/2, 1/2)$? Between $(1/2, 1/3, 1/6)$ and $(3/4, 1/8, 1/8)$?

Exercise 9.2: Show that the trace distance between probability distributions ($p, 1-p$) and $(q, 1-q)$ is $|p-q|$.

A second measure of distance between probability distributions, the fidelity of the probability distributions $\{p_x\}$ and $\{q_x\}$, is defined by

$$F\left(p_x, q_x\right) \equiv \sum_x \sqrt{p_x q_x} \tag{9.2}$$

The fidelity is a very different way of measuring distance between probability distributions than is the trace distance. To begin with, it is not a metric, although later we discuss a metric derived from the fidelity. To see that the fidelity is not a metric note that when the distributions $\{p_x\}$ and $\{q_x\}$ are identical, $F(p_x, q_x) = \sum_x p_x = 1$. A better geometric understanding of the fidelity is illustrated in Figure 9.1; the fidelity is just the inner product between vectors with components $\sqrt{p_x}$ and $\sqrt{q_x}$, which lie on a unit sphere.

Exercise 9.3: What is the fidelity of the probability distributions (1,0) and ($1/2, 1/2$)? Of $(1/2, 1/3, 1/6)$ and $(3/4, 1/8, 1/8)$?

The trace distance and fidelity are mathematically useful means of defining the notion of a distance between two probability distributions. Do these measures have physically motivated operational meanings? In the case of the trace distance, the answer to this

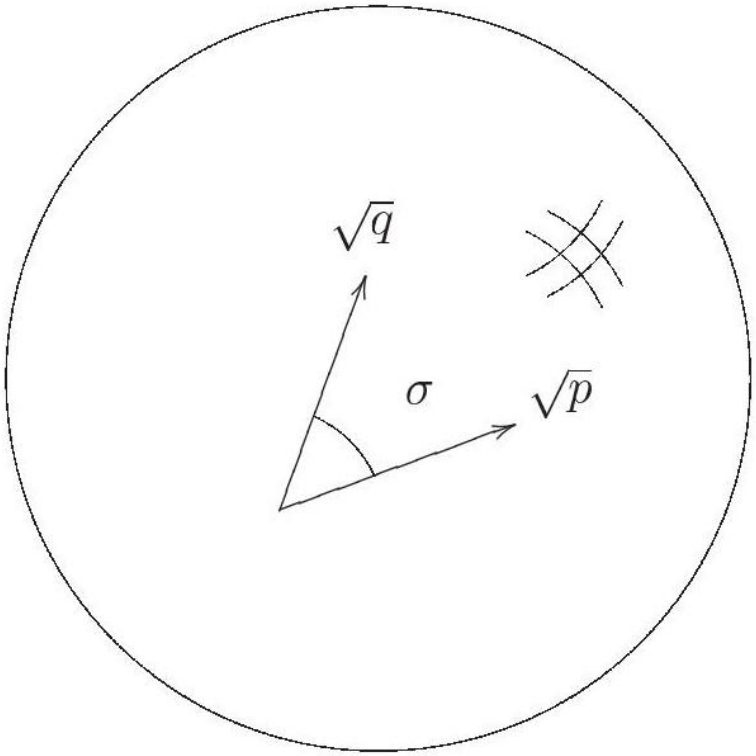


Figure 9.1. Geometric interpretation of the fidelity as the inner product between vectors $\sqrt{p_x}$ and $\sqrt{q_x}$ lying on a unit sphere. (Since $1 = \sum_x \left(\sqrt{p_x}\right)^2 = \sum_x \left(\sqrt{q_x}\right)^2$.)

$$F(p, q) = \sqrt{p} \cdot \sqrt{q} = \cos(\sigma)$$

question is yes. In particular, it is simple to prove that

$$D(p_x, q_x) = \max_S |p(S) - q(S)| = \max_S \left| \sum_{x \in S} p_x - \sum_{x \in S} q_x \right|, \tag{9.3}$$

where the maximization is over all subsets S of the index set $\{x\}$. The quantity being maximized is the difference between the probability that the event S occurs, according to the distribution $\{p_x\}$, and the probability that the event S occurs, according to the distribution $\{q_x\}$. The event S is thus in some sense the optimal event to examine when trying to distinguish the distributions $\{p_x\}$ and $\{q_x\}$, with the trace distance governing how well it is possible to make this distinction.

Unfortunately, a similarly clear interpretation for the fidelity is not known. However, in the next section we show that the fidelity is a sufficiently useful quantity for mathematical purposes to justify its study, even without a clear physical interpretation. Moreover, we cannot rule out the possibility that a clear interpretation of the fidelity will be discovered in the future. Finally, it turns out that there are close connections between the fidelity and the trace distance, so properties of one quantity can often be used to deduce properties of the other, a fact which is useful surprisingly often.

Exercise 9.4: Prove (9.3).

Exercise 9.5: Show that the absolute value signs may be removed from Equation (9.3), that is,

$$D\left(p_x, q_x\right) = \max_S (p(S) - q(S)) = \max_S \left(\sum_{x \in S} p_x - \sum_{x \in S} q_x \right). \tag{9.4}$$

The trace distance and fidelity are static measures of distance for comparing two fixed probability distributions. There is a third notion of distance which is a dynamic measure of distance in the sense that it measures how well information is preserved by some physical process. Suppose a random variable X is sent through a noisy channel, giving as output another random variable Y, to form a Markov process $X \rightarrow Y$. For convenience we assume both X and Y have the same range of values, denoted by x. Then the probability that Y is not equal to $X, p(X \neq Y)$, is an obvious and important measure of the degree to which information has been preserved by the process.

Surprisingly, this dynamic measure of distance can be understood as a special case of the static trace distance! Imagine that the random variable X is given to you, and you make a copy of X, creating a new random variable $\tilde{X} = X$. The random variable X now passes through the noisy channel, leaving as output the random variable Y, as illustrated in Figure 9.2. How close is the initial perfectly correlated pair, $(\tilde{X}, X)$, to the final pair, $(\tilde{X}, Y)$? Using the trace distance as our measure of 'closeness', we obtain with some simple algebra,

$$\begin{aligned}
D((\tilde{X}, X), (X, Y)) &= \frac{1}{2} \sum_{xx'} \left| \delta_{xx'} p(X = x) - p\left(\tilde{X} = x, Y = x'\right) \right| && (9.5) \\
&= \frac{1}{2} \sum_{x \neq x'} p\left(\tilde{X} = x, Y = x'\right) + \frac{1}{2} \sum_x |p(X = x) - p(\tilde{X} = x, Y = x)| \\
&= \frac{1}{2} \sum_{x \neq x'} p\left(\tilde{X} = x, Y = x'\right) + \frac{1}{2} \sum_x (p(X = x) - p(\tilde{X} = x, Y = x)) && (9.6) \\
&= \frac{p(\tilde{X} \neq Y) + 1 - p(\tilde{X} = Y)}{2} && (9.7) \\
&= \frac{p(X \neq Y) + p(\tilde{X} \neq Y)}{2} && (9.9) \\
&= p(X \neq Y) && (9.10)
\end{aligned}$$

Thus, as illustrated in Figure 9.3, the probability of an error in the channel is equal to the trace distance between the probability distribution for $(\tilde{X}, X)$ and $(\tilde{X}, Y)$. This is an important construction, since it will be the basis for analogous quantum constructions. This is necessary because there is no direct quantum analogue of the probability $p(X \neq Y)$, since there is no notion in quantum mechanics analogous to the joint probability distribution for variables X and Y that exist at different times. Instead, to define dynamic measures of quantum distance we use an approach similar to the construction just given, based on the idea that it is quantum

entanglement, rather than classical correlation, which is the important thing to preserve during a quantum channel's dynamics.

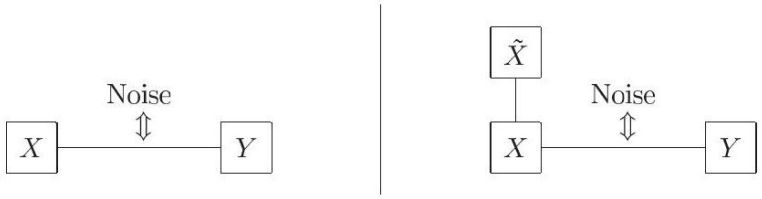


Figure 9.2. Given a Markov process $X \to Y$ we may first make a copy of $X, \tilde{X}$, before subjecting X to the noise which turns it into Y.}

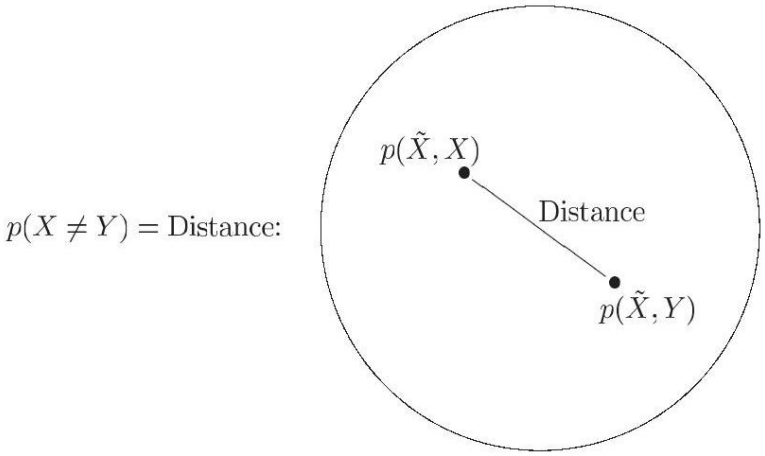


Figure 9.3. The probability of an error in the channel is equal to the trace distance between the probability distributions for ($\tilde{X}$, X$) and ($\tilde{X}, Y$).}

9.2.2 9.2 How close are two quantum states?

How close are two quantum states? Over the next few sections we describe quantum generalizations of the classical notions of trace distance and fidelity, and discuss in detail the properties of these quantities.

9.2.3 9.2.1 Trace distance

We begin by defining the trace distance between quantum states ρ and σ,

$$D(\rho, \sigma) \equiv \frac{1}{2} \operatorname{tr} |\rho - \sigma|. \tag{9.11}$$

where as per usual we define $|A| \equiv \sqrt{A^\dagger A}$ to be the positive square root of $A^\dagger A$. Notice that the quantum trace distance generalizes the classical trace distance in the sense that if ρ and σ commute then the (quantum) trace distance between ρ and σ is equal to the classical trace distance between the eigenvalues of ρ and σ. More explicitly, if ρ and σ commute they are diagonal in the same basis,

$$\rho = \sum_i r_i |i\rangle\langle i|; \quad \sigma = \sum_i s_i |i\rangle\langle i|, \tag{9.12}$$

for some orthonormal basis $|i\rangle$. Thus

$$D(\rho,\sigma) = \frac{1}{2}\operatorname{tr}\left|\sum_i (r_i - s_i)\right| i\Big\rangle\langle i|\,| \tag{9.13}$$

$$= D\left(r_i, s_i\right) \tag{9.14}$$

Exercise 9.6: What is the trace distance between the density operators

$$\frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|; \quad \frac{2}{3}|0\rangle\langle 0| + \frac{1}{3}|1\rangle\langle 1|? \tag{9.15}$$

Between:

$$\frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|; \quad \frac{2}{3}|+\rangle\langle +| + \frac{1}{3}|-\rangle\langle -|? \tag{9.16}$$

(Recall that $|\pm\rangle \equiv (|0\rangle \pm |1\rangle)/\sqrt{2}$.)

A good way of getting a feel for the trace distance is to understand it for the special case of a qubit, in the Bloch sphere representation. Suppose ρ and σ have respective Bloch vectors $\vec{r}$ and $\vec{s}$,

$$\rho = \frac{I + \vec{r}\cdot\vec{\sigma}}{2}; \quad \sigma = \frac{I + \vec{s}\cdot\vec{\sigma}}{2}. \tag{9.17}$$

(Recall that $\vec{\sigma}$ denotes a vector of Pauli matrices; it should not be confused with the state σ.) The trace distance between ρ and σ is easily calculated:

$$D(\rho,\sigma) = \frac{1}{2}\operatorname{tr}|\rho - \sigma| \tag{9.18}$$

$$= \frac{1}{4}\operatorname{tr}|(\vec{r} - \vec{s})\cdot\vec{\sigma}| \tag{9.19}$$

$(\vec{r} - \vec{s})\cdot\vec{\sigma}$ has eigenvalues $\pm|\vec{r} - \vec{s}|$, so the trace of $|(\vec{r} - \vec{s})\cdot\sigma|$ is $2|\vec{r} - \vec{s}|$, and we see that

$$D(\rho,\sigma) = \frac{|\vec{r} - \vec{s}|}{2} \tag{9.20}$$

That is, the distance between two single qubit states is equal to one half the ordinary Euclidean distance between them on the Bloch sphere!

This intuitive geometric picture of the trace distance for qubits is often useful when trying to understand general properties of the trace distance. Conjectured properties can be suggested, refuted, or gain plausibility by looking at simple examples on the Bloch sphere. For example, rotations of the Bloch sphere leave the Euclidean distance invariant. This suggests that the trace distance might be preserved under unitary transformations in general,

$$D\left(U\rho U^\dagger, U\sigma U^\dagger\right) = D(\rho,\sigma) \tag{9.21}$$

a conjecture which you can easily verify with a moment's thought. We will come back to the Bloch sphere picture often in our investigation of distance measures.

To understand the properties of the trace distance a good starting point is to prove a formula for the trace distance generalizing Equation (9.3) for the classical trace distance:

$$D(\rho,\sigma) = \max_P \operatorname{tr}(P(\rho - \sigma)) \tag{9.22}$$

where the maximization may be taken alternately over all projectors, P, or over all positive operators $P \leq I$; the formula is valid in either case. This formula gives rise to an appealing interpretation of the trace distance. Recalling that POVM elements are positive operators $P \leq I$, the trace distance is therefore equal to the difference in probabilities that a measurement outcome with POVM element P may occur, depending on whether the state is ρ or σ, maximized over all possible POVM elements P.

We prove Equation (9.22) for the case where the maximization is over projectors; the case of positive operators $P \leq I$ follows the same reasoning. The proof is based on the fact that $\rho - \sigma$ can be expressed as $\rho - \sigma = Q - S$, where Q and S are positive operators with orthogonal support (see Exercise 9.7). It implies that $|\rho - \sigma| = Q + S$, so $D(\rho, \sigma) = (\mathrm{tr}(Q) + \mathrm{tr}(S))/2$. But $\mathrm{tr}(Q - S) = \mathrm{tr}(\rho - \sigma) = 0$, so $\mathrm{tr}(Q) = \mathrm{tr}(S)$, and therefore $D(\rho, \sigma) = \mathrm{tr}(Q)$. Let P be the projector onto the support of Q. Then $\mathrm{tr}(P(\rho - \sigma)) = \mathrm{tr}(P(Q - S)) = \mathrm{tr}(Q) = D(\rho, \sigma)$. Conversely, let P be any projector.

Then $\mathrm{tr}(P(\rho - \sigma)) = \mathrm{tr}(P(Q - S)) \leq \mathrm{tr}(PQ) \leq \mathrm{tr}(Q) = D(\rho, \sigma)$. This completes the proof.

Exercise 9.7: Show that for any states ρ and σ, one may write $\rho - \sigma = Q - S$, where Q and S are positive operators with support on orthogonal vector spaces. (Hint: use the spectral decomposition $\rho - \sigma = UDU^\dagger$, and split the diagonal matrix D into positive and negative parts. This fact will continue to be useful later.)

There is a closely related way of viewing the quantum trace distance which relates it more closely to the classical trace distance:

Theorem 9.1: Let $\{E_m\}$ be a POVM, with $p_m \equiv \mathrm{tr}\,(\rho E_m)$ and $q_m \equiv \mathrm{tr}\,(\sigma E_m)$ as the probabilities of obtaining a measurement outcome labeled by m. Then

$$D(\rho, \sigma) = \max_{\{E_m\}} D\,(p_m, q_m)\,, \tag{9.23}$$

where the maximization is over all POVMs $\{E_m\}$.

Proof

Note that

$$D\,(p_m, q_m) = \frac{1}{2} \sum_m \left|\mathrm{tr}\,(E_m(\rho - \sigma))\right|. \tag{9.24}$$

Using the spectral decomposition we may write $\rho - \sigma = Q - S$, where Q and S are positive operators with orthogonal support. Thus $|\rho - \sigma| = Q + S$, and

$$\begin{aligned} \left|\mathrm{tr}\,(E_m(\rho - \sigma))\right| &= \left|\mathrm{tr}\,(E_m(Q - S))\right| && (9.25)\\ &\leq \mathrm{tr}\,(E_m(Q + S)) && (9.26)\\ &\leq \mathrm{tr}\,(E_m|\rho - \sigma|)\,. && (9.27) \end{aligned}$$

Thus

$$\begin{aligned} D\,(p_m, q_m) &\leq \frac{1}{2} \sum_m \mathrm{tr}\,(E_m|\rho - \sigma|) && (9.28)\\ &= \frac{1}{2}\,\mathrm{tr}(|\rho - \sigma|) && (9.29)\\ &= D(\rho, \sigma), && (9.30) \end{aligned}$$

where we have applied the completeness relation for POVM elements, $\sum_m E_m = I$. Conversely, by choosing a measurement whose POVM elements include projectors onto the

support of Q and S, we see that there exist measurements which give rise to probability distributions such that $D\left(p_m, q_m\right) = D(\rho, \sigma)$.

Thus, if two density operators are close in trace distance, then any measurement performed on those quantum states will give rise to probability distributions which are close together in the classical sense of trace distance, giving a second interpretation of the trace distance between two quantum states as an achievable upper bound on the trace distance between probability distributions arising from measurements performed on those quantum states.

We call the trace distance a 'distance', so we should check to see whether it has the property of being a metric on the space of density operators. From our geometric picture for a single qubit this is obviously true for a single qubit; is it true more generally? It is clear that $D(\rho, \sigma) = 0$ if and only if $\rho = \sigma$, and that $D(\cdot, \cdot)$ is a symmetric function of its inputs. All that remains to check is that the triangle inequality holds,

$$D(\rho, \tau) \leq D(\rho, \sigma) + D(\sigma, \tau). \tag{9.31}$$

To see this, note from Equation (9.22) that there exists a projector P such that

$$\begin{aligned} D(\rho, \tau) &= \operatorname{tr}(P(\rho - \tau)) && (9.32)\\ &= \operatorname{tr}(P(\rho - \sigma)) + \operatorname{tr}(P(\sigma - \tau)) && (9.33)\\ &\leq D(\rho, \sigma) + D(\sigma, \tau), && (9.34) \end{aligned}$$

establishing that the trace distance is a metric.

At this stage, we don't know a whole lot about the trace distance. However, we're in a good position to prove some genuinely spectacular results, useful in a wide variety of contexts. The most interesting result is that no physical process ever increases the distance between two quantum states, a result illustrated in Figure 9.4. We state this more formally as a theorem:

Theorem 9.2: (Trace-preserving quantum operations are contractive) Suppose $\mathcal{E}$ is a trace-preserving quantum operation. Let ρ and σ be density operators. Then

$$D(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \leq D(\rho, \sigma). \tag{9.35}$$

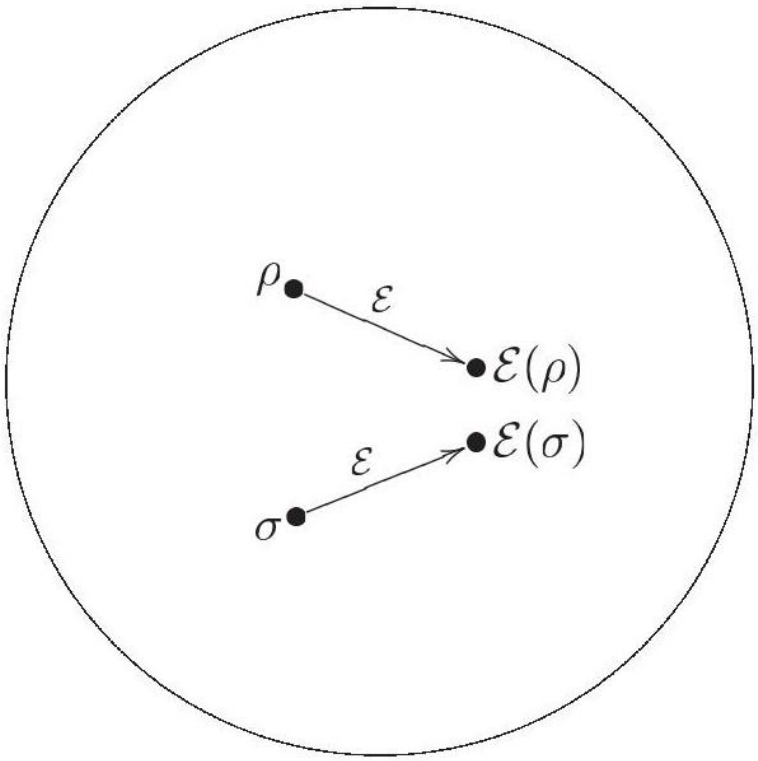


Figure 9.4. Trace-preserving quantum operations cause a contraction on the space of density operators.

Proof

Use the spectral decomposition to write $\rho - \sigma = Q - S$, where Q and S are positive matrices with orthogonal support, and let P be a projector such that $D(\mathcal{E}(\rho), \mathcal{E}(\sigma)) = \mathrm{tr}[P(\mathcal{E}(\rho) - \mathcal{E}(\sigma))]$. Observe that $\mathrm{tr}(Q) - \mathrm{tr}(S) = \mathrm{tr}(\rho) - \mathrm{tr}(\sigma) = 0$, so $\mathrm{tr}(Q) = \mathrm{tr}(S)$ and thus $\mathrm{tr}(\mathcal{E}(Q)) = \mathrm{tr}(\mathcal{E}(S))$. Using this observation we see that

$$\begin{aligned}
D(\rho, \sigma) &= \frac{1}{2} \mathrm{tr} \, |\rho - \sigma| && (9.36)\\
&= \frac{1}{2} \mathrm{tr} \, |Q - S| && (9.37)\\
&= \frac{1}{2} \mathrm{tr}(Q) + \frac{1}{2} \mathrm{tr}(S) && (9.38)\\
&= \frac{1}{2} \mathrm{tr}(\mathcal{E}(Q)) + \frac{1}{2} \mathrm{tr}(\mathcal{E}(S)) && (9.39)\\
&= \mathrm{tr}(\mathcal{E}(Q)) && (9.40)\\
&\geq \mathrm{tr}(P\mathcal{E}(Q)) && (9.41)\\
&\geq \mathrm{tr}(P(\mathcal{E}(Q) - \mathcal{E}(S))) && (9.42)\\
&= \mathrm{tr}(P(\mathcal{E}(\rho) - \mathcal{E}(\sigma))) && (9.43)\\
&= D(\mathcal{E}(\rho), \mathcal{E}(\sigma)) && (9.44)
\end{aligned}$$

which completes the proof.

There is an important special case of this result which can be understood by the following analogy. Imagine somebody shows you two different paintings in a gallery. Provided you have reasonably good vision, you shouldn't have any difficulty telling them apart. On the other hand,

if somebody covers up most of the two paintings then you might have more difficulty telling the two apart, as illustrated in Figure 9.5. Similarly, if we 'cover up' parts of two quantum states then we can show that the distance between those two states is never increased. To prove this, recall from page 374 that the partial trace is a trace-preserving quantum operation. By Theorem 9.2, if we take quantum states ρ^{AB} and σ^{AB} of a composite quantum system AB then the distance between $\rho^A = \mathrm{tr}_B\left(\rho^{AB}\right)$ and $\sigma^A = \mathrm{tr}_B\left(\sigma^{AB}\right)$ is never more than the distance between ρ^{AB} and σ^{AB},

$$D\left(\rho^A, \sigma^A\right) \leq D\left(\rho^{AB}, \sigma^{AB}\right). \tag{9.45}$$

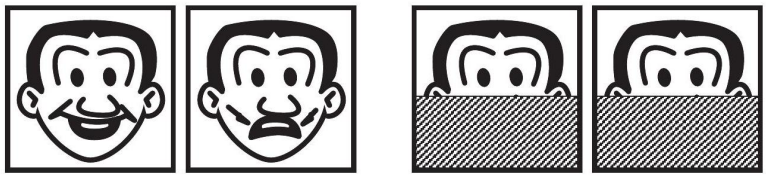


Figure 9.5. Objects become less distinguishable when only partial information is available.

In many applications we want to estimate the trace distance for a mixture of inputs. Such estimates are greatly aided by the following theorem:

Theorem 9.3: (Strong convexity of the trace distance) Let $\{p_i\}$ and $\{q_i\}$ be probability distributions over the same index set, and ρ_i and σ_i be density operators, also with indices from the same index set. Then

$$D\left(\sum_i p_i\rho_i, \sum_i q_i\sigma_i\right) \leq D\left(p_i, q_i\right) + \sum_i p_i D\left(\rho_i, \sigma_i\right), \tag{9.46}$$

where $D\left(p_i, q_i\right)$ is the classical trace distance between the probability distributions $\{p_i\}$ and $\{q_i\}$.

This result can be used to prove convexity results for the trace distance so we refer to this property as the strong convexity property for trace distance.

Proof

By Equation (9.22) there exists a projector P such that

$$\begin{aligned} D\left(\sum_i p_i\rho_i, \sum_i q_i\sigma_i\right) &= \sum_i p_i \,\mathrm{tr}\left(P\rho_i\right) - \sum_i q_i \,\mathrm{tr}\left(P\sigma_i\right) && (9.47)\\ &= \sum_i p_i \,\mathrm{tr}\left(P\left(\rho_i - \sigma_i\right)\right) + \sum_i \left(p_i - q_i\right)\mathrm{tr}\left(P\sigma_i\right) && (9.48)\\ &\leq \sum_i p_i D\left(\rho_i, \sigma_i\right) + D\left(p_i, q_i\right) && (9.49) \end{aligned}$$

where $D\left(p_i, q_i\right)$ is the trace distance between the probability distributions $\{p_i\}$ and $\{q_i\}$, and we used Equation (9.22) in the last line.

As a special case of this result, we see that the trace distance is jointly convex in its inputs,

$$D\left(\sum_i p_i\rho_i, \sum_i p_i\sigma_i\right) \leq \sum_i p_i D\left(\rho_i, \sigma_i\right). \tag{9.50}$$

Exercise 9.8: (Convexity of the trace distance) Show that the trace distance is convex in its first input,

$$D\left(\sum_i p_i \rho_i, \sigma\right) \leq \sum_i p_i D\left(\rho_i, \sigma\right). \tag{9.51}$$

By symmetry convexity in the second entry follows from convexity in the first.
Exercise 9.9: (Existence of fixed points) Schauder's fixed point theorem is a classic result from mathematics that implies that any continuous map on a convex, compact subset of a Hilbert space has a fixed point. Use Schauder's fixed point theorem to prove that any trace-preserving quantum operation $\mathcal{E}$ has a fixed point, that is, ρ such that $\mathcal{E}(\rho) = \rho$.

Exercise 9.10: Suppose $\mathcal{E}$ is a strictly contractive trace-preserving quantum operation, that is, for any ρ and $\sigma, D(\mathcal{E}(\rho), \mathcal{E}(\sigma)) < D(\rho, \sigma)$. Show that $\mathcal{E}$ has a unique fixed point.

Exercise 9.11: Suppose $\mathcal{E}$ is a trace-preserving quantum operation for which there exists a density operator ρ_0 and a trace-preserving quantum operation $\mathcal{E}'$ such that

$$\mathcal{E}(\rho) = p\rho_0 + (1-p)\mathcal{E}'(\rho), \tag{9.52}$$

for some $p, 0 < p \leq 1$. Physically, this means that with probability p the input state is thrown out and replaced with the fixed state ρ_0, while with probability
$1 - p$ the operation $\mathcal{E}'$ occurs. Use joint convexity to show that $\mathcal{E}$ is a strictly contractive quantum operation, and thus has a unique fixed point.

Exercise 9.12: Consider the depolarizing channel introduced in Section 8.3.4 on page 378, $\mathcal{E}(\rho) = pI/2 + (1-p)\rho$. For arbitrary ρ and σ find $D(\mathcal{E}(\rho), \mathcal{E}(\sigma))$ using the Bloch representation, and prove explicitly that the map $\mathcal{E}$ is strictly contractive, that is, $D(\mathcal{E}(\rho), \mathcal{E}(\sigma)) < D(\rho, \sigma)$.

Exercise 9.13: Show that the bit flip channel (Section 8.3.3) is contractive but not strictly contractive. Find the set of fixed points for the bit flip channel.

9.2.4 9.2.2 Fidelity

A second measure of distance between quantum states is the fidelity. The fidelity is not a metric on density operators, but we will see that it does give rise to a useful metric. This section reviews the definition and basic properties of the fidelity. The fidelity of states ρ and σ is defined to be

$$F(\rho, \sigma) \equiv \operatorname{tr} \sqrt{\rho^{1/2} \sigma \rho^{1/2}} \tag{9.53}$$

It is certainly not immediately obvious that this is a useful measure of distance between ρ and σ. It doesn't even look symmetric! Yet we will see that the fidelity is symmetric in its inputs, and has many of the other properties we expect of a good distance measure.

There are two important special cases where it is possible to give more explicit formulae for the fidelity. The first is when ρ and σ commute, that is, are diagonal in the same basis,

$$\rho = \sum_i r_i |i\rangle\langle i|; \quad \sigma = \sum_i s_i |i\rangle\langle i|, \tag{9.54}$$

for some orthonormal basis $|i\rangle$. In this case we see that

$$F(\rho,\sigma) = \operatorname{tr}\sqrt{\sum_i r_i s_i |i\rangle\langle i|} \tag{9.55}$$

$$= \operatorname{tr}\left(\sum_i \sqrt{r_i s_i}|i\rangle\langle i|\right) \tag{9.56}$$

$$= \sum_i \sqrt{r_i s_i} \tag{9.57}$$

$$= F\left(r_i, s_i\right). \tag{9.58}$$

That is, when ρ and σ commute the quantum fidelity $F(\rho,\sigma)$ reduces to the classical fidelity $F\left(r_i, s_i\right)$ between the eigenvalue distributions r_i and s_i of ρ and σ.

Our second example is to calculate the fidelity between a pure state $|\psi\rangle$ and an arbitrary state, ρ. From Equation (9.53) we see that

$$F(|\psi\rangle,\rho) = \operatorname{tr}\sqrt{\langle\psi|\rho|\psi\rangle|\psi\rangle\langle\psi|} \tag{9.59}$$

$$= \sqrt{\langle\psi|\rho|\psi\rangle} \tag{9.60}$$

That is, the fidelity is equal to the square root of the overlap between $|\psi\rangle$ and ρ. This is an important result which we will make use of often.

For the case of a qubit we were able to explicitly evaluate the trace distance between two states, and give it a simple geometric interpretation as half the Euclidean distance between points on the Bloch sphere. Unfortunately, no similarly clear geometric interpretation is known for the fidelity between two states of a qubit.

However, the fidelity does satisfy many of the same properties as the trace distance. For example, it is invariant under unitary transformations:

$$F\left(U\rho U^\dagger, U\sigma U^\dagger\right) = F(\rho,\sigma). \tag{9.61}$$

Exercise 9.14: (Invariance of fidelity under unitary transforms) Prove (9.61) by using the fact that for any positive operator A, $\sqrt{UAU^\dagger} = U\sqrt{A}U^\dagger$.

There is also a useful characterization of the fidelity analogous to the characterization (9.22) for the trace distance.

Theorem 9.4: (Uhlmann's theorem) Suppose ρ and σ are states of a quantum system Q. Introduce a second quantum system R which is a copy of Q. Then

$$F(\rho,\sigma) = \max_{|\psi\rangle,|\varphi\rangle} |\langle\psi \mid \varphi\rangle|, \tag{9.62}$$

where the maximization is over all purifications $|\psi\rangle$ of ρ and $|\varphi\rangle$ of σ into RQ.

Before giving the proof of Uhlmann's theorem we need an easily proved lemma.

Lemma 9.5: Let A be any operator, and U unitary. Then

$$|\operatorname{tr}(AU)| \leq \operatorname{tr}|A|, \tag{9.63}$$

with equality being attained by choosing $U = V^\dagger$, where $A = |A|V$ is the polar decomposition of A.

Proof

Equality is clearly attained under the conditions stated. Observe that

$$|\operatorname{tr}(AU)| = |\operatorname{tr}(|A|VU)| = \left|\operatorname{tr}\left(|A|^{1/2}|A|^{1/2}VU\right)\right|. \tag{9.64}$$

The Cauchy-Schwarz inequality for the Hilbert-Schmidt inner product gives:

$$|\operatorname{tr}(AU)| \leq \sqrt{\operatorname{tr}|A| \operatorname{tr}\left(U^\dagger V^\dagger |A| VU\right)} = \operatorname{tr}|A|, \tag{9.65}$$

which completes the proof.

Proof

(Uhlmann's theorem)

Fix orthonormal bases $|i_R\rangle$ and $|i_Q\rangle$ in systems R and Q. Because R and Q are of the same dimension, the index i may be assumed to run over the same set of values. Define $|m\rangle \equiv \sum_i |i_R\rangle |i_Q\rangle$. Let $|\psi\rangle$ be any purification of ρ. Then the Schmidt decomposition and a moment's thought should convince you that

$$|\psi\rangle = (U_R \otimes \sqrt{\rho} U_Q)|m\rangle, \tag{9.66}$$

for some unitary operators U_R and U_Q on systems R and Q. Similarly, if $|\varphi\rangle$ is any purification of σ then there exist unitary operators V_R and V_Q such that

$$|\varphi\rangle = \left(V_R \otimes \sqrt{\sigma} V_Q\right)|m\rangle. \tag{9.67}$$

Taking the inner product gives

$$|\langle \psi \mid \varphi\rangle| = \left|\langle m| \left(U_R^\dagger V_R \otimes U_Q^\dagger \sqrt{\rho}\sqrt{\sigma} V_Q\right) \middle| m\right\rangle|. \tag{9.68}$$

Using Exercise 9.16 on this page we see that

$$|\langle \psi \mid \varphi\rangle| = \left|\operatorname{tr}\left(V_R^\dagger U_R U_Q^\dagger \sqrt{\rho}\sqrt{\sigma} V_Q\right)\right|. \tag{9.69}$$

Setting $U \equiv V_Q V_R^\dagger U_R U_Q^\dagger$ we see that

$$|\langle \psi \mid \varphi\rangle| = |\operatorname{tr}(\sqrt{\rho}\sqrt{\sigma} U)|. \tag{9.70}$$

By Lemma 9.5,

$$|\langle \psi \mid \varphi\rangle| \leq \operatorname{tr}|\sqrt{\rho}\sqrt{\sigma}| = \operatorname{tr}\sqrt{\rho^{1/2}\sigma\rho^{1/2}}. \tag{9.71}$$

To see that equality may be attained, suppose $\sqrt{\rho}\sqrt{\sigma} = |\sqrt{\rho}\sqrt{\sigma}|V$ is the polar decomposition of $\sqrt{\rho}\sqrt{\sigma}$. Choosing $U_Q = U_R = V_R = I$ and $V_Q = V^\dagger$ we see that equality is attained. □

Exercise 9.15: Show that

$$F(\rho, \sigma) = \max_{|\varphi\rangle} |\langle \psi \mid \varphi\rangle|, \tag{9.72}$$

where $|\psi\rangle$ is any fixed purification of ρ, and the maximization is over all purifications of σ.

Exercise 9.16: (The Hilbert-Schmidt inner product and entanglement)
Suppose R and Q are two quantum systems with the same Hilbert space. Let $|i_R\rangle$ and $|i_Q\rangle$ be orthonormal basis sets for R and Q. Let A be an operator on R and B an operator on Q. Define $|m\rangle \equiv \sum_i |i_R\rangle |i_Q\rangle$. Show that

$$\mathrm{tr}\left(A^\dagger B\right) = \langle m|(A \otimes B)|m\rangle, \tag{9.73}$$

where the multiplication on the left hand side is of matrices, and it is understood that the matrix elements of A are taken with respect to the basis $|i_R\rangle$ and those for B with respect to the basis $|i_Q\rangle$.

Uhlmann's formula (9.62) does not provide a calculational tool for evaluating the fidelity, as does Equation (9.53). However, in many instances, properties of the fidelity are more easily proved using Uhlmann's formula than Equation (9.53). For example, Uhlmann's formula makes it clear that the fidelity is symmetric in its inputs, $F(\rho, \sigma) = F(\sigma, \rho)$, and that the fidelity is bounded between 0 and $1, 0 \leq F(\rho, \sigma) \leq 1$. If $\rho = \sigma$ then it is clear that $F(\rho, \sigma) = 1$, from Uhlmann's formula. If $\rho \neq \sigma$ then $|\psi\rangle \neq |\varphi\rangle$ for any purifications $|\psi\rangle$ and $|\varphi\rangle$ of ρ and σ, respectively, so $F(\rho, \sigma) < 1$. On the other hand, Equation (9.53) is sometimes useful as a means for understanding properties of the fidelity. For instance, we see that $F(\rho, \sigma) = 0$ if and only if ρ and σ have support on orthogonal subspaces. Intuitively, when ρ and σ are supported on orthogonal subspaces
they are perfectly distinguishable, so we should expect the fidelity to be minimized at this point. Summarizing, the fidelity is symmetric in its inputs, $0 \leq F(\rho, \sigma) \leq 1$, with equality in the first inequality if and only if ρ and σ have orthogonal support, and equality in the second inequality if and only if $\rho = \sigma$.

We saw that the quantum trace distance could be related to the classical trace distance by considering the probability distributions induced by a measurement. In a similar way, we can show that

$$F(\rho, \sigma) = \min_{\{E_m\}} F\left(p_m, q_m\right), \tag{9.74}$$

where the minimum is over all POVMs $\{E_m\}$, and $p_m \equiv \mathrm{tr}\left(\rho E_m\right), q_m \equiv \mathrm{tr}\left(\sigma E_m\right)$ are the probability distributions for ρ and σ corresponding to the POVM $\{E_m\}$. To see that this is true, apply the polar decomposition $\sqrt{\rho^{1/2}\sigma\rho^{1/2}} = \sqrt{\rho}\sqrt{\sigma}U$, and note that

$$F(\rho, \sigma) = \mathrm{tr}(\sqrt{\rho}\sqrt{\sigma}U) \tag{9.75}$$

$$= \sum_m \mathrm{tr}\left(\sqrt{\rho}\sqrt{E_m}\sqrt{E_m}\sqrt{\sigma}U\right). \tag{9.76}$$

The Cauchy-Schwarz inequality and some simple algebra gives

$$F(\rho, \sigma) \leq \sum_m \sqrt{\mathrm{tr}\left(\rho E_m\right)\mathrm{tr}\left(\sigma E_m\right)} \tag{9.77}$$

$$= F\left(p_m, q_m\right) \tag{9.78}$$

which establishes that

$$F(\rho, \sigma) \leq \min_{\{E_m\}} F\left(p_m, q_m\right) \tag{9.79}$$

To see that equality can be attained in this inequality, we need to find a POVM $\{E_m\}$ such that the Cauchy-Schwarz inequality is satisfied with equality for each term in the sum, that is, $\sqrt{E_m}\sqrt{\rho} = \alpha_m\sqrt{E_m}\sqrt{\sigma}U$ for some set of complex numbers α_m. But $\sqrt{\rho}\sqrt{\sigma}U = \sqrt{\rho^{1/2}\sigma\rho^{1/2}}$, so for invertible ρ,

$$\sqrt{\sigma}U = \rho^{-1/2}\sqrt{\rho^{1/2}\sigma\rho^{1/2}} \tag{9.80}$$

Substituting, we find that the equality conditions are that

$$\sqrt{E_m}\,(I - \alpha_m M) = 0 \tag{9.81}$$

where $M \equiv \rho^{-1/2}\sqrt{\rho^{1/2}\sigma\rho^{1/2}}\rho^{-1/2}$. If $M = \sum_m \beta_m |m\rangle\langle m|$ is a spectral decomposition for M then we choose $E_m = |m\rangle\langle m|$ and $\alpha_m = 1/\beta_m$. The case of non-invertible ρ follows from continuity.

We proved three important properties of the trace distance - the metric property, contractivity, and strong convexity. Rather remarkably, analogous properties all hold for the fidelity. What is more, the proof techniques used for fidelity differ considerably from those used for the trace distance. For that reason it's worth looking at these results in some detail.

The fidelity is not a metric; however, there is a simple way of turning the fidelity into a metric. The basic idea can be gleaned from Figure 9.6, by noticing that the angle between two points on the sphere is a metric. For the quantum case, Uhlmann's theorem tells us that the fidelity between two states is equal to the maximum inner product between purifications of those states. This suggests that we define the angle between states ρ and σ by

$$A(\rho, \sigma) \equiv \arccos F(\rho, \sigma). \tag{9.82}$$

Obviously the angle is non-negative, symmetric in its inputs, and is equal to zero if and only if $\rho = \sigma$. If we can show that the angle obeys the triangle inequality then we will have established that the angle is a metric.

We prove the triangle inequality using Uhlmann's theorem and some obvious facts about vectors in three dimensions. Let $|\varphi\rangle$ be a purification of σ, and choose purifications $|\psi\rangle$ of ρ and $|\gamma\rangle$ of τ such that

$$F(\rho, \sigma) = \langle \psi \mid \varphi \rangle \tag{9.83}$$
$$F(\sigma, \tau) = \langle \varphi \mid \gamma \rangle, \tag{9.84}$$

and $\langle \psi \mid \gamma \rangle$ is real and positive. (Note that this can always be done, by multiplying $|\psi\rangle, |\varphi\rangle$ and $|\gamma\rangle$ by appropriate phase factors, if necessary.) It is clear from Figure 9.6 that

$$\arccos(\langle \psi \mid \gamma \rangle) \leq A(\rho, \sigma) + A(\sigma, \tau). \tag{9.85}$$

But by Uhlmann's theorem, $F(\rho, \tau) \geq \langle \psi \mid \gamma \rangle$, so $A(\rho, \tau) \leq \arccos(\langle \psi \mid \gamma \rangle)$. Combining with the previous inequality gives the triangle inequality,

$$A(\rho, \tau) \leq A(\rho, \sigma) + A(\sigma, \tau). \tag{9.86}$$

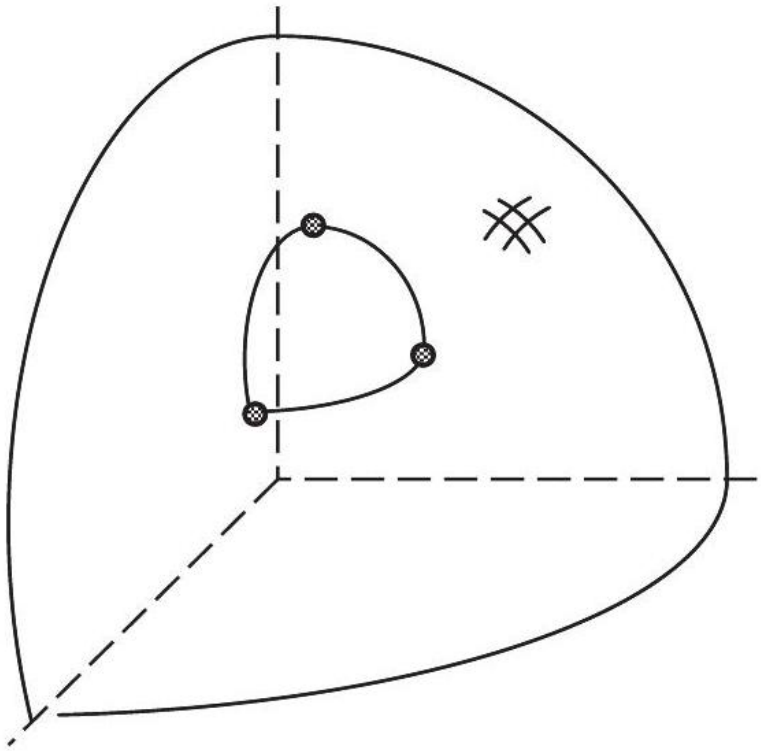


Figure 9.6. The angle between points on the surface of the unit sphere is a metric.

Exercise 9.17: Show that $0 \leq A(\rho, \sigma) \leq \pi/2$, with equality in the first inequality if and only if $\rho = \sigma$.

Qualitatively, the fidelity behaves like an 'upside-down' version of the trace distance, decreasing as two states become more distinguishable, and increasing as they become less distinguishable. Therefore, we should not expect the contractivity or non-increasing property of the trace distance to hold for fidelity. Instead, the analogous property of being non-decreasing does hold for fidelity. We will refer to this as the monotonicity of the fidelity under quantum operations.

Theorem 9.6: (Monotonicity of the fidelity) Suppose $\mathcal{E}$ is a trace-preserving quantum operation. Let ρ and σ be density operators. Show that

$$F(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \geq F(\rho, \sigma). \tag{9.87}$$

Proof

Let $|\psi\rangle$ and $|\varphi\rangle$ be purifications of ρ and σ into a joint system RQ such that $F(\rho, \sigma) = |\langle \psi \mid \varphi \rangle|$. Introduce a model environment E for the quantum operation, $\mathcal{E}$, which starts in a pure state $|0\rangle$, and interacts with the quantum system Q via a unitary interaction U. Note that $U|\psi\rangle|0\rangle$ is a purification of $\mathcal{E}(\rho)$, and $U|\varphi\rangle|0\rangle$ is a purification of $\mathcal{E}(\sigma)$. By Uhlmann's theorem it follows that

$$\begin{aligned} F(\mathcal{E}(\rho), \mathcal{E}(\sigma)) &\geq \left| \langle \psi | \langle 0 | U^\dagger U \right| \varphi \rangle \left| 0 \right\rangle \right| && (9.88) \\ &= |\langle \psi \mid \varphi \rangle| && (9.89) \\ &= F(\rho, \sigma), && (9.90) \end{aligned}$$

establishing the property we set out to prove. □

Exercise 9.18: (Contractivity of the angle) Let $\mathcal{E}$ be a trace-preserving quantum operation. Show that

$$A(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \leq A(\rho, \sigma). \tag{9.91}$$

We finish off our study of the elementary properties of fidelity by proving a result for the fidelity analogous to the strong convexity of the trace distance, using Uhlmann's theorem.

Theorem 9.7: (Strong concavity of the fidelity) Let p_i and q_i be probability distributions over the same index set, and ρ_i and σ_i density operators also indexed by the same index set. Then

$$F\left(\sum_i p_i \rho_i, \sum_i q_i \sigma_i\right) \geq \sum_i \sqrt{p_i q_i} F\left(\rho_i, \sigma_i\right). \tag{9.92}$$

Not surprisingly, this result may be used to prove concavity results for the fidelity, for which reason we dub it the strong concavity property for the fidelity. This property is not strictly analogous to the strong convexity of the trace distance; however, the similarity in spirit leads us to use similar nomenclature.

Proof

Let $|\psi_i\rangle$ and $|\varphi_i\rangle$ be purifications of ρ_i and σ_i chosen such that $F\left(\rho_i, \sigma_i\right) = \langle \psi_i \mid \varphi_i \rangle$. Introduce an ancillary system which has orthonormal basis states $|i\rangle$ corresponding to the index set i for the probability distributions. Define

$$|\psi\rangle \equiv \sum_i \sqrt{p_i} |\psi_i\rangle |i\rangle; \quad |\varphi\rangle \equiv \sum_i \sqrt{q_i} |\varphi_i\rangle |i\rangle. \tag{9.93}$$

Note that $|\psi\rangle$ is a purification of $\sum_i p_i \rho_i$ and $|\varphi\rangle$ is a purification of $\sum_i q_i \sigma_i$, so by Uhlmann's formula,

$$F\left(\sum_i p_i \rho_i, \sum_i q_i \sigma_i\right) \geq |\langle \psi \mid \varphi \rangle| = \sum_i \sqrt{p_i q_i} \langle \psi_i \mid \varphi_i \rangle = \sum_i \sqrt{p_i q_i} F\left(\rho_i, \sigma_i\right), \tag{9.94}$$

which establishes the result we set out to prove.

Exercise 9.19: (Joint concavity of fidelity) Prove that the fidelity is jointly concave,

$$F\left(\sum_i p_i \rho_i, \sum_i p_i \sigma_i\right) \geq \sum_i p_i F\left(\rho_i, \sigma_i\right). \tag{9.95}$$

Exercise 9.20: (Concavity of fidelity) Prove that the fidelity is concave in the first entry,

$$F\left(\sum_i p_i \rho_i, \sigma\right) \geq \sum_i p_i F\left(\rho_i, \sigma\right). \tag{9.96}$$

By symmetry the fidelity is also concave in the second entry.

9.2.5 9.2.3 Relationships between distance measures

The trace distance and the fidelity are closely related, despite their very different forms. Qualitatively, they may be considered to be equivalent measures of distance for many applications. In this section we quantify more precisely the relationship between trace distance and fidelity.

In the case of pure states, the trace distance and the fidelity are completely equivalent to one another. To see this, consider the trace distance between two pure states, $|a\rangle$ and $|b\rangle$. Using the Gram-Schmidt procedure we may find orthonormal states $|0\rangle$ and $|1\rangle$ such that $|a\rangle = |0\rangle$ and $|b\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$. Note that $F(|a\rangle, |b\rangle) = |\cos\theta|$. Furthermore,

$$D(|a\rangle, |b\rangle) = \frac{1}{2} \operatorname{tr} \left| \begin{bmatrix} 1 - \cos^2\theta & -\cos\theta \sin\theta \\ -\cos\theta \sin\theta & -\sin^2\theta \end{bmatrix} \right| \tag{9.97}$$

$$= |\sin\theta| \tag{9.98}$$

$$= \sqrt{1 - F(|a\rangle, |b\rangle)^2} \tag{9.99}$$

Thus the trace distance between two pure states is a function of the fidelity of those states, and vice versa. This relationship at the level of pure states can be used to deduce a relationship at the level of mixed states. Let ρ and σ be any two quantum states, and let $|\psi\rangle$ and $|\varphi\rangle$ be purifications chosen such that $F(\rho, \sigma) = |\langle\psi \mid \varphi\rangle| = F(|\psi\rangle, |\varphi\rangle)$. Recalling that trace distance is non-increasing under the partial trace, we see that

$$D(\rho, \sigma) \leq D(|\psi\rangle, |\varphi\rangle) \tag{9.100}$$

$$= \sqrt{1 - F(\rho, \sigma)^2} \tag{9.101}$$

Thus, if the fidelity between two states is close to one, it follows that the states are also close in trace distance. The converse is also true. To see this, let $\{E_m\}$ be a POVM such that

$$F(\rho, \sigma) = \sum_m \sqrt{p_m q_m} \tag{9.102}$$

where $p_m \equiv \operatorname{tr}(\rho E_m), q_m \equiv \operatorname{tr}(\sigma E_m)$ are the probabilities for obtaining outcome m for the states ρ and σ, respectively. Observe first that

$$\sum_m \left(\sqrt{p_m} - \sqrt{q_m}\right)^2 = \sum_m p_m + \sum_m q_m - 2F(\rho, \sigma) \tag{9.103}$$

$$= 2(1 - F(\rho, \sigma)). \tag{9.104}$$

However, it is also true that $\left|\sqrt{p_m} - \sqrt{q_m}\right| \leq \left|\sqrt{p_m} + \sqrt{q_m}\right|$, so

$$\sum_m \left(\sqrt{p_m} - \sqrt{q_m}\right)^2 \leq \sum_m \left|\sqrt{p_m} - \sqrt{q_m}\right| \left|\sqrt{p_m} + \sqrt{q_m}\right| \tag{9.105}$$

$$= \sum_m |p_m - q_m| \tag{9.106}$$

$$= 2D(p_m, q_m) \tag{9.107}$$

$$\leq 2D(\rho, \sigma) \tag{9.108}$$

Comparing (9.104) and (9.108) we see that

$$1 - F(\rho, \sigma) \leq D(\rho, \sigma) \tag{9.109}$$

Summarizing, we have

$$1 - F(\rho, \sigma) \leq D(\rho, \sigma) \leq \sqrt{1 - F(\rho, \sigma)^2} \tag{9.110}$$

The implication is that the trace distance and the fidelity are qualitatively equivalent measures of closeness for quantum states. Indeed, for many purposes it does not matter whether the trace distance or the fidelity is used to quantify distance, since results about one may be used to deduce equivalent results about the other.

Exercise 9.21: When comparing pure states and mixed states it is possible to make a stronger statement than (9.110) about the relationship between trace distance and fidelity. Prove that

$$1 - F(|\psi\rangle, \sigma)^2 \leq D(|\psi\rangle, \sigma) \tag{9.111}$$

9.2.6 9.3 How well does a quantum channel preserve information?

Friends come and go, but enemies accumulate

- Jones' Law, attributed to Thomas Jones

How well does a quantum channel preserve information? More precisely, suppose a quantum system is in the state $|\psi\rangle$ and some physical process occurs, changing the quantum system to the state $\mathcal{E}(|\psi\rangle\langle\psi|)$. How well has the channel $\mathcal{E}$ preserved the state $|\psi\rangle$ of the quantum system? The static measures of distance discussed in previous sections will be used in this section to develop measures of how well a quantum channel preserves information.

This type of scenario occurs often in quantum computation and quantum information. For example, in the memory of a quantum computer, $|\psi\rangle$ is the initial state of the memory, and $\mathcal{E}$ represents the dynamics that the memory undergoes, including noise processes arising from interaction with the environment. A second example is provided by a quantum communication channel for transmitting the state $|\psi\rangle$ from one location to another. No channel is ever perfect, so the action of the channel is described by a quantum operation $\mathcal{E}$.

An obvious way of quantifying how well the state $|\psi\rangle$ is preserved by the channel is to make use of the static distance measures introduced in the previous section. For example, we can compute the fidelity between the starting state $|\psi\rangle$ and the ending state $\mathcal{E}(|\psi\rangle\langle\psi|)$. For the case of the depolarizing channel, we obtain

$$F(|\psi\rangle, \mathcal{E}(|\psi\rangle\langle\psi|)) = \sqrt{\langle\psi| \left(p\frac{I}{2} + (1-p)|\psi\rangle\langle\psi| \right) |\psi\rangle} \tag{9.112}$$

$$= \sqrt{1 - \frac{p}{2}} \tag{9.113}$$

This result agrees well with our intuition - the higher the probability p of depolarizing, the lower the fidelity of the final state with the initial state. Provided p is very small the fidelity is close to one, and the state $\mathcal{E}(\rho)$ is practically indistinguishable from the initial state $|\psi\rangle$.

There is nothing special about the use of the fidelity in the above expression. We could equally well have used the trace distance. However, for the remainder of this chapter we are going to restrict ourselves to measures of distance based upon the fidelity and derived quantities. Using the properties of the trace distance established in the last section it is not difficult, for the most part, to give a parallel development based upon the trace distance. However, it turns out that the fidelity is an easier tool to calculate with, and for that reason we restrict ourselves to considerations based upon the fidelity.

Our prototype measure for information preservation, the fidelity $F(|\psi\rangle, \mathcal{E}(|\psi\rangle\langle\psi|))$, has some drawbacks which need to be remedied. In a real quantum memory or quantum communications channel, we don't know in advance what the initial state $|\psi\rangle$ of the system will be. However,

we can quantify the worst-case behavior of the system by minimizing over all possible initial states,

$$F_{\min}(\mathcal{E}) \equiv \min_{|\psi\rangle} F(|\psi\rangle, \mathcal{E}(|\psi\rangle\langle\psi|)) \tag{9.114}$$

For example, for the p-depolarizing channel $F_{\min} = \sqrt{1-p/2}$, as the fidelity of the channel is the same for all input states $|\psi\rangle$. A more interesting example is the phase damping channel,

$$\mathcal{E}(\rho) = p\rho + (1-p)Z\rho Z. \tag{9.115}$$

For the phase damping channel the fidelity is given by

$$F(|\psi\rangle, \mathcal{E}(|\psi\rangle\langle\psi|)) = \sqrt{\langle\psi|(p|\psi\rangle\langle\psi| + (1-p)Z|\psi\rangle\langle\psi|Z)|\psi\rangle} \tag{9.116}$$

$$= \sqrt{p + (1-p)\langle\psi|Z|\psi\rangle^2} \tag{9.117}$$

The second term under the square root sign is non-negative, and equal to zero when $|\psi\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. Thus for the phase damping channel the minimum fidelity is

$$F_{\min}(\mathcal{E}) = \sqrt{p} \tag{9.118}$$

You might wonder why we minimized over pure states in the definition of $F_{\min}$. After all, might not the quantum system of interest start in a mixed state ρ ? For example, a quantum memory might be entangled with the rest of the quantum computer, and therefore would start out in a mixed state. Fortunately, the joint concavity of the fidelity can be used to show that allowing mixed states does not change $F_{\min}$. To see this, suppose
that $\rho = \sum_i \lambda_i |i\rangle\langle i|$ is the initial state of the quantum system. Then we have

$$F(\rho, \mathcal{E}(\rho)) = F\left(\sum_i \lambda_i |i\rangle\langle i|, \sum_i \lambda_i \mathcal{E}(|i\rangle\langle i|)\right) \tag{9.119}$$

$$\geq \sum_i \lambda_i F(|i\rangle, \mathcal{E}(|i\rangle\langle i|)) \tag{9.120}$$

It follows that

$$F(\rho, \mathcal{E}(\rho)) \geq F(|i\rangle, \mathcal{E}(|i\rangle\langle i|)) \tag{9.121}$$

for at least one of the states $|i\rangle$, and thus $F(\rho, \mathcal{E}(\rho)) \geq F_{\min}$.
Of course, we are interested not only in protecting quantum states as they are transmitted through a quantum communications channel, but also as they dynamically undergo computation. Suppose, for example, that as part of a quantum computation we attempt to implement a quantum gate described by the unitary operator U. As described in the last chapter, any such attempt will inevitably encounter some (hopefully not too severe) noise, so the correct description of the gate is using a trace-preserving quantum operation $\mathcal{E}$. A natural measure of how successful our gate has been is the gate fidelity,

$$F(U, \mathcal{E}) \equiv \min_{|\psi\rangle} F(U|\psi\rangle, \mathcal{E}(|\psi\rangle\langle\psi|)) \tag{9.122}$$

Suppose, for example, that we try to implement a NOT gate on a single qubit, but instead implement the noisy operation $\mathcal{E}(\rho) = (1-p)X\rho X + pZ\rho Z$, for some small noise parameter p. Then the gate fidelity for this operation is given by

$$F(X,\mathcal{E}) = \min_{|\psi\rangle} \sqrt{\langle\psi|X((1-p)X|\psi\rangle\langle\psi|X + pZ|\psi\rangle\langle\psi|Z)X|\psi\rangle} \tag{9.123}$$

$$= \min_{|\psi\rangle} \sqrt{(1-p) + p\langle\psi|Y|\psi\rangle^2} \tag{9.124}$$

$$= \sqrt{(1-p)} \tag{9.125}$$

In Exercise 9.22 you will show that performing a sequence of gates each with high fidelity is sufficient to ensure that the total operation has high fidelity, and thus for the purposes of quantum computation it is sufficient to perform each gate in the computation with high fidelity. (Compare also the similar but less general arguments of Chapter 4 on approximating quantum circuits.)

Exercise 9.22: (Chaining property for fidelity measures) Suppose U and V are unitary operators, and $\mathcal{E}$ and $\mathcal{F}$ are trace-preserving quantum operations meant to approximate U and V. Letting $d(\cdot,\cdot)$ be any metric on the space of density matrices satisfying $d\left(U\rho U^\dagger, U\sigma U^\dagger\right) = d(\rho,\sigma)$ for all density matrices ρ and σ and unitary U (such as the angle $\arccos(F(\rho,\sigma))$), define the corresponding error $E(U,\mathcal{E})$ by

$$E(U,\mathcal{E}) \equiv \max_\rho d\left(U\rho U^\dagger, \mathcal{E}(\rho)\right) \tag{9.126}$$

and show that $E(VU, \mathcal{F}\circ\mathcal{E}) \leq E(U,\mathcal{E}) + E(V,\mathcal{F})$. Thus, to perform a quantum computation with high fidelity it suffices to complete each step of the computation with high fidelity.

Quantum sources of information and the entanglement fidelity

We've been talking about dynamic measures of information preservation, without defining exactly what we mean by a quantum source of information. We'll now explain two possible definitions for this notion, and use these definitions to motivate the introduction of some dynamic measures of information preservation. A priori, it is not entirely clear how best to go about defining the notion of a quantum source of information. Classically, the best solution to this definitional problem is not at all obvious, and it is possible to come up with inequivalent definitions, each yielding a rich and useful theory of information. Since quantum information contains classical information as a subfield, it should not be surprising if there are even more ways of defining the notion of an information source quantum mechanically! To conclude this chapter we introduce two possible quantum definitions for the notion of an information source, explain how they motivate corresponding distance measures for the preservation of information, and prove some elementary properties of these distance measures. Further discussion of quantum sources of information is deferred until Chapter 12.

One attractive definition for quantum sources is to imagine a stream of identical quantum systems (say, qubits) being produced by some physical process, where the states of the respective systems are given by $\rho_{X_1}, \rho_{X_2}, \ldots$, the X_j are independent and identically distributed random variables, and ρ_j is some fixed set of density operators. For example, one might imagine a stream of qubits, each of which is prepared in the state $|0\rangle$ with probability one half, or in the state $(|0\rangle + |1\rangle)/\sqrt{2}$ with probability one half.

This ensemble notion of a quantum source leads naturally to a notion of ensemble average fidelity which captures the idea that the source is well-preserved under the action of a noisy channel described by a trace-preserving quantum operation $\mathcal{E}$, namely

$$F = \sum_j p_j F\left(\rho_j, \mathcal{E}\left(\rho_j\right)\right)^2, \tag{9.127}$$

where p_j are the respective probabilities for the different possible preparations of the system ρ_j. Obviously, $0 \leq F \leq 1$, and provided $F \approx 1$ we can be confident that, on average, the channel $\mathcal{E}$ preserves the states emitted by the source with a high degree of accuracy. You may wonder why the fidelity appearing on the right hand side of the definition is squared. There are two answers to this question, one simple, and one complex. The simple answer is that including this square term makes the ensemble fidelity more naturally related to the entanglement fidelity, as defined below. The more complex answer is that quantum information is, at present, in a state of infancy and it is not entirely clear what the 'correct' definitions for notions such as information preservation are! Nevertheless, as we shall see in Chapter 12, the ensemble average fidelity and the entanglement fidelity give rise to a rich theory of quantum information, which leads us to believe that these measures are on the right track, even though a complete theory of quantum information has not yet been developed.

Exercise 9.23: Show that $\bar{F} = 1$ if and only if $\mathcal{E}(\rho_j) = \rho_j$ for all j such that $p_j > 0$.

There is a second notion of a quantum source we may consider, motivated by the idea that a channel which preserves information well is a channel that preserves entanglement well. The basic idea comes from the discussion of the classical probability of error in Section 9.1. As noted there, a direct analogue of the probability of error $p(X \neq Y)$
cannot be defined for quantum processes, for there is no direct quantum analogue of a probability distribution defined at two times. Instead, we will use a quantum analogue of the idea illustrated in Figure 9.7, which is that a dynamic measure of distance can be defined by first copying the random variable X to $\tilde{X}$, then subjecting X to noise to obtain Y, and using as our measure of distance some metric quantity $D\left[(\tilde{X}, X), \left(\tilde{X}', Y\right)\right]$ between the joint distributions for ($\tilde{X}, X$) and ($\tilde{X}', Y$).

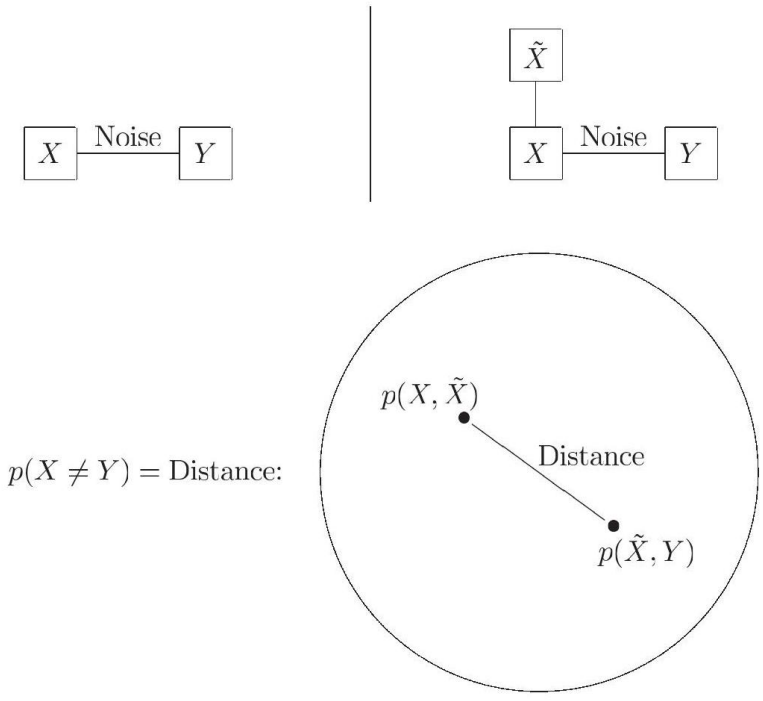


Figure 9.7. The probability of an error in the channel is equal to the trace distance between the probability distributions for ($\tilde{X}, X$) and ($\tilde{X}, Y$).}

A quantum analogue of this model is as follows. A quantum system, Q, is prepared in a state ρ. The state of Q is assumed to be entangled in some way with the external world. This

entanglement replaces the correlation between X and $\tilde{X}$ in the classical model. We represent the entanglement by introducing a fictitious system R, such that the joint state of RQ is a pure state. It turns out that all results that we prove do not depend in any way on how this purification is performed, so we may as well suppose that this is an arbitrary entanglement with the outside world. The system Q is then subjected to a dynamics described by a quantum operation, $\mathcal{E}$. The basic situation is illustrated in Figure 9.8.

How well is the entanglement between R and Q preserved by the quantum operation $\mathcal{E}$? We quantify this by the entanglement fidelity $F(\rho, \mathcal{E})$ which is a function of ρ and $\mathcal{E}$ defined for trace-preserving quantum operations $\mathcal{E}$ by

$$F(\rho, \mathcal{E}) \equiv F\left(RQ, R'Q'\right)^2 \tag{9.128}$$

$$= \langle RQ| \left[\left(\mathcal{I}_R \otimes \mathcal{E}\right)\left(|RQ\rangle\langle RQ|\right)\right] |RQ\rangle \tag{9.129}$$

where the use of a prime indicates the state of a system after the quantum operation has been applied, and the absence of a prime indicates the state of a system before the

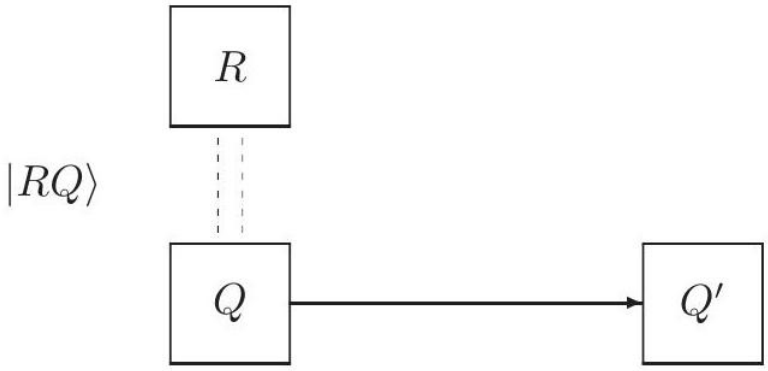


Figure 9.8. The RQ picture of a quantum channel. The initial state of RQ is a pure state.

quantum operation has been applied. The quantity appearing on the right hand side of this definition is the square of the static fidelity between the initial and final states of RQ. The use of the square of the static fidelity is purely a convenience, since it simplifies certain properties of the entanglement fidelity. Note that the entanglement fidelity depends only upon ρ and $\mathcal{E}$, and not (as it may appear) upon the details of the purification $|RQ\rangle$. To see this, we use the fact, proved in Exercise 2.81, that any two purifications $|R_1Q_1\rangle$ and $|R_2Q_2\rangle$ of ρ are related by a unitary operation, U, that acts upon R alone, $|R_2Q_2\rangle = U\,|R_1Q_1\rangle$. Thus

$$F\left(|R_2Q_2\rangle, \rho^{R_2'Q_2'}\right) = F\left(|R_1Q_1\rangle, \rho^{R_1'Q_2'}\right), \tag{9.130}$$

which establishes the result. The entanglement fidelity provides a measure of how well the entanglement between R and Q is preserved by the process $\mathcal{E}$, with values close to 1 indicating that the entanglement has been well preserved, and values close to 0 indicating that most of the entanglement has been destroyed. The choice of whether to use the static fidelity squared or the static fidelity is essentially arbitrary; the present definition results in slightly more attractive mathematical properties.

One of the attractive properties of the entanglement fidelity is that there is a very simple formula which enables it to be calculated exactly. Suppose E_i is a set of operation elements for a quantum operation $\mathcal{E}$. Then

$$F(\rho, \mathcal{E}) = \langle RQ|\rho^{R'Q'}|RQ\rangle = \sum_i \left|\langle RQ|E_i|\, RQ\right\rangle|^2 . \tag{9.131}$$

Suppose we write $|RQ\rangle = \sum_j \sqrt{p_j}|j\rangle|j\rangle$, where $\rho = \sum_j p_j|j\rangle\langle j|$. Then

$$\langle RQ|E_i|RQ\rangle = \sum_{jk} \sqrt{p_j p_k}\langle j \mid k\rangle\langle j|E_i|k\rangle \tag{9.132}$$

$$= \sum_j p_j \langle j|E_i|j\rangle \tag{9.133}$$

$$= \mathrm{tr}\left(E_i \rho\right). \tag{9.134}$$

Substituting this expression into Equation (9.131) we obtain the useful computational formula

$$F(\rho, \mathcal{E}) = \sum_i \left|\mathrm{tr}\left(\rho E_i\right)\right|^2 . \tag{9.135}$$

Thus, for example, the entanglement fidelity for the phase damping channel $\mathcal{E}(\rho) = p\rho + (1-p)Z\rho Z$ is given by

$$F(\rho, \mathcal{E}) = p|\,\mathrm{tr}(\rho)|^2 + (1-p)|\,\mathrm{tr}(\rho Z)|^2 = p + (1-p)\,\mathrm{tr}(\rho Z)^2, \tag{9.136}$$

so we see that as p decreases, the entanglement fidelity decreases, as we intuitively expect. We've defined two notions of a quantum information source and associated distance measures, one based on the idea that we want to preserve an ensemble of quantum states with high average fidelity, the other based on the idea that it is entanglement between the source and some reference system that we wish to preserve. Perhaps surprisingly, these two definitions turn out to be closely related! The reason for this lies in two useful properties of the entanglement fidelity. First, the entanglement fidelity is a lower bound on the square of the static fidelity between the input and output to the process,

$$F(\rho, \mathcal{E}) \leq \left[F(\rho, \mathcal{E}(\rho))\right]^2 \tag{9.137}$$

Intuitively, this result states that it is harder to preserve a state plus entanglement with the outside world than it is to merely preserve the state alone. The proof is an elementary application of the monotonicity of the static fidelity under partial trace, $F(\rho, \mathcal{E}) = F\left(|RQ\rangle, \rho^{R'Q'}\right)^2 \leq F\left(\rho^Q, \rho^{Q'}\right)^2$.

The second property of entanglement fidelity we need to relate it to the ensemble average definition is that it is a convex function of ρ. To see this, define $f(x) \equiv F\left(x\rho_1 + (1-x)\rho_2, \mathcal{E}\right)$, and using Equation (9.135) and elementary calculus we find

$$f''(x) = \sum_i \left|\mathrm{tr}\left(\left(\rho_1 - \rho_2\right) E_i\right)\right|^2 , \tag{9.138}$$

so that $f''(x) \geq 0$, which implies the convexity of the entanglement fidelity, as required. Combining these two results we see that

$$F\left(\sum_j p_j \rho_j, \mathcal{E}\right) \leq \sum_j p_j F\left(\rho_j, \mathcal{E}\right) \tag{9.139}$$

$$\leq \sum_j p_j F\left(\rho_j, \mathcal{E}\left(\rho_j\right)\right)^2 \tag{9.140}$$

and thus

$$F\left(\sum_j p_j \rho_j, \mathcal{E}\right) \leq \bar{F} \quad ! \tag{9.141}$$

Thus, any quantum channel $\mathcal{E}$ which does a good job of preserving the entanglement between a source described by a density operator ρ and a reference system will automatically do a good job of preserving an ensemble source described by probabilities p_j and states ρ_j such that $\rho = \sum_j p_j \rho_j$. In this sense the notion of a quantum source based on entanglement fidelity is a more stringent notion than the ensemble definition, and for this reason we will prefer the entanglement fidelity based definition in our study of quantum information theory, in Chapter 12.

We conclude the chapter with a short list of some easily proved properties of the entanglement fidelity that will be useful in later chapters:
(1) $0 \leq F(\rho, \mathcal{E}) \leq 1$. Immediate from properties of the static fidelity.
(2) The entanglement fidelity is linear in the quantum operation input. This is immediate from the definition of the entanglement fidelity.
(3) For pure state inputs, the entanglement fidelity is equal to the static fidelity squared between input and output,

$$F(|\psi\rangle, \mathcal{E}) = F(|\psi\rangle, \mathcal{E}(|\psi\rangle\langle\psi|))^2. \tag{9.142}$$

This is immediate from the observation that the state $|\psi\rangle$ is a purification of itself, and the definition of the entanglement fidelity.
(4) $F(\rho, \mathcal{E}) = 1$ if and only if for all pure states $|\psi\rangle$ in the support of ρ,

$$\mathcal{E}(|\psi\rangle\langle\psi|) = |\psi\rangle\langle\psi|. \tag{9.143}$$

To prove this, suppose $F(\rho, \mathcal{E}) = 1$, and $|\psi\rangle$ is a pure state in the support of ρ. Define $p \equiv 1/\langle\psi|\rho^{-1}|\psi\rangle > 0$ (compare Exercise 2.73 on page 105) and σ to be a density operator such that $(1-p)\sigma = \rho - p|\psi\rangle\langle\psi|$. Then by convexity,

$$1 = F(\rho, \mathcal{E}) \leq p\sqrt{F(|\psi\rangle, \mathcal{E})} + (1-p), \tag{9.144}$$

and thus $F(|\psi\rangle, \mathcal{E}) = 1$, establishing the result one way. The converse is a straightforward application of the definition of the entanglement fidelity.
(5) Suppose that $\langle\psi|\mathcal{E}(|\psi\rangle\langle\psi|)|\psi\rangle \geq 1 - \eta$ for all $|\psi\rangle$ in the support of ρ, for some η. Then $F(\rho, \mathcal{E}) \geq 1 - (3\eta/2)$. (See Problem 9.3.)

Problem 9.1: (Alternate characterization of the fidelity) Show that

$$F(\rho, \sigma) = \inf_P \operatorname{tr}(\rho P) \operatorname{tr}\left(\sigma P^{-1}\right), \tag{9.145}$$

where the infimum is taken over all invertible positive matrices P.
Problem 9.2: Let $\mathcal{E}$ be a trace-preserving quantum operation. Show that for each ρ there is a set of operation elements $\{E_i\}$ for $\mathcal{E}$ such that

$$F(\rho, \mathcal{E}) = \left|\operatorname{tr}\left(\rho E_1\right)\right|^2. \tag{9.146}$$

Problem 9.3: Prove fact (5) on this page.
Summary of Chapter 9: Distance measures for quantum information

- Trace distance: $D(\rho, \sigma) \equiv \frac{1}{2}\operatorname{tr}|\rho - \sigma|$. Doubly convex metric on density operators, contractive under quantum operations.

- Fidelity:

$$F(\rho,\sigma) \equiv \mathrm{tr}\sqrt{\rho^{1/2}\sigma\rho^{1/2}} = \max_{|\psi\rangle,|\varphi\rangle} |\langle\psi \mid \varphi\rangle|.$$

Strongly concave, $F\left(\sum_i p_i\rho_i, \sum_i q_i\sigma_i\right) \geq \sum_i \sqrt{p_i q_i} F\left(\rho_i, \sigma_i\right)$.

- Entanglement fidelity: $F(\rho, \mathcal{E})$. Measure of how well entanglement is preserved during a quantum mechanical process, starting with the state ρ of a system Q, which is assumed to be entangled with another quantum system, R, and applying the quantum operation $\mathcal{E}$ to system Q.

History and further reading

Readers wishing to learn more about distance measures for quantum information would be well advised to start with Fuchs' 1996 Ph.D. Dissertation [Fuc96]. It contains a wealth of material on distance measures for quantum information, including a list of 528 references on related topics, organized into subject areas. Notably, the proof of Equation (9.74) may be found there, as well as much else of interest. Also see the article by Fuchs and van de Graaf [FvdG99]; this paper is the origin of the inequality (9.110), and is also a good overview of distance measures for quantum information, especially in the context of quantum cryptography. The contractivity of the trace distance was proved by Ruskai[Rus94]. The monotonicity of the fidelity was proved by Barnum, Caves, Fuchs, Jozsa and Schumacher [BCF+96]. In the literature both the quantity we call fidelity and its square have been referred to as the fidelity. Uhlmann's paper [Uhl 176] in which he proves the eponymous theorem also contains an extensive discussion of the elementary properties of fidelity. The proof of Uhlmann's theorem given here is due to Jozsa [Joz 44]. Chaining properties for fidelity measures and the relation to noisy quantum computation are discussed in more detail by Aharonov, Kitaev and Nisan [AKN98]. Schumacher [Sch96 b] introduced the entanglement fidelity and proved many elementary properties. Knill and Laflamme [KL 97] established the connection between subspace fidelity and entanglement fidelity, Problem 9.3. A more detailed proof of this fact appeared in Barnum, Knill and Nielsen [BKN98]. Problem 9.1 is due to Alberti [Alb83].

9.3 10 Quantum error-correction

We have learned that it is possible to fight entanglement with entanglement. - John Preskill
To be an Error and to be Cast out is part of God's Design

- William Blake

This chapter explains how to do quantum information processing reliably in the presence of noise. The chapter covers three broad topics: the basic theory of quantum errorcorrecting codes, fault-tolerant quantum computation, and the threshold theorem. We begin by developing the basic theory of quantum error-correcting codes, which protect quantum information against noise. These codes work by encoding quantum states in a special way that make them resilient against the effects of noise, and then decoding when it is wished to recover the original state. Section 10.1 explains the basic ideas of classical error-correction, and some of the conceptual challenges that must be overcome to make quantum error-correction possible. Section 10.2 explains a simple example of a quantum error-correcting code, which we then generalize into a theory of quantum error-correcting codes in Section 10.3. Section 10.4 explains some ideas from the classical theory of linear codes, and how they give rise to an interesting class of

quantum codes known as Calderbank-Shor-Steane (CSS) codes. Section 10.5 concludes our introductory survey of quantum error-correcting codes with a discussion of stabilizer codes, a richly structured class of codes with a close connection to classical error-correcting codes.

Our discussion of quantum error-correction assumes that encoding and decoding of quantum states can be done perfectly, without error. This is useful, for example, if we wish to send quantum states over a noisy communication channel and can use almostnoiseless quantum computers to perform pretty good encoding and decoding of the states at each end of the channel. However, this assumption cannot be made if the quantum gates used to do the encoding and decoding are themselves noisy. Fortunately, the theory of fault-tolerant quantum computation, developed in Section 10.6, allows us to remove the assumption of perfect encoding and decoding. Even more impressively, fault-tolerance allow us to perform logical operations on encoded quantum states, in a manner which tolerates faults in the underlying gate operations. The chapter culminates in Section 10.6.4 with the threshold theorem for quantum computation: provided the noise in individual quantum gates is below a certain constant threshold it is possible to efficiently perform an arbitrarily large quantum computation. Of course there are caveats to this result, which we spend some time discussing. Nevertheless, the threshold theorem is a remarkable result indicating that noise likely poses no fundamental barrier to the performance of large-scale quantum computations.

9.3.1 10.1 Introduction

Noise is a great bane of information processing systems. Whenever possible we build our systems to avoid noise completely, and where that is not possible, we try to protect against the effects of noise. For example, components in modern computers are extremely reliable, with a failure rate typically below one error in 10^{17} operations. For most practical purposes we can act as if computer components are completely noiseless. On the other hand, many systems in widespread use do suffer from a substantial noise problem. Modems and CD players both make use of error-correcting codes to protect against the effects of noise. The details of the techniques used to protect against noise in practice are sometimes rather complicated, but the basic principles are easily understood. The key idea is that if we wish to protect a message against the effects of noise, then we should encode the message by adding some redundant information to the message. That way, even if some of the information in the encoded message is corrupted by noise, there will be enough redundancy in the encoded message that it is possible to recover or decode the message so that all the information in the original message is recovered.

For example, suppose we wish to send a bit from one location to another through a noisy classical communications channel. The effect of the noise in the channel is to flip the bit being transmitted with probability $p > 0$, while with probability $1 - p$ the bit is transmitted without error. Such a channel is known as a binary symmetric channel, and is illustrated in Figure 10.1. A simple means of protecting the bit against the effects of noise in the binary symmetric channel is to replace the bit we wish to protect with three copies of itself:

$$0 \rightarrow 000 \tag{10.1}$$

$$1 \rightarrow 111. \tag{10.2}$$

The bit strings 000 and 111 are sometimes referred to as the logical 0 and logical 1, since they play the role of 0 and 1 , respectively. We now send all three bits through the channel. At the receiver's end of the channel three bits are output, and the receiver has to decide what the value of the original bit was. Suppose 001 were output from the channel. Provided the probability p of a bit flip is not too high, it is very likely that the third bit was flipped by the channel, and that 0 was the bit that was sent.

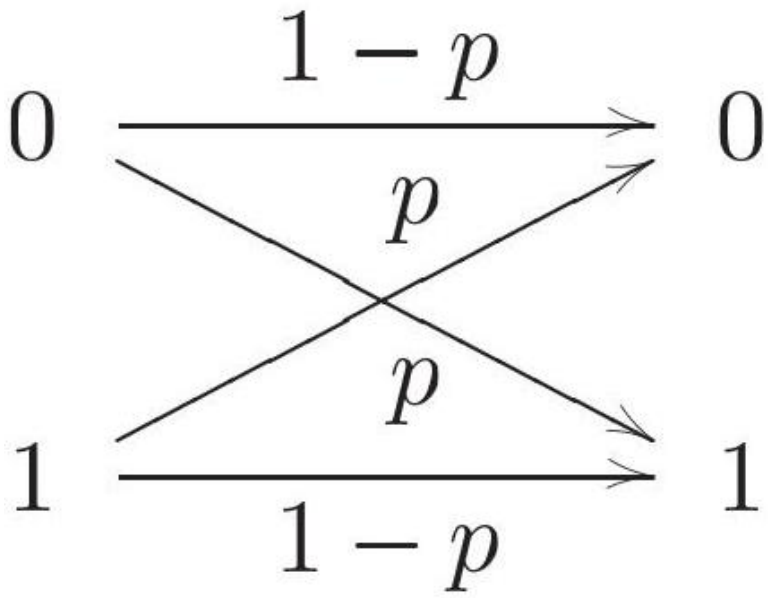


Figure 10.1. Binary symmetric channel.

This type of decoding is called majority voting, since the decoded output from the channel is whatever value, 0 or 1 , appears more times in the actual channel output. Majority voting fails if two or more of the bits sent through the channel were flipped, and succeeds otherwise. The probability that two or more of the bits are flipped is
$3p^2(1-p)+p^3$, so the probability of error is $p_{\rm e} = 3p^2 - 2p^3$. Without encoding, the probability of an error was p, so the code makes the transmission more reliable provided $p_{\rm e} < p$, which occurs whenever $p < 1/2$.

The type of code just described is called a repetition code, since we encode the message to be sent by repeating it a number of times. A similar technique has been used for millennia as a part of everyday conversation: if we're having difficulty understanding someone's spoken language, perhaps because they have a foreign accent, we ask them to repeat what they're saying. We may not catch all the words either time, but we can put the iterations together to comprehend a coherent message. Many clever techniques have been developed in the theory of classical error-correcting codes; however, the key idea is always to encode messages by adding enough redundancy that the original message is recoverable after noise has acted on the encoded message, with the amount of redundancy needing to be added depending on the severity of noise in the channel.

9.3.2 10.1.1 The three qubit bit flip code

To protect quantum states against the effects of noise we would like to develop quantum error-correcting codes based upon similar principles. There are some important differences between classical information and quantum information that require new ideas to be introduced to make such quantum error-correcting codes possible. In particular, at a first glance we have three rather formidable difficulties to deal with:

- No cloning: One might try to implement the repetition code quantum mechanically by duplicating the quantum state three or more times. This is forbidden by the no-cloning theorem discussed in Box 12.1 on page 532. Even if cloning were possible, it would not be possible to measure and compare the three quantum states output from the channel.

- Errors are continuous: A continuum of different errors may occur on a single qubit. Determining which error occurred in order to correct it would appear to require infinite precision, and therefore infinite resources.

- Measurement destroys quantum information: In classical error-correction we observe the output from the channel, and decide what decoding procedure to adopt. Observation in quantum mechanics generally destroys the quantum state under observation, and makes recovery impossible.

Fortunately, none of these problems is fatal, as we shall demonstrate. Suppose we send qubits through a channel which leaves the qubits untouched with probability $1 - p$, and flips the qubits with probability p. That is, with probability p the state $|\psi\rangle$ is taken to the state $X|\psi\rangle$, where X is the usual Pauli sigma x operator, or bit flip operator. This channel is called the bit flip channel, and we now explain the bit flip code, which may be used to protect qubits against the effects of noise from this channel.

Suppose we encode the single qubit state $a|0\rangle + b|1\rangle$ in three qubits as $a|000\rangle + b|111\rangle$. A convenient way to write this encoding is

$$|0\rangle \rightarrow |0_L\rangle \equiv |000\rangle \tag{10.3}$$
$$|1\rangle \rightarrow |1_L\rangle \equiv |111\rangle, \tag{10.4}$$

where it is understood that superpositions of basis states are taken to corresponding superpositions of encoded states. The notation $|0_L\rangle$ and $|1_L\rangle$ indicates that these are the logical $|0\rangle$ and logical $|1\rangle$ states, not the physical zero and one states. A circuit performing this encoding is illustrated in Figure 10.2.

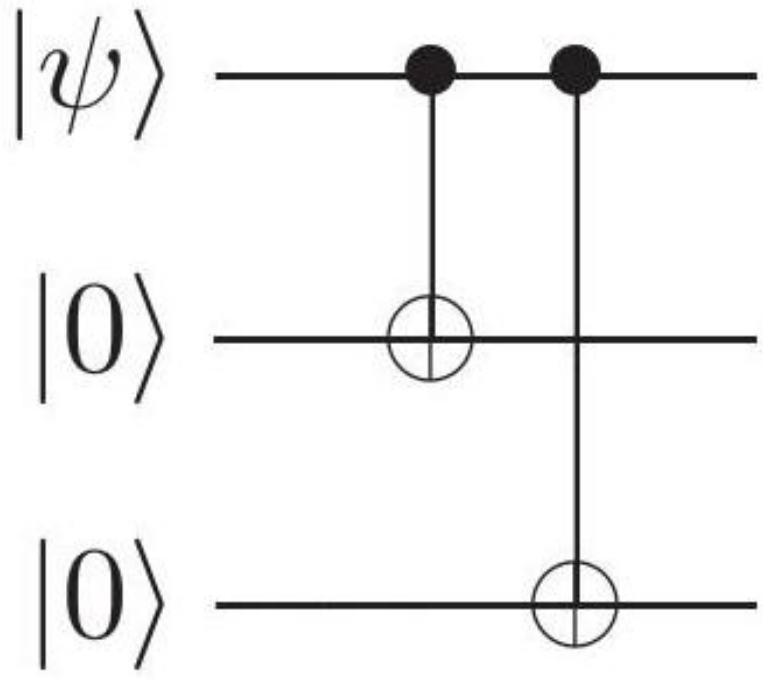


Figure 10.2. Encoding circuit for the three qubit bit flip code. The data to be encoded enters the circuit on the top line.

Exercise 10.1: Verify that the encoding circuit in Figure 10.2 works as claimed.
Suppose the initial state $a|0\rangle + b|1\rangle$ has been perfectly encoded as $a|000\rangle + b|111\rangle$. Each of the

three qubits is passed through an independent copy of the bit flip channel. Suppose a bit flip occurred on one or fewer of the qubits. There is a simple two stage error-correction procedure which can be used to recover the correct quantum state in this case:
(1) Error-detection or syndrome diagnosis: We perform a measurement which tells us what error, if any, occurred on the quantum state. The measurement result is called the error syndrome. For the bit flip channel there are four error syndromes, corresponding to the four projection operators:

$$P_0 \equiv |000\rangle\langle 000| + |111\rangle\langle 111| \text{ no error} \tag{10.5}$$
$$P_1 \equiv |100\rangle\langle 100| + |011\rangle\langle 011| \text{ bit flip on qubit one} \tag{10.6}$$
$$P_2 \equiv |010\rangle\langle 010| + |101\rangle\langle 101| \text{ bit flip on qubit two} \tag{10.7}$$
$$P_3 \equiv |001\rangle\langle 001| + |110\rangle\langle 110| \text{ bit flip on qubit three.} \tag{10.8}$$

Suppose for example that a bit flip occurs on qubit one, so the corrupted state is $a|100\rangle + b|011\rangle$. Notice that $\langle\psi|P_1|\psi\rangle = 1$ in this case, so the outcome of the measurement result (the error syndrome) is certainly 1 . Furthermore, the syndrome measurement does not cause any change to the state: it is $a|100\rangle + b|011\rangle$ both before and after syndrome measurement. Note that the syndrome contains only information about what error has occurred, and does not allow us to infer anything about the value of a or b, that is, it contains no information about the state being protected. This is a generic feature of syndrome measurements, since to obtain information about the identity of a quantum state it is in general necessary to perturb that state.
(2) Recovery: We use the value of the error syndrome to tell us what procedure to use to recover the initial state. For example, if the error syndrome was 1 , indicating a bit flip on the first qubit, then we flip that qubit again, recovering the original state $a|000\rangle + b|111\rangle$ with perfect accuracy. The four possible error syndromes and the recovery procedure in each case are: 0 (no error) - do nothing; 1 (bit flip on first qubit) - flip the first qubit again; 2 (bit flip on second qubit) - flip the second qubit
again; 3 (bit flip on third qubit) - flip the third qubit again. For each value of the error syndrome it is easy to see that the original state is recovered with perfect accuracy, given that the corresponding error occurred.

This error-correction procedure works perfectly, provided bit flips occur on one or fewer of the three qubits. This occurs with probability $(1-p)^3 + 3p(1-p)^2 = 1 - 3p^2 + 2p^3$. The probability of an error remaining uncorrected is therefore $3p^2 - 2p^3$, just as for the classical repetition code we studied earlier. Once again, provided $p < 1/2$ the encoding and decoding improve the reliability of storage of the quantum state.

Improving the error analysis

This error analysis is not completely adequate. The problem is that not all errors and states in quantum mechanics are created equal: quantum states live in a continuous space, so it is possible for some errors to corrupt a state by a tiny amount, while others mess it up completely. An extreme example is provided by the bit flip 'error' X, which does not affect the state $(|0\rangle + |1\rangle)/\sqrt{2}$ at all, but flips the $|0\rangle$ state so it becomes a $|1\rangle$. In the former case we would not be worried about a bit flip error occurring, while in the latter case we would obviously be very worried.

To address this problem we make use of the fidelity quantity introduced in Chapter 9 . Recall that the fidelity between a pure and a mixed state is given by $F(|\psi\rangle, \rho) = \sqrt{\langle\psi|\rho|\psi\rangle}$. The object of quantum error-correction is to increase the fidelity with which quantum information is stored (or communicated) up near the maximum possible fidelity of one. Let's compare the minimum

fidelity achieved by the three qubit bit flip code with the fidelity when no error-correction is performed. Suppose the quantum state of interest is $|\psi\rangle$. Without using the error-correcting code the state of the qubit after being sent through the channel is

$$\rho = (1-p)|\psi\rangle\langle\psi| + pX|\psi\rangle\langle\psi|X. \tag{10.9}$$

The fidelity is given by

$$F = \sqrt{\langle\psi|\rho|\psi\rangle} = \sqrt{(1-p) + p\langle\psi|X|\psi\rangle\langle\psi|X|\psi\rangle}. \tag{10.10}$$

The second term under the square root is non-negative, and equal to zero when $|\psi\rangle = |0\rangle$, so we see that the minimum fidelity is $F = \sqrt{1-p}$. Suppose the three qubit errorcorrecting code is used to protect the state $|\psi\rangle = a\,|0_L\rangle + b\,|1_L\rangle$. The quantum state after both the noise and error-correction is:

$$\rho = \left[(1-p)^3 + 3p(1-p)^2\right]|\psi\rangle\langle\psi| + \cdots \tag{10.11}$$

The omitted terms represent contributions from bit flips on two or three qubits. All the omitted terms are positive operators, so the fidelity we calculate will be a lower bound on the true fidelity. We see that $F = \sqrt{\langle\psi|\rho|\psi\rangle} \geq \sqrt{(1-p)^3 + 3p(1-p)^2}$. That is, the fidelity is at least $\sqrt{1-3p^2+2p^3}$, so the fidelity of storage for the quantum state is improved provided $p < 1/2$, which is the same conclusion we came to earlier based on a much cruder analysis.

Exercise 10.2: The action of the bit flip channel can be described by the quantum operation $\mathcal{E}(\rho) = (1-p)\rho + pX\rho X$. Show that this may be given an alternate operator-sum representation, as $\mathcal{E}(\rho) = (1-2p)\rho + 2pP_+\rho P_+ + 2pP_-\rho P_-$where
$P_+$and $P_-$are projectors onto the +1 and -1 eigenstates of X, $(|0\rangle + |1\rangle)/\sqrt{2}$ and $(|0\rangle - |1\rangle)/\sqrt{2}$, respectively. This latter representation can be understood as a model in which the qubit is left alone with probability $1-2p$, and is
'measured' by the environment in the $|+\rangle, |-\rangle$ basis with probability $2p$.
There is a different way of understanding the syndrome measurement that is useful in generalizing the three qubit code. Suppose that instead of measuring the four projectors P_0, P_1, P_2, P_3 we performed two measurements, the first of the observable Z_1Z_2 (that is, $Z \otimes Z \otimes I$), and the second of the observable Z_2Z_3. Each of these observables has eigenvalues ± 1, so each measurement provides a single bit of information, for a total of two bits of information - four possible syndromes, just as in the earlier description. The first measurement, of Z_1Z_2, can be thought of as comparing the first and second qubits to see if they are the same. To see why this is so, note that Z_1Z_2 has spectral decomposition

$$Z_1Z_2 = (|00\rangle\langle 00| + |11\rangle\langle 11|) \otimes I - (|01\rangle\langle 01| + |10\rangle\langle 10|) \otimes I, \tag{10.12}$$

which corresponds to a projective measurement with projectors $(|00\rangle\langle 00| + |11\rangle\langle 11|) \otimes I$ and $(|01\rangle\langle 01| + |10\rangle\langle 10|) \otimes I$. Thus, measuring Z_1Z_2 can be thought of as comparing the values of the first and second qubits, giving +1 if they are the same, and -1 if they are different. Similarly, measuring Z_2Z_3 compares the values of the second and third qubits, giving +1 if they are the same, and -1 if they are different. Combining these two measurement results we can determine whether a bit flip occurred on one of the qubits or not, and if so, which one: if both measurement results give +1 then with high probability no bit flip has occurred; if measuring Z_1Z_2 gives +1 and measuring Z_2Z_3 gives -1 then with high probability just the third qubit flipped; if measuring Z_1Z_2 gives -1 and measuring Z_2Z_3 gives +1 then with high probability just the first qubit flipped; and finally if both measurements give -1 then with high probability just the second qubit flipped. What is crucial to the success of these measurements is that neither measurement gives any information about the amplitudes a and b of the encoded

quantum state, and thus neither measurement destroys the superpositions of quantum states that we wish to preserve using the code.

Exercise 10.3: Show by explicit calculation that measuring Z_1Z_2 followed by Z_2Z_3 is equivalent, up to labeling of the measurement outcomes, to measuring the four projectors defined by (10.5)-(10.8), in the sense that both procedures result in the same measurement statistics and post-measurement states.

9.3.3 10.1.2 Three qubit phase flip code

The bit flip code is interesting, but it does not appear to be that significant an innovation over classical error-correcting codes, and leaves many problems open (for example, many kinds of errors other than bit flips can happen to qubits). A more interesting noisy quantum channel is the phase flip error model for a single qubit. In this error model the qubit is left alone with probability $1 - p$, and with probability p the relative phase of the $|0\rangle$ and $|1\rangle$ states is flipped. More precisely, the phase flip operator Z is applied to the qubit with probability $p > 0$, so the state $a|0\rangle + b|1\rangle$ is taken to the state $a|0\rangle - b|1\rangle$ under the phase flip. There is no classical equivalent to the phase flip channel, since classical channels don't have any property equivalent to phase. However, there is an easy way to turn the phase flip channel into a bit flip channel. Suppose we work in the qubit basis
$|+\rangle \equiv (|0\rangle + |1\rangle)/\sqrt{2}, |-\rangle \equiv (|0\rangle - |1\rangle)/\sqrt{2}$. With respect to this basis the operator Z takes $|+\rangle$ to $|-\rangle$ and vice versa, that is, it acts just like a bit flip with respect to the labels + and - ! This suggests using the states $|0_L\rangle \equiv |++\rangle$ and $|1_L\rangle \equiv |--\rangle$ as logical zero and one states for protection against phase flip errors. All the operations needed for error-correction - encoding, error-detection, and recovery - are performed just as for the bit flip channel, but with respect to the $|+\rangle, |-\rangle$ basis instead of the $|0\rangle, |1\rangle$ basis. To accomplish this basis change we simply apply the Hadamard gate and its inverse (also the Hadamard gate) at appropriate points in the procedure, since the Hadamard gate accomplishes the change back and forth between the $|0\rangle, |1\rangle$ basis and the $|+\rangle, |-\rangle$ basis.

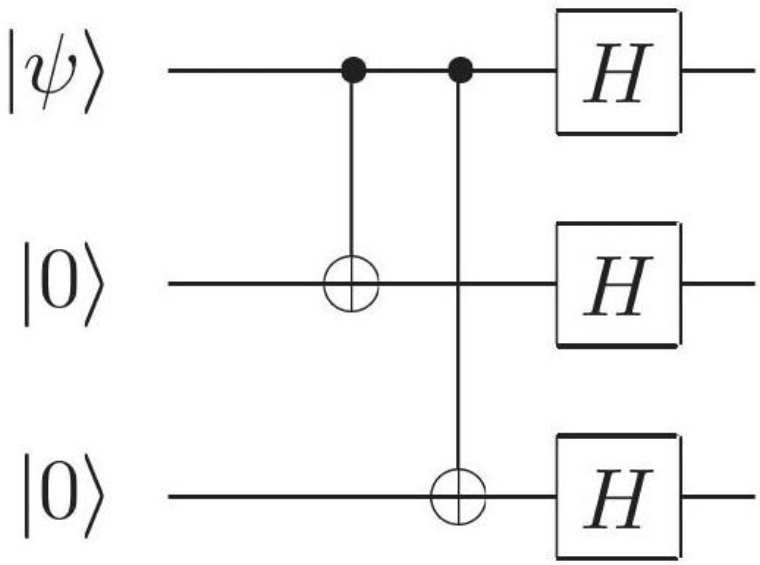


Figure 10.3. Encoding circuits for the phase flip code.

More explicitly, the encoding for the phase flip channel is performed in two steps: first, we encode in three qubits exactly as for the bit flip channel; second, we apply a Hadamard gate

to each qubit (Figure 10.3). Error-detection is achieved by applying the same projective measurements as before, but conjugated by Hadamard gates: $P_j \rightarrow P'_j \equiv H^{\otimes 3} P_j H^{\otimes 3}$. Equivalently, syndrome measurement may be performed by measuring the observables $H^{\otimes 3} Z_1 Z_2 H^{\otimes 3} = X_1 X_2$ and $H^{\otimes 3} Z_2 Z_3 H^{\otimes 3} = X_2 X_3$. It is interesting to interpret these measurements along similar lines to the measurement of $Z_1 Z_2$ and $Z_2 Z_3$ for the bit flip code. Measurement of the observables $X_1 X_2$ and $X_2 X_3$ corresponds to comparing the sign of qubits one and two, and two and three, respectively, in the sense that measurement of $X_1 X_2$, for example, gives $+1$ for states like $|+\rangle|+\rangle \otimes (\cdot)$ or $|-\rangle|-\rangle \otimes (\cdot)$, and -1 for states like $|+\rangle|-\rangle \otimes (\cdot)$ or $|-\rangle|+\rangle \otimes (\cdot)$. Finally, error-correction is completed with the recovery operation, which is the Hadamard-conjugated recovery operation from the bit flip code. For example, suppose we detected a flip in the sign of the first qubit from $|+\rangle$ to $|-\rangle$. Then we recover by applying $H X_1 H = Z_1$ to the first qubit. Similar procedures apply for other error syndromes.

Obviously this code for the phase flip channel has the same characteristics as the code for the bit flip channel. In particular, the minimum fidelity for the phase flip code is the same as that for the bit flip code, and we have the same criteria for the code producing an improvement over the case with no error-correction. We say that these two channels are unitarily equivalent, since there is a unitary operator U (in this case the Hadamard gate) such that the action of one channel is the same as the other, provided the first channel is preceded by U and followed by $U^\dagger$. These operations may be trivially incorporated into the encoding and error-correction operations. For general unitary operators these ideas are worked out in Problem 10.1 on page 495.

Exercise 10.4: Consider the three qubit bit flip code. Suppose we had performed the error syndrome measurement by measuring the eight orthogonal projectors corresponding to projections onto the eight computational basis states.
(1) Write out the projectors corresponding to this measurement, and explain how the measurement result can be used to diagnose the error syndrome: either no bits flipped or bit number j flipped, where j is in the range one to three.
(2) Show that the recovery procedure works only for computational basis states.
(3) What is the minimum fidelity for the error-correction procedure?

9.3.4 10.2 The Shor code

There is a simple quantum code which can protect against the effects of an arbitrary error on a single qubit! The code is known as the Shor code, after its inventor. The code is a combination of the three qubit phase flip and bit flip codes. We first encode the qubit using the phase flip code: $|0\rangle \rightarrow |++\!+\rangle, |1\rangle \rightarrow |--\!-\rangle$. Next, we encode each of these qubits using the three qubit bit flip code: $|+\rangle$ is encoded as $(|000\rangle + |111\rangle)\sqrt{2}$ and $|-\rangle$ is encoded as $(|000\rangle - |111\rangle)\sqrt{2}$. The result is a nine qubit code, with codewords given by:

$$\begin{aligned} |0\rangle \rightarrow |0_L\rangle &\equiv \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}} \\ |1\rangle \rightarrow |1_L\rangle &\equiv \frac{(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}}. \end{aligned} \tag{10.13}$$

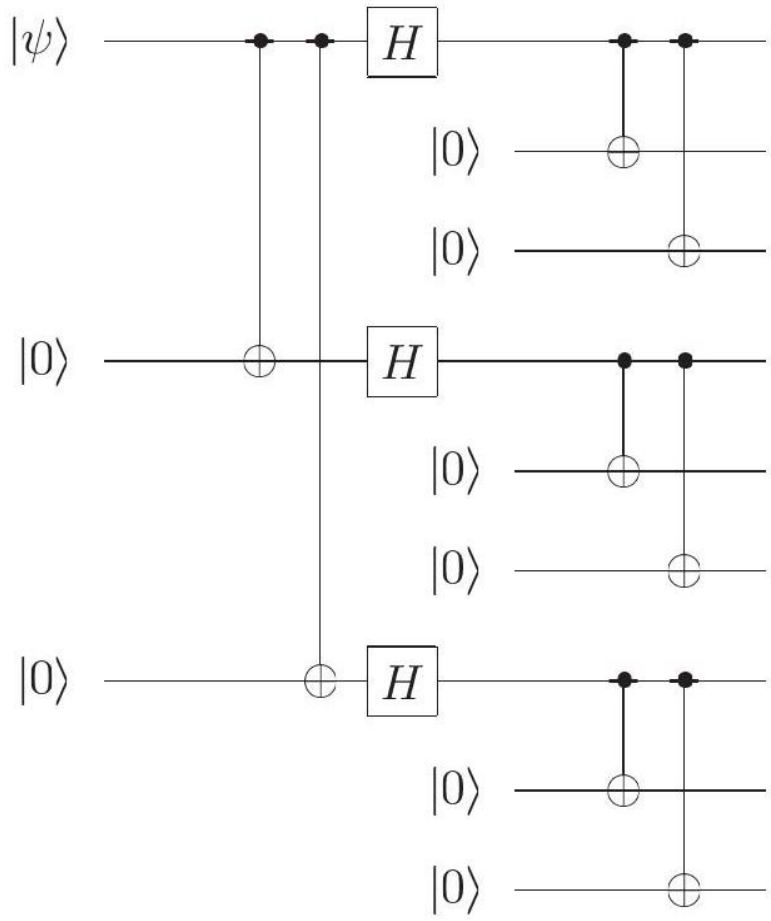


Figure 10.4. Encoding circuit for the Shor nine qubit code. Some of the $|0\rangle$ states appear indented, simply to emphasize the concatenated nature of the encoding.

The quantum circuit encoding the Shor code is shown in Figure 10.4. As described above, the first part of the circuit encodes the qubit using the three qubit phase flip code; comparison with Figure 10.3 shows that the circuits are identical. The second part of the circuit encodes each of these three qubits using the bit flip code, using three copies of the bit flip code encoding circuit, Figure 10.2. This method of encoding using a hierarchy of levels is known as concatenation. It's a great trick for obtaining new codes from old, and we use it again later to prove some important results about quantum error-correction.

The Shor code is able to protect against phase flip and bit flip errors on any qubit. To see this, suppose a bit flip occurs on the first qubit. As for the bit flip code, we perform a measurement of $Z_1 Z_2$ comparing the first two qubits, and find that they are different. We conclude that a bit flip error occurred on the first or second qubit. Next we compare the second and third qubit by performing a measurement of $Z_2 Z_3$. We find that they are the same, so it could not have been the second qubit which flipped. We conclude that the first qubit must have flipped, and recover from the error by flipping the first qubit again, back to its original state. In a similar way we can detect and recover from the effects of bit flip errors on any of the nine qubits in the code.

We cope in a similar manner with phase flips on the qubits. Suppose a phase flip occurs on the first qubit. Such a phase flip flips the sign of the first block of qubits, changing $|000\rangle + |111\rangle$ to $|000\rangle - |111\rangle$, and vice versa. Indeed, a phase flip on any of the first three qubits has this effect, and the error-correction procedure we describe works for any of these three possible errors. Syndrome measurement begins by comparing the sign of the first and second blocks of three qubits, just as syndrome measurement for the phase flip code began by comparing the

sign of the first and second qubits. For example, $(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)$ has the same sign (-) in both blocks of qubits, while $(|000\rangle - |111\rangle)(|000\rangle + |111\rangle)$ has different signs. When a phase flip occurs on any of the first three qubits we find that the signs of the first and second blocks are different. The second and final stage of syndrome measurement is to compare the sign of the second and third blocks of qubits. We find that these are the same, and conclude that the phase must have flipped in the first block of three qubits. We recover from this by flipping the sign in the first block of three qubits back to its original value. We can recover from a phase flip on any of the nine qubits in a similar manner.

Exercise 10.5: Show that the syndrome measurement for detecting phase flip errors in the Shor code corresponds to measuring the observables $X_1X_2X_3X_4X_5X_6$ and $X_4X_5X_6X_7X_8X_9$.

Exercise 10.6: Show that recovery from a phase flip on any of the first three qubits may be accomplished by applying the operator $Z_1Z_2Z_3$.

Suppose both bit and phase flip errors occur on the first qubit, that is, the operator Z_1X_1 is applied to that qubit. Then it is easy to see that the procedure for detecting a bit flip error will detect a bit flip on the first qubit, and correct it, and the procedure for detecting a phase flip error will detect a phase flip on the first block of three qubits, and correct it. Thus, the Shor code also enables the correction of combined bit and phase flip errors on a single qubit.

Indeed, the Shor code protects against much more than just bit and phase flip errors on a single qubit - we now show that it protects against completely arbitrary errors, provided they only affect a single qubit! The error can be tiny - a rotation about the z axis of the Bloch sphere by $\pi/263$ radians, say - or it can be an apparently disastrous error like removing the qubit entirely and replacing it with garbage! The interesting thing
is, no additional work needs to be done in order to protect against arbitrary errors - the procedure already described works just fine. This is an example of the extraordinary fact that the apparent continuum of errors that may occur on a single qubit can all be corrected by correcting only a discrete subset of those errors; all other possible errors being corrected automatically by this procedure! This discretization of the errors is central to why quantum error-correction works, and should be regarded in contrast to classical error-correction for analog systems, where no such discretization of errors is possible.

To simplify the analysis, suppose noise of an arbitrary type is occurring on the first qubit only; we'll come back to what happens when noise is affecting other qubits as well. Following Chapter 8 we describe the noise by a trace-preserving quantum operation $\mathcal{E}$. It is most convenient to analyze error-correction by expanding $\mathcal{E}$ in an operator-sum representation with operation elements $\{E_i\}$. Supposing the state of the encoded qubit is $|\psi\rangle = \alpha\,|0_L\rangle + \beta\,|1_L\rangle$ before the noise acts, then after the noise has acted the state is $\mathcal{E}(|\psi\rangle\langle\psi|) = \sum_i E_i|\psi\rangle\langle\psi|E_i^\dagger$. To analyze the effects of error-correction it's easiest to focus on the effect error-correction has on a single term in this sum, say $E_i|\psi\rangle\langle\psi|E_i^\dagger$. As an operator on the first qubit alone E_i may be expanded as a linear combination of the identity, I, the bit flip, X_1, the phase flip, Z_1, and the combined bit and phase flip, X_1Z_1 :

$$E_i = e_{i0}I + e_{i1}X_1 + e_{i2}Z_1 + e_{i3}X_1Z_1. \tag{10.14}$$

The (un-normalized) quantum state $E_i|\psi\rangle$ can thus be written as a superposition of four terms, $|\psi\rangle, X_1|\psi\rangle, Z_1|\psi\rangle, X_1Z_1|\psi\rangle$. Measuring the error syndrome collapses this superposition into one of the four states $|\psi\rangle, X_1|\psi\rangle, Z_1|\psi\rangle$ or $X_1Z_1|\psi\rangle$ from which recovery may then be performed by applying the appropriate inversion operation, resulting in the final state $|\psi\rangle$. The same is true for all the other operation elements E_i. Thus, errorcorrection results in the original state $|\psi\rangle$ being recovered, despite the fact that the error on the first qubit was arbitrary. This is a fundamental and deep fact about quantum error-correction, that by correcting just a discrete set of errors - the bit flip, phase flip, and combined bit-phase flip, in this example - a quantum error-correcting code is able to automatically correct an apparently much larger (continuous!)

class of errors.

What happens when noise is affecting more than just the first qubit? Two basic ideas are used to cope with this. First, in many situations it is a good approximation to assume that the noise acts on qubits independently. Provided the effect of the noise on one qubit is fairly small, we can expand the total effect of the noise as a sum over terms involving errors on no qubits, on a single qubit, on two qubits, and so on, with the terms with errors on no qubits and on a single qubit dominating the higher order terms. Performing error-correction results in the zeroth and first order terms being corrected properly, and leaves only the much smaller second and higher order errors, achieving a net suppression of error. A more detailed analysis of this idea will be given later. Sometimes, of course, it is not reasonable to assume that the noise acts on qubits independently. When this occurs we use a different idea - error-correcting codes which can correct errors on more than a single qubit. Such codes may be constructed along similar lines to the Shor code, and we explain the basic ideas behind how this can be done later in this chapter.

9.3.5 10.3 Theory of quantum error-correction

Can we construct a general theory of quantum error-correcting codes? This section develops a general framework for studying quantum error-correction, including the quantum error-correction conditions, a set of equations which must be satisfied if quantum errorcorrection is to be possible. Of course, possessing such a framework doesn't guarantee us that good quantum error-correcting codes exist - that topic is taken up in Section 10.4 on page 445! But it does provide background to enable us to find good quantum errorcorrecting codes.

The basic ideas of the theory of quantum error-correction generalize in a natural way the ideas introduced by the Shor code. Quantum states are encoded by a unitary operation into a quantum error-correcting code, formally defined as a subspace C of some larger Hilbert space. It is useful to have a notation for the projector onto the code space C, so we use the notation P; for the three qubit bit flip code $P = |000\rangle\langle 000| + |111\rangle\langle 111|$. After encoding the code is subjected to noise, following which a syndrome measurement is performed to diagnose the type of error which occurred, that is, the error syndrome. Once this has been determined, a recovery operation is performed, to return the quantum system to the original state of the code. The basic picture is illustrated in Figure 10.5: different error syndromes correspond to undeformed and orthogonal subspaces of the total Hilbert space. The subspaces must be orthogonal, otherwise they couldn't be reliably distinguished by the syndrome measurement. Furthermore, the different subspaces must be undeformed versions of the original code space, in the sense that the errors mapping to the different subspaces must take the (orthogonal) codewords to orthogonal states, in order to be able to recover from the error. This intuitive picture is essentially the content of the quantum error-correction conditions discussed below.

To develop a general theory of quantum error-correction it behooves us to make as few assumptions as possible about the nature of noise and about the procedure used to do the error-correction. That is, we won't necessarily assume that the error-correction is done via a two-stage detection-recovery method, and we won't make any assumptions about the noise occurring for qubit systems, or being weak. Instead, we just make two very broad assumptions: the noise is described by a quantum operation $\mathcal{E}$, and the complete error-correction procedure is effected by a trace-preserving quantum operation $\mathcal{R}$, which we call the error-correction operation. This error-correction operation bundles into one piece the two steps that we have called error-detection and recovery above. In order for error-correction to be deemed successful, we require that for any state ρ whose support lies in the code C,

$$(\mathcal{R} \circ \mathcal{E})(\rho) \propto \rho. \tag{10.15}$$

You may be wondering why we wrote $\propto$ rather than $=$ in the last equation. If $\mathcal{E}$ were a trace-preserving quantum operation then by taking traces of both sides of the equation we see that $\propto$ would be $=$. However, sometimes we may be interested in error-correcting non-trace-preserving operations $\mathcal{E}$, such as measurements, for which $\propto$ is appropriate. Of course, the error-correction step $\mathcal{R}$ must succeed with probability 1 , which is why we required $\mathcal{R}$ to be trace-preserving.

The quantum error-correction conditions are a simple set of equations which can be checked to determine whether a quantum error-correcting code protects against a particular type of noise $\mathcal{E}$. We will use these conditions to construct a plethora of quantum

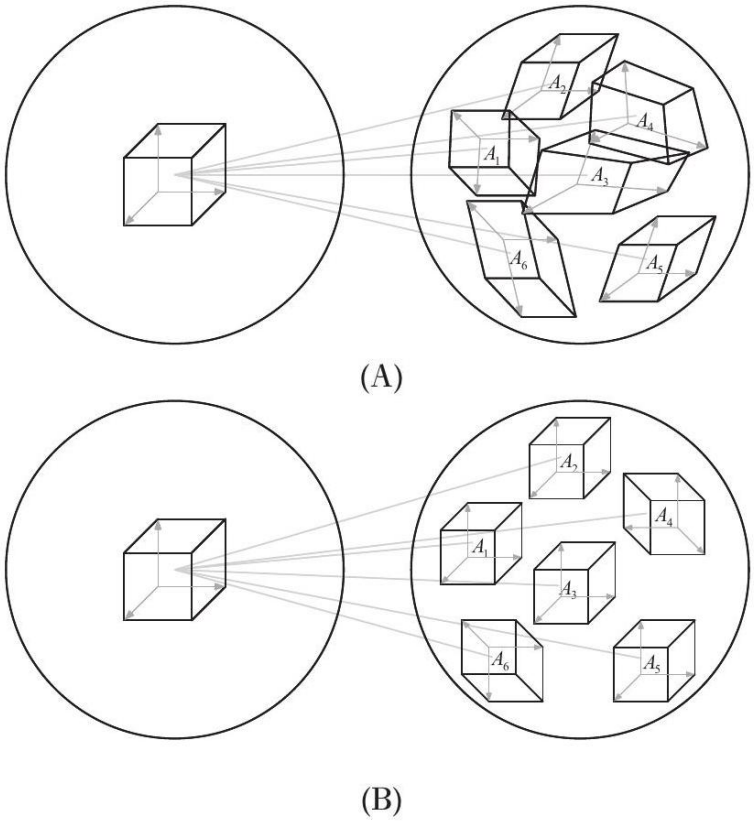


Figure 10.5. The packing of Hilbert spaces in quantum coding: (A) bad code, with non-orthogonal, deformed resultant spaces, and (B) good code, with orthogonal (distinguishable), undeformed spaces.

codes, and also to investigate some of the general properties of quantum error-correcting codes.

Theorem 10.1: (Quantum error-correction conditions) Let C be a quantum code, and let P be the projector onto C. Suppose $\mathcal{E}$ is a quantum operation with operation elements $\{E_i\}$. A necessary and sufficient condition for the existence of an error-correction operation $\mathcal{R}$ correcting $\mathcal{E}$ on C is that

$$PE_i^\dagger E_j P = \alpha_{ij} P, \tag{10.16}$$

for some Hermitian matrix α of complex numbers.
We call the operation elements $\{E_i\}$ for the noise $\mathcal{E}$ errors, and if such an $\mathcal{R}$ exists we say that $\{E_i\}$ constitutes a correctable set of errors.

Proof

We prove sufficiency first, by constructing an explicit error-correction operation $\mathcal{R}$ whenever (10.16) is satisfied. The construction we use is of the two-part form used for the Shor code - error-detection and then recovery - so the proof also shows that error-correction can always be accomplished using such a two-part procedure. Suppose $\{E_i\}$ is a set of operation elements satisfying the quantum error-correction conditions, (10.16). By assumption α is a Hermitian matrix, and thus can be diagonalized, $d = u^\dagger \alpha u$, where u is a unitary matrix and d is diagonal. Define operators $F_k \equiv \sum_i u_{ik} E_i$. Recalling Theorem 8.2 , we see that $\{F_k\}$ is also a set of operation elements for $\mathcal{E}$. By direct substitution,

$$PF_k^\dagger F_l P = \sum_{ij} u_{ki}^\dagger u_{jl} P E_i^\dagger E_j P \tag{10.17}$$

Substituting (10.16) simplifies this to $PF_k^\dagger F_l P = \sum_{ij} u_{ki}^\dagger \alpha_{ij} u_{jl} P$ and since $d = u^\dagger \alpha u$ we obtain

$$PF_k^\dagger F_l P = d_{kl} P \tag{10.18}$$

which can be thought of as a simplification of the quantum error-correction conditions (10.16), because d_{kl} is diagonal.

We use the simplified conditions (10.18) and the polar decomposition (Section 2.1.10 on page 78) to define the syndrome measurement. From the polar decomposition, we see that $F_k P = U_k \sqrt{P F_k^\dagger F_k P} = \sqrt{d_{kk}} U_k P$ for some unitary U_k. The effect of F_k is therefore to rotate the coding subspace into the subspace defined by the projector $P_k \equiv U_k P U_k^\dagger = F_k P U_k^\dagger / \sqrt{d_{kk}}$. Equation (10.18) implies that these subspaces are orthogonal, since when $k \neq l$,

$$P_l P_k = P_l^\dagger P_k = \frac{U_l P F_l^\dagger F_k P U_k^\dagger}{\sqrt{d_{ll} d_{kk}}} = 0 \tag{10.19}$$

The syndrome measurement is a projective measurement defined by the projectors P_k, augmented by an additional projector if necessary to satisfy the completeness relation $\sum_k P_k = I$. Recovery is accomplished simply by applying $U_k^\dagger$. To see that this errorcorrection procedure works, note that the combined detection-recovery step corresponds to the quantum operation $\mathcal{R}(\sigma) = \sum_k U_k^\dagger P_k \sigma P_k U_k$. For states ρ in the code, simple algebra and the definitions show that:

$$\begin{aligned} U_k^\dagger P_k F_l \sqrt{\rho} &= U_k^\dagger P_k^\dagger F_l P \sqrt{\rho} && (10.20)\\ &= \frac{U_k^\dagger U_k P F_k^\dagger F_l P \sqrt{\rho}}{\sqrt{d_{kk}}} && (10.21)\\ &= \delta_{kl} \sqrt{d_{kk}} P \sqrt{\rho} && (10.22)\\ &= \delta_{kl} \sqrt{d_{kk}} \sqrt{\rho}. && (10.23) \end{aligned}$$

Thus

$$\begin{aligned} \mathcal{R}(\mathcal{E}(\rho)) &= \sum_{kl} U_k^\dagger P_k F_l \rho F_l^\dagger P_k U_k && (10.24)\\ &= \sum_{kl} \delta_{kl} d_{kk} \rho && (10.25)\\ &\propto \rho, && (10.26) \end{aligned}$$

as required.

To prove necessity of the quantum error-correction conditions (10.16), suppose $\{E_i\}$ is a set of errors which is perfectly correctable by an error-correction operation $\mathcal{R}$ with operation elements $\{R_j\}$. Define a quantum operation $\mathcal{E}_C$ by $\mathcal{E}_C(\rho) \equiv \mathcal{E}(P\rho P)$. Since $P\rho P$ is in the code space for all ρ, it follows that

$$\mathcal{R}\left(\mathcal{E}_C(\rho)\right) \propto P\rho P \tag{10.27}$$

for all states ρ. Moreover, the proportionality factor must be a constant c, not depending on ρ, if both right and left hand sides are to be linear. Rewriting the last equation explicitly in terms of the operation elements gives

$$\sum_{ij} R_j E_i P \rho P E_i^\dagger R_j^\dagger = cP\rho P \tag{10.28}$$

This equation holds for all ρ. It follows that the quantum operation with operation elements $\{R_j E_i\}$ is identical to the quantum operation with a single operation element $\sqrt{c}P$. Theorem 8.2 implies that there exist complex numbers c_{ki} such that

$$R_k E_i P = c_{ki} P \tag{10.29}$$

Taking the adjoint of this equation gives $PE_i^\dagger R_k^\dagger = c_{ki}^* P$ and therefore $PE_i^\dagger R_k^\dagger R_k E_j P = c_{ki}^* c_{kj} P$. But $\mathcal{R}$ is a trace-preserving operation, so $\sum_k R_k^\dagger R_k = I$. Summing the equation $PE_i^\dagger R_k^\dagger R_k E_j P = c_{ki}^* c_{kj} P$ over k we deduce that

$$PE_i^\dagger E_j P = \alpha_{ij} P \tag{10.30}$$

where $\alpha_{ij} \equiv \sum_k c_{ki}^* c_{kj}$ is just a Hermitian matrix of complex numbers. These are the quantum error-correction conditions.

Direct verification of the quantum error-correction conditions is an easy but timeconsuming task. In Sections 10.4 and 10.5 we describe a theoretical formalism which uses the quantum error-correction conditions as a launching point for the construction of many interesting classes of codes, and which circumvents much of the difficulty associated with verifying the quantum error-correction conditions directly. For now, you should work through the following example, which demonstrates the quantum error-correction conditions in action:

Exercise 10.7: Consider the three qubit bit flip code of Section 10.1.1, with corresponding projector $P = |000\rangle\langle 000| + |111\rangle\langle 111|$. The noise process this code protects against has operation elements $\left\{\sqrt{(1-p)^3}I, \sqrt{p(1-p)^2}X_1, \sqrt{p(1-p)^2}X_2, \sqrt{p(1-p)^2}X_3\right\}$, where p is the probability that a bit flips. Note that this quantum operation is not trace-preserving, since we have omitted operation elements corresponding to bit flips on two and three qubits. Verify the quantum error-correction conditions for this code and noise process.

9.3.6 10.3.1 Discretization of the errors

We have discussed the protection of quantum information against a specific noise process $\mathcal{E}$. In general, however, we don't know exactly what noise is afflicting a quantum system. It would be useful if a specific code C and error-correction operation $\mathcal{R}$ could be used to protect against an entire class of noise processes. Fortunately, the quantum errorcorrection conditions are easily adapted to provide exactly this sort of protection.

Theorem 10.2: Suppose C is a quantum code and $\mathcal{R}$ is the error-correction operation constructed in the proof of Theorem 10.1 to recover from a noise process $\mathcal{E}$ with operation elements

$\{E_i\}$. Suppose $\mathcal{F}$ is a quantum operation with operation elements $\{F_j\}$ which are linear combinations of the E_i, that is $F_j = \sum_i m_{ji} E_i$ for some matrix m_{ji} of complex numbers. Then the error-correction operation $\mathcal{R}$ also corrects for the effects of the noise process $\mathcal{F}$ on the code C.

Box 10.1: Quantum error-correction without measurement

In the main text we have described quantum error-correction as a two stage process: an error-detection step effected using quantum measurement, followed by a recovery step effected using conditioned unitary operations. It is possible to perform quantum error-correction using only unitary operations and ancilla systems prepared in standard states. The advantage of knowing how to do this is that for some real-world quantum systems it is very difficult to perform the quantum measurements needed for quantum error-correction, so an alternate procedure is needed. The techniques we use to do that are essentially the same as those described in Chapter 8 for mocking up an arbitrary quantum operation; we now recap the basic idea in the context of quantum error-correction.

Suppose the syndrome measurement on the principal system - the one being errorcorrected - is described by measurement operators M_i, and the corresponding conditional unitary operation is U_i. Introduce an ancilla system with basis states $|i\rangle$ corresponding to the possible error syndromes. The ancilla starts in a standard pure state $|0\rangle$ before error-correction. Define a unitary operator U on the principal system plus ancilla by

$$U|\psi\rangle|0\rangle \equiv \sum_i \left(U_i M_i |\psi\rangle\right)|i\rangle. \tag{10.31}$$

This can be extended to a unitary operator acting on the whole space since

$$\langle\varphi|\langle 0|U^\dagger U|\psi\rangle|0\rangle = \sum_{ij} \langle\varphi|M_i^\dagger M_j|\psi\rangle \delta_{ij} \tag{10.32}$$

$$= \sum_i \langle\varphi|M_i^\dagger M_i|\psi\rangle \tag{10.33}$$

$$= \langle\varphi \mid \psi\rangle. \tag{10.34}$$

That is, U preserves inner products, and can thus be extended to a unitary operator on the entire state space. The effect of U is to effect the transformation $\mathcal{R}(\sigma) = \sum_i U_i M_i \sigma M_i^\dagger U_i^\dagger$ on the system being error-corrected, exactly the same quantum operation as described in the main text for the performance of quantum errorcorrection. Note that in order for this error-correction procedure to work it is necessary to use a fresh ancilla each time error-correction is performed.

Proof

By Theorem 10.1 the operation elements $\{E_i\}$ must satisfy the quantum error-correction conditions, $PE_i E_j^\dagger P = \alpha_{ij} P$. As shown in the proof of Theorem 10.1, without loss of generality we may assume that the operation elements for $\mathcal{E}$ have been chosen such that $\alpha_{ij} = d_{ij}$ is diagonal with real entries. The error-correction operation $\mathcal{R}$ has operation elements $U_k^\dagger P_k$, where by Equation (10.23) the U_k and P_k are chosen such that for any ρ in the code space:

$$U_k^\dagger P_k E_i \sqrt{\rho} = \delta_{ki} \sqrt{d_{kk}} \sqrt{\rho}. \tag{10.35}$$

Substituting $F_j = \sum_i m_{ji} E_i$ gives

$$U_k^\dagger P_k F_j \sqrt{\rho} = \sum_i m_{ji} \delta_{ki} \sqrt{d_{kk}} \sqrt{\rho} \tag{10.36}$$

$$= m_{jk} \sqrt{d_{kk}} \sqrt{\rho} \tag{10.37}$$

and thus

$$\mathcal{R}(\mathcal{F}(\rho)) = \sum_{kj} U_k^\dagger P_k F_j \rho F_j^\dagger P_k U_k \tag{10.38}$$

$$= \sum_{kj} |m_{jk}|^2 d_{kk} \rho \tag{10.39}$$

$$\propto \rho \tag{10.40}$$

as required.

This result enables the introduction of a more powerful language to describe quantum error-correcting codes. Instead of talking about the class of error processes $\mathcal{E}$ correctable by a code C and error-correction operation $\mathcal{R}$ we can talk about a set of error operators (or simply errors) $\{E_i\}$ which are correctable. By this, we mean that the quantum errorcorrection conditions hold for these operators,

$$P E_i E_j^\dagger P = \alpha_{ij} P \tag{10.41}$$

Theorems 10.1 and 10.2 together imply that any noise process $\mathcal{E}$ whose operation elements are built from linear combinations of these error operators $\{E_i\}$ will be corrected by the recovery operation $\mathcal{R}$!

Let's look at an example of this powerful new viewpoint in action. Suppose $\mathcal{E}$ is a quantum operation acting on a single qubit. Then its operation elements $\{E_i\}$ can each be written as a linear combination of the Pauli matrices $\sigma_0, \sigma_1, \sigma_2, \sigma_3$. Therefore, to check that the Shor code corrects against arbitrary single qubit errors on the first qubit it is sufficient to verify that the equations

$$P \sigma_i^1 \sigma_j^1 P = \alpha_{ij} P \tag{10.42}$$

are satisfied, where σ_i^1 are the Pauli matrices (I, X, Y and Z) acting on the first qubit. Once this is done it is assured that any error process whatsoever on the first qubit may be corrected! (The actual calculation is quite simple, and is done as part of Exercise 10.10.) Indeed this example explains a point that can be somewhat mysterious when first confronted with the literature on quantum error-correction: many authors have what appears to be a suspicious fondness for the depolarizing channel, $\mathcal{E}(\rho) = (1-p)\rho + \frac{p}{3}(X\rho X + Y\rho Y + Z\rho Z)$. It is tempting to assume that this greatly limits the validity of their models of error-correction, but this is not so, for as the discussion just now implies, the ability to error-correct the depolarizing channel automatically implies the ability to error-correct an arbitrary single qubit quantum operation.

Summarizing, we have learnt that it is possible to discretize quantum errors, that to fight the continuum of errors possible on a single qubit it is sufficient merely to win the war against a finite set of errors, the four Pauli matrices. Similar results hold for higherdimensional quantum systems. This stands in remarkable contrast to the theory of errorcorrection for analog classical systems. Error-correction in such systems is extremely difficult because in principle there are an infinite number of different error syndromes.

Digital error-correction for classical information processing is much more successful because it involves only a finite number of error syndromes. The surprising thing we have learnt is that quantum error-correction seems much more similar to classical digital error-correction than it is to classical analog error-correction.

Exercise 10.8: Verify that the three qubit phase flip code $|0_L\rangle = |++\!+\rangle, |1_L\rangle = |--\!-\rangle$ satisfies the quantum error-correction conditions for the set of error operators $\{I, Z_1, Z_2, Z_3\}$.

Exercise 10.9: Again, consider the three qubit phase flip code. Let P_i and Q_i be the projectors onto the $|0\rangle$ and $|1\rangle$ states, respectively, of the i th qubit. Prove that the three qubit phase flip code protects against the error set $\{I, P_1, Q_1, P_2, Q_2, P_3, Q_3\}$.

Exercise 10.10: Explicitly verify the quantum error-correction conditions for the Shor code, for the error set containing I and the error operators X_j, Y_j, Z_j for $j = 1$ through 9.

Exercise 10.11: Construct operation elements for a single qubit quantum operation $\mathcal{E}$ that upon input of any state ρ replaces it with the completely randomized state $I/2$. It is amazing that even such noise models as this may be corrected by codes such as the Shor code!

9.3.7 10.3.2 Independent error models

How can we make the connection between quantum error-correction and the criteria for doing reliable quantum information processing introduced in Chapter 9? In this section we explain the basic idea of how this may be done using the assumption of independent errors on different qubits. Intuitively, if a noise process acts independently on the different qubits in the code, then provided the noise is sufficiently weak error-correction should improve the storage fidelity of the encoded state over the unencoded state. To illustrate this, we begin with the example of the depolarizing channel, which provides an especially simple demonstration of the basic ideas, and then broaden the ideas to include other important channels.

Recall that the depolarizing channel may be described by a single parameter, a probability p. The action of the depolarizing channel on a single qubit is defined by the equation $\mathcal{E}(\rho) = (1-p)\rho + p/3[X\rho X + Y\rho Y + Z\rho Z]$, and can be interpreted as saying that nothing happens to the qubit with probability $1-p$, and each of the operators X, Y and Z is applied to the qubit with probability $p/3$. The depolarizing channel is especially easy to analyze in the context of quantum error-correction because it has such a nice interpretation in terms of the four basic errors I, X, Y and Z which are most commonly used in the analysis of quantum codes. We'll explain how this analysis is performed, and then return to the question of what happens when we consider a process which doesn't have such a simple interpretation in terms of the I, X, Y and Z operations. A simple calculation shows that the minimum fidelity for states sent through a depolarizing channel is given by $F = \sqrt{1-2p/3} = 1 - p/3 + O(p^2)$.

Exercise 10.12: Show that the fidelity between the state $|0\rangle$ and $\mathcal{E}(|0\rangle\langle 0|)$ is $\sqrt{1-2p/3}$, and use this to argue that the minimum fidelity for the depolarizing channel is $\sqrt{1-2p/3}$.

Suppose we encode a single qubit of information in an n qubit quantum code which corrects errors on any single qubit. Suppose the depolarizing channel with parameter p acts independently on each of the qubits, giving rise to a joint action on all n qubits of

$$\mathcal{E}^{\otimes n}(\rho) = (1-p)^n \rho + \sum_{j=1}^{n} \sum_{k=1}^{3} (1-p)^{n-1} \frac{p}{3} \sigma_k^j \rho \sigma_k^j + \cdots \tag{10.43}$$

where the '...' indicates higher-order terms which are positive and will drop out of the analysis. After error-correction has been performed all terms appearing in this sum will be returned to the state ρ, provided ρ was in the code originally,

$$\left(\mathcal{R} \otimes \mathcal{E}^{\otimes n}\right)(\rho) = \left[(1-p)^n + n(1-p)^{n-1} p\right] \rho + \cdots, \tag{10.44}$$

so the fidelity satisfies

$$F \geq \sqrt{(1-p)^{n-1}(1-p+np)} = 1 - \frac{\binom{n}{2}}{2}p^2 + O\left(p^3\right) \tag{10.45}$$

Thus, provided the probability of error p is sufficiently small, using the quantum errorcorrecting code leads to an improvement in the fidelity of the quantum states being protected by the code.

Not all noisy channels can be interpreted so easily as a random combination of no error, bit flips, phase flips and combinations of the two. Many naturally occurring quantum channels have no such interpretation. Consider the example of amplitude damping (Section 8.3.5), which has operation elements E_0 and E_1 :

$$E_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix}; \quad E_1 = \begin{bmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{bmatrix}. \tag{10.46}$$

The parameter γ is a small positive parameter characterizing the strength of the amplitude damping process - as γ gets closer to zero, the strength decreases, until ultimately we end up with an essentially noise-free quantum channel. We might reasonably guess that the amplitude damping channel has an equivalent description in terms of a set of operation elements including a term proportional to the identity, $\{f(\gamma)I, E_1', E_2', \ldots\}$, where $f(\gamma) \rightarrow 1$ as $\gamma \rightarrow 0$. If this were the case then an analysis of error-correction for the amplitude damping channel acting independently on multiple qubits could be done that was similar to the analysis of error-correction performed for the depolarizing channel. Surprisingly, it turns out that no such description is possible! This follows from Theorem 8.2 simply because for $\gamma > 0$ no linear combination of E_0 and E_1 can ever be proportional to the identity, and thus no set of operation elements for the amplitude damping channel can ever include a term proportional to the identity.

Similarly, many other noise processes in quantum mechanics are close to the identity in a physical sense, yet no operator-sum representation for the process contains a large identity component. Intuitively it seems reasonable that in such a circumstance errorcorrection should result in a net gain in the storage fidelity for quantum information, provided the noise is sufficiently weak. We will now show that this is in fact the case, using the specific example of the amplitude damping channel for concreteness. A simple calculation shows that the minimum fidelity for the amplitude damping channel applied
to a single qubit is $\sqrt{1-\gamma}$. Suppose the qubit is encoded in an n qubit quantum code capable of correcting arbitrary errors on a single qubit, and that amplitude damping channels of parameter γ act independently on each qubit. We will sketch the basic idea showing that the effect of quantum error-correction is to change the fidelity of storage to $1-O\left(\gamma^2\right)$, so for small γ encoding the qubit in the quantum code results in a net suppression of error.

Exercise 10.13: Show that the minimum fidelity $F(|\psi\rangle, \mathcal{E}(|\psi\rangle\langle\psi|))$ when $\mathcal{E}$ is the amplitude damping channel with parameter γ, is $\sqrt{1-\gamma}$.

Using $E_{j,k}$ to denote the action of E_j on the k th qubit, the effect of the noise on the encoded qubits may be written:

$$\begin{aligned} \mathcal{E}^{\otimes n}(\rho) = (E_{0,1} \otimes E_{0,2} \otimes \cdots \otimes E_{0,n})\, \rho \left(E_{0,1}^\dagger \otimes E_{0,2}^\dagger \otimes \cdots \otimes E_{0,n}^\dagger\right) \\ + \sum_{j=1}^{n} \left[E_{1,j} \otimes \left(\bigotimes_{k \neq j} E_{0,k}\right)\right] \rho \left[E_{1,j}^\dagger \otimes \left(\bigotimes_{k \neq j}\right.\right. \\ + O\left(\gamma^2\right). \end{aligned} \tag{10.47}$$

Suppose we write $E_0 = (1-\gamma/4)I + \gamma Z/4 + O\left(\gamma^2\right)$, and $E_1 = \sqrt{\gamma}(X+iY)/2$. Substituting these expressions in (10.47) gives

$$\mathcal{E}^{\otimes n}(\rho) = \left(1-\frac{\gamma}{4}\right)^{2n}\rho + \frac{\gamma}{4}\left(1-\frac{\gamma}{4}\right)^{2n-1}\sum_{j=1}^{n}\left(Z_j\rho+\rho Z_j\right)$$
$$+\frac{\gamma}{4}\left(1-\frac{\gamma}{4}\right)^{2n-2}\sum_{j=1}^{n}\left(X_j+iY_j\right)\rho\left(X_j-iY_j\right)+O\left(\gamma^2\right). \quad (10.48)$$

Suppose ρ is a state of the code. Obviously, the effect of error-correction on ρ is to leave it invariant! The effect of error-correction on terms like $Z_j\rho$ and ρZ_j is most easily understood by considering the effect on $Z_j|\psi\rangle\langle\psi|$, where $|\psi\rangle$ is a state of the code. We suppose the code is such that the error Z_j takes $|\psi\rangle$ to a subspace which is orthogonal to the code, so that when the syndrome measurement is performed terms like $Z_j|\psi\rangle\langle\psi|$ disappear. (Note that even if this orthogonality assumption is not made a similar analysis can still be made, by working in terms of error operators which do take the code to orthogonal subspaces.) Thus terms like $Z_j\rho$ vanish after error-correction, as do terms like $\rho Z_j, X_j\rho Y_j$ and $Y_j\rho X_j$. Furthermore, error-correction takes $X_j\rho X_j$ and $Y_j\rho Y_j$ back to ρ, since the code can correct errors on one qubit. Thus, after error-correction the state of the system is

$$\left(1-\frac{\gamma}{4}\right)^{2n}\rho + 2n\frac{\gamma}{4}\left(1-\frac{\gamma}{4}\right)^{2n-2}\rho + O\left(\gamma^2\right) = \rho + O\left(\gamma^2\right). \quad (10.49)$$

Thus, to order γ^2 error-correction returns the quantum system to its original state ρ, and for weak noise (small γ) error-correction results in a net suppression of errors, just as for the depolarizing channel. Our analysis here was for the amplitude damping noise model, but it is not difficult to generalize this argument to obtain similar conclusions for other noise models. In general, however, for the remainder of this chapter we work mainly with noise models which can be understood as stochastic application of errors corresponding
to the Pauli matrices, similar to the depolarizing channel, allowing us to do the analysis using familiar concepts from classical probability theory. Keep in mind that the ideas we describe can be extended beyond this simple error model to apply to a much wider range of error models using principles similar to those we have just outlined.

9.3.8 10.3.3 Degenerate codes

In many respects quantum error-correcting codes are quite similar to classical codes - an error is identified by measuring the error syndrome, and then corrected as appropriate, just as in the classical case. There is, however, an interesting class of quantum codes known as degenerate codes possessing a striking property unknown in classical codes. The idea is most easily illustrated for the case of the Shor code. Consider the effect of the errors Z_1 and Z_2 on the codewords for the Shor code. As we have already noted, the effect of these errors is the same on both codewords. For classical error-correcting codes errors on different bits necessarily lead to different corrupted codewords. The phenomenon of degenerate quantum codes is a sort of good news-bad news situation for quantum codes. The bad news is that some of the proof techniques used classically to prove bounds on error-correction fall down because they can't be applied to degenerate codes. We'll see an example of this in the next section and the quantum Hamming bound. The good news is that degenerate quantum codes seem to be among the most interesting quantum codes! In some sense they are able to 'pack more information in' than are classical codes, because distinct errors do not necessarily have to take the code space to orthogonal spaces, and it is possible (though has not yet been shown) that this extra ability may lead to degenerate codes that can store quantum information more efficiently than any non-degenerate code.

9.3.9 10.3.4 The quantum Hamming bound

For applications we would like to make use of the 'best' possible quantum codes. What 'best' means in any given circumstance depends on the application. For this reason we would like to have criteria for determining whether or not a code with particular characteristics exists or not. In this section we develop the quantum Hamming bound, a simple bound which gives some insights into the general properties of quantum codes. Unfortunately the quantum Hamming bound only applies to non-degenerate codes, but it gives us an idea of what more general bounds may look like. Suppose a non-degenerate code is used to encode k qubits in n qubits in such a way that it can correct errors on any subset of t or fewer qubits. Suppose j errors occur, where $j \leq t$. There are $\binom{n}{j}$ sets of locations where errors may occur. With each such set of locations there are three possible errors - the three Pauli matrices X, Y, Z - that may occur in each qubit, for a total of 3^j possible errors. The total number of errors that may occur on t or fewer qubits is therefore

$$\sum_{j=0}^{t} \binom{n}{j} 3^j. \tag{10.50}$$

(Note that $j = 0$ corresponds to the case of no errors on any qubit, the 'error' I.) In order to encode k qubits in a non-degenerate way each of these errors must correspond to an orthogonal 2^k-dimensional subspace. All of these subspaces must be fitted into the
total 2^n-dimensional space available to n qubits, leading to the inequality

$$\sum_{j=0}^{t} \binom{n}{j} 3^j 2^k \leq 2^n, \tag{10.51}$$

which is the quantum Hamming bound. Consider, for example, the case where we wish to encode one qubit in n qubits in such a way that errors on one qubit are tolerated. In this case the quantum Hamming bound reads:

$$2(1 + 3n) \leq 2^n \tag{10.52}$$

Substitution shows that this inequality is not satisfied for $n \leq 4$, while it is for values of $n \geq 5$. Therefore, there is no non-degenerate code encoding one qubit in fewer than five qubits in such a way as to protect from all possible errors on a single qubit.

Of course, not all quantum codes are non-degenerate, so the quantum Hamming bound is more useful as a rule of thumb than as a hard and fast bound on the existence of quantum codes. (In particular, at the time of writing no codes are known that violate the quantum Hamming bound, even allowing degenerate codes.) Later, we will have occasion to look at some bounds on quantum codes that apply to all quantum codes, not just non-degenerate codes. For example, in Section 12.4.3 we prove the quantum Singleton bound, which implies that any quantum code encoding k qubits in n qubits and able to correct errors on any t qubits must satisfy $n \geq 4t + k$. It follows that the smallest code encoding a single qubit and able to correct an arbitrary error on a single qubit must satisfy $n \geq 4 + 1 = 5$, and indeed, we will soon exhibit such a five qubit code.

9.3.10 10.4 Constructing quantum codes

We now have a theoretical framework for the study of quantum error-correcting codes, but we don't as yet have many examples of such codes! We begin to remedy this defect by taking a brief tour into the theory of classical linear codes in Section 10.4.1, and then in Section 10.4.2 explain how ideas from classical linear codes can be used to construct a large class of quantum

codes known as Calderbank-Shor-Steane (CSS) codes. Our job is completed in Section 10.5 with the development of the stabilizer codes, a class of codes even more general than the CSS codes which offers a powerful means for constructing a wide variety of quantum codes.

9.3.11 10.4.1 Classical linear codes

Classical error-correcting codes have many varied and important technological applications, so it is unsurprising that a powerful theory of such codes has been developed. Our interest in the techniques of classical error-correction is that many of these techniques have important implications for quantum error-correction, especially the theory of classical linear codes, which can be used to develop a wide variety of good quantum error-correcting codes. In this section we review classical linear codes, emphasizing especially those ideas important to quantum error-correction.

A linear code C encoding k bits of information into an n bit code space is specified by an n by k generator matrix G whose entries are all elements of $\mathbf{Z}_2$, that is, zeroes and ones. The matrix G maps messages to their encoded equivalent. Thus the k bit message x is encoded as Gx, where the message x is treated as a column vector in the obvious
way. Furthermore, the multiplication operation, and all our other arithmetic operations in this section, are done modulo 2 . As a simple example, the repetition code mapping a single bit to three repetitions is specified by the generator matrix

$$G = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \tag{10.53}$$

since G maps the possible messages, 0 and 1 , to their encoded form, $G[0] = (0, 0, 0)$ and $G[1] = (1, 1, 1)$. (Recall that $(a, b, \ldots, z)$ is our shorthand notation for column vectors.) We say that a code using n bits to encode k bits of information is an $[n, k]$ code; this example is therefore a [3,1] code. A slightly more complicated example is to encode two bits using three repetitions of each bit - a [6,2] code. This has generator matrix

$$G = \begin{bmatrix} 1 & 0 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \\ 0 & 1 \end{bmatrix}, \tag{10.54}$$

from which we see that

$$\begin{array}{ll} G(0,0) = (0,0,0,0,0,0); & G(0,1) = (0,0,0,1,1,1); \\ G(1,0) = (1,1,1,0,0,0); & G(1,1) = (1,1,1,1,1,1), \end{array} \tag{10.56}$$

just as we expect. The set of possible codewords for the code corresponds to the vector space spanned by the columns of G, so in order that all messages be uniquely encoded we require that the columns of G be linearly independent, but otherwise place no constraints on G.

Exercise 10.14: Write an expression for a generator matrix encoding k bits using r repetitions for each bit. This is an $[rk, k]$ linear code, and should have an $rk \times k$ generator matrix.

Exercise 10.15: Show that adding one column of G to another results in a generator matrix generating the same code.

A great advantage of linear codes over general error-correcting codes is their compact specification. A general code encoding k bits in n bits requires 2^k codewords each of length n to

specify the encoding, a total of $n2^k$ bits to specify a description of the code. With a linear code we need only specify the kn bits of the generator matrix, an exponential saving in the amount of memory required! This compact description is mirrored in the ability to do efficient encoding and decoding, important features which classical linear codes share with their quantum cousins, the stabilizer codes. We can already see how to perform efficient encoding of a classical linear code: one simply multiplies the k bit message by the n by k generator matrix G to obtain the n bit encoded message, a procedure which can be done using $O(nk)$ operations.

One of the attractive features of the generator matrix definition of linear codes is the transparent connection between the messages we wish to encode and how they are encoded. It is not so clear how to perform error-correction. Error-correction for linear
codes is most easily understood by introducing an alternative (but equivalent) formulation of linear codes in terms of parity check matrices. In this definition an $[n, k]$ code is defined to consist of all n-element vectors x over $\mathbf{Z}_2$ such that

$$Hx = 0, \tag{10.57}$$

where H is an $n - k$ by n matrix known as the parity check matrix, with entries all zeroes and ones. Equivalently, but more succinctly, the code is defined to be the kernel of H. A code encoding k bits has 2^k possible codewords so the kernel of H must be k-dimensional, and therefore we require that H have linearly independent rows.

Exercise 10.16: Show that adding one row of the parity check matrix to another does not change the code. Using Gaussian elimination and swapping of bits it is therefore possible to assume that the parity check matrix has the standard form $[A \mid I_{n-k}]$, where A is an $(n-k) \times k$ matrix.

To connect the parity check picture of linear codes with the generator matrix picture we need to develop a procedure that enables us to convert back and forth between the parity check matrix H and the generator matrix G. To go from the parity check matrix to the generator matrix, pick k linearly independent vectors $y_1, \ldots, y_k$ spanning the kernel of H, and set G to have columns y_1 through y_k. To go from the generator matrix to the parity check matrix, pick $n - k$ linearly independent vectors $y_1, \ldots, y_{n-k}$ orthogonal to the columns of G, and set the rows of H to be $y_1^T, \ldots, y_{n-k}^T$. (By orthogonal, we mean that the inner product modulo 2 must be zero.) As an example, consider the [3,1] repetition code defined by the generator matrix (10.53). To construct H we pick out $3 - 1 = 2$ linearly independent vectors orthogonal to the columns of G, say $(1, 1, 0)$ and $(\ 0, 1, 1\ )$, and define the parity check matrix as:

$$H \equiv \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}. \tag{10.58}$$

It is easy to check that $Hx = 0$ only for the codewords $x = (0, 0, 0)$ and $x = (1, 1, 1)$.
Exercise 10.17: Find a parity check matrix for the [6,2] repetition code defined by the generator matrix in (10.54).

Exercise 10.18: Show that the parity check matrix H and generator matrix G for the same linear code satisfy $HG = 0$.

Exercise 10.19: Suppose an $[n, k]$ linear code C has a parity check matrix of the form $H = [A \mid I_{n-k}]$, for some $(n - k) \times k$ matrix A. Show that the corresponding generator matrix is

$$G = \left[\frac{I_k}{-A}\right]. \tag{10.59}$$

(Note that $-A = A$ since we are working modulo 2 ; however, this equation also holds for linear codes over more general fields than $\mathbf{Z}_2$.)

The parity check matrix makes error-detection and recovery quite transparent. Suppose that we encode the message x as $y = Gx$, but an error e due to noise corrupts y giving the corrupted codeword $y' = y + e$. (Note that $+$ here denotes bitwise addition modulo 2.) Because $Hy = 0$ for all codewords, it follows that $Hy' = He$. We call Hy' the error syndrome, and it plays a role similar to the role played by the error syndrome in quantum error-correction; it is a function Hy' of the corrupted state y', just as the quantum error syndrome is determined by measuring the corrupted quantum state, and because of the relation $Hy' = He$, the error syndrome contains information about the error that occurred that hopefully will enable recovery to the original codeword y. To see how this is possible, suppose no errors or just one error occurred. Then the error syndrome Hy' is equal to 0 in the no error case and is equal to He_j when an error occurs on the j th bit, where e_j is the unit vector with component 1 in the j th component. If we assume that errors occur on at most one bit, it is therefore possible to perform error-correction by computing the error syndrome Hy' and comparing it to the different possible values of He_j to determine which (if any) bit needs to be corrected.

More generally, insight into how error-correction may be performed with a linear code can be attained using the concept of distance. Suppose x and y are words of n bits each. The (Hamming) distance $d(x, y)$ between x and y is defined to be the number of places at which x and y differ. Thus $d((1, 1, 0, 0), (0, 1, 0, 1)) = 2$, for example. The (Hamming) weight of a word x is defined to be the distance from the string of all zeroes, $\mathrm{wt}(x) \equiv d(x, 0)$, that is, the number of places at which x is non-zero. Note that $d(x, y) = \mathrm{wt}(x + y)$. To understand the connection with error-correction suppose we encode x as $y = Gx$ using a linear error-correcting code. Noise corrupts the encoded bit string producing $y' = y + e$. Provided the probability of a bit flip is less than $1/2$, the most likely codeword to have been encoded is the codeword y which minimizes the number of bit flips needed to get from y to y', that is, which minimizes $\mathrm{wt}(e) = d(y, y')$. In principle, error-correction with a linear code may be accomplished by simply replacing y' by such a y. In practice this may be rather inefficient, since determining the minimal distance $d(y, y')$ in general requires searching all 2^k possible codewords y. A great deal of effort in classical coding theory has gone into constructing codes with special structure that enable error-correction to be performed more efficiently, however these constructions are beyond the scope of this book.

The global properties of the code can also be understood using the Hamming distance. We define the distance of a code to be the minimum distance between any two codewords,

$$d(C) \equiv \min_{x,y \in C, x \neq y} d(x, y). \tag{10.60}$$

But $d(x, y) = \mathrm{wt}(x + y)$. Since the code is linear, $x + y$ is a codeword if x and y are, so we see that

$$d(C) = \min_{x \in C, x \neq 0} \mathrm{wt}(x). \tag{10.61}$$

Setting $d \equiv d(C)$, we say that C is an $[n, k, d]$ code. The importance of the distance is that a code with distance at least $2t + 1$ for some integer t is able to correct errors on up to t bits, simply by decoding the corrupted encoded message y' as the unique codeword y satisfying $d(y, y') \leq t$.

Exercise 10.20: Let H be a parity check matrix such that any $d - 1$ columns are linearly independent, but there exists a set of d linearly dependent columns. Show that the code defined by H has distance d.

Exercise 10.21: (Singleton bound) Show that an $[n, k, d]$ code must satisfy

$$n - k \geq d - 1$$

A good illustrative class of linear error-correcting codes are the Hamming codes. Suppose $r \geq 2$ is an integer and let H be the matrix whose columns are all $2^r - 1$ bit strings of length r which are not identically 0 . This parity check matrix defines a $[2^r - 1, 2^r - r - 1]$ linear code known as a Hamming code. An especially important example for quantum error-correction is the case $r = 3$, which is a [7,4] code having parity check matrix:

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \tag{10.62}$$

Any two columns of H are different, and therefore linearly independent; the first three columns are linearly dependent, so by Exercise 10.20 the distance of the code is 3 . It follows that this code is able to correct an error on any single bit. Indeed, the errorcorrection method is very simple. Suppose an error occurs on the j th bit. Inspection of (10.62) reveals that the syndrome He_j is just a binary representation for j, telling us which bit to flip to correct the error.

Exercise 10.22: Show that all Hamming codes have distance 3, and thus can correct an error on a single bit. The Hamming codes are therefore $[2^r - 1, 2^r - r - 1, 3]$ codes.

What can we say more generally about the properties of linear codes? In particular, we would like conditions telling us whether or not codes with particular code parameters exist. Not surprisingly, many techniques for proving such conditions exist. One such set of conditions is known as the Gilbert-Varshamov bound, which states that for large n there exists an $[n, k]$ error-correcting code protecting against errors on t bits for some k such that

$$\frac{k}{n} \geq 1 - H\left(\frac{2t}{n}\right), \tag{10.63}$$

where $H(x) \equiv -x \log(x) - (1 - x) \log(1 - x)$ is the binary Shannon entropy, studied in detail in Chapter 11. The importance of the Gilbert-Varshamov bound is that it guarantees the existence of good codes, provided one doesn't try to encode too many bits (k) into too small a number of bits (n). The proof of the Gilbert-Varshamov bound is quite simple, and is left as an exercise.

Exercise 10.23: Prove the Gilbert-Varshamov bound.

We conclude our survey of classical error-correction by explaining an important construction for codes known as the dual construction. Suppose C is an $[n, k]$ code with generator matrix G and parity check matrix H. Then we can define another code, the dual of C, denoted $C^\perp$, to be the code with generator matrix H^T and parity check matrix G^T. Equivalently, the dual of C consists of all codewords y such that y is orthogonal to all the codewords in C. A code is said to be weakly self-dual if $C \subseteq C^\perp$, and strictly self-dual if $C = C^\perp$. Rather remarkably, the dual construction for classical linear codes arises naturally in the study of quantum error-correction, and is the key to the construction of an important class of quantum codes known as CSS codes.

Exercise 10.24: Show that a code with generator matrix G is weakly self-dual if and only if $G^T G = 0$.

Exercise 10.25: Let C be a linear code. Show that if $x \in C^\perp$ then

$$\sum_{y \in C} (-1)^{x \cdot y} = |C|, \text{ while if } x \notin C^\perp \text{ then } \sum_{y \in C} (-1)^{x \cdot y} = 0.$$

9.3.12 10.4.2 Calderbank-Shor-Steane codes

Our first example of a large class of quantum error-correcting codes is the Calderbank-Shor-Steane codes, more usually known as CSS codes, after the initials of the inventors of this class

of codes. CSS codes are an important subclass of the more general class of stabilizer codes.

Suppose C_1 and C_2 are $[n, k_1]$ and $[n, k_2]$ classical linear codes such that $C_2 \subset C_1$ and C_1 and $C_2^\perp$ both correct t errors. We will define an $[n, k_1 - k_2]$ quantum code $\mathrm{CSS}(C_1, C_2)$ capable of correcting errors on t qubits, the CSS code of C_1 over C_2, via the following construction. Suppose $x \in C_1$ is any codeword in the code C_1. Then we define the quantum state $|x + C_2\rangle$ by

$$|x + C_2\rangle \equiv \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x + y\rangle \tag{10.64}$$

where $+$ is bitwise addition modulo 2 . Suppose x' is an element of C_1 such that $x - x' \in C_2$. Then it is easy to see that $|x + C_2\rangle = |x' + C_2\rangle$, and thus the state $|x + C_2\rangle$ depends only upon the coset of C_1/C_2 which x is in, explaining the coset notation we have used for $|x + C_2\rangle$. Furthermore, if x and x' belong to different cosets of C_2, then for no $y, y' \in C_2$ does $x+y = x'+y'$, and therefore $|x + C_2\rangle$ and $|x' + C_2\rangle$ are orthonormal states. The quantum code $\mathrm{CSS}(C_1, C_2)$ is defined to be the vector space spanned by the states $|x + C_2\rangle$ for all $x \in C_1$. The number of cosets of C_2 in C_1 is $|C_1| / |C_2|$ so the dimension of $\mathrm{CSS}(C_1, C_2)$ is $|C_1| / |C_2| = 2^{k_1 - k_2}$, and therefore $\mathrm{CSS}(C_1, C_2)$ is an $[\, n, k_1 - k_2 \,]$ quantum code.

We can exploit the classical error-correcting properties of C_1 and $C_2^\perp$ to detect and correct quantum errors! In fact, it is possible to error-correct up to t bit and phase flip errors on $\mathrm{CSS}(C_1, C_2)$ by making use of the error-correcting properties of C_1 and $C_2^\perp$, respectively. Suppose the bit flip errors are described by an n bit vector e_1 with 1 s where bit flips occurred, and 0 s elsewhere, and the phase flip errors are described by an n bit vector e_2 with 1 s where phase flips occurred, and 0 s elsewhere. If $|x + C_2\rangle$ was the original state then the corrupted state is:

$$\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{(x+y)\cdot e_2} |x + y + e_1\rangle . \tag{10.65}$$

To detect where bit flips occurred it is convenient to introduce an ancilla containing sufficient qubits to store the syndrome for the code C_1, and initially in the all zero state $|0\rangle$. We use reversible computation to apply the parity matrix H_1 for the code C_1, taking $|x + y + e_1\rangle |0\rangle$ to $|x + y + e_1\rangle |H_1 (x + y + e_1)\rangle = |x + y + e\rangle |H_1 e_1\rangle$, since $(x + y) \in C_1$ is annihilated by the parity check matrix. The effect of this operation is to produce the state:

$$\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{(x+y)\cdot e_2} |x + y + e_1\rangle |H_1 e_1\rangle . \tag{10.66}$$

Exercise 10.26: Suppose H is a parity check matrix. Explain how to compute the transformation $|x\rangle|0\rangle \rightarrow |x\rangle|Hx\rangle$ using a circuit composed entirely of controlled-NOTs.

Error-detection for the bit flip errors is completed by measuring the ancilla to obtain the result $H_1 e_1$ and discarding the ancilla, giving the state

$$\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{(x+y)\cdot e_2} |x + y + e_1\rangle . \tag{10.67}$$

Knowing the error syndrome $H_1 e_1$ we can infer the error e_1 since C_1 can correct up to t errors, which completes the error-detection. Recovery is performed simply by applying not gates to the qubits at whichever positions in the error e_1 a bit flip occurred, removing all the bit flip errors and giving the state

$$\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{(x+y)\cdot e_2} |x + y\rangle . \tag{10.68}$$

To detect phase flip errors we apply Hadamard gates to each qubit, taking the state to

$$\frac{1}{\sqrt{|C_2|\,2^n}} \sum_z \sum_{y \in C_2} (-1)^{(x+y)\cdot(e_2+z)} |z\rangle, \tag{10.69}$$

where the sum is over all possible values for n bit z. Setting $z' \equiv z + e_2$, this state may be rewritten:

$$\frac{1}{\sqrt{|C_2|\,2^n}} \sum_{z'} \sum_{y \in C_2} (-1)^{(x+y)\cdot z'} \, |z' + e_2\rangle \, . \tag{10.70}$$

(The next step appeared as Exercise 10.25 on page 450.) Supposing $z' \in C_2^\perp$ it is easy to see that $\sum_{y \in C_2} (-1)^{y \cdot z'} = |C_2|$, while if $z' \notin C_2^\perp$ then $\sum_{y \in C_2} (-1)^{y \cdot z'} = 0$. Thus the state may be rewritten:

$$\frac{1}{\sqrt{2^n / |C_2|}} \sum_{z' \in C_2^\perp} (-1)^{x \cdot z'} \, |z' + e_2\rangle \, , \tag{10.71}$$

which looks just like a bit flip error described by the vector e_2 ! As for the error-detection for bit flips we introduce an ancilla and reversibly apply the parity check matrix H_2 for $C_2^\perp$ to obtain $H_2 e_2$, and correct the 'bit flip error' e_2, obtaining the state

$$\frac{1}{\sqrt{2^n / |C_2|}} \sum_{z' \in C_2^\perp} (-1)^{x \cdot z'} \, |z'\rangle \, . \tag{10.72}$$

The error-correction is completed by again applying Hadamard gates to each qubit; we can either compute the result of these gates directly, or note that the effect is to apply Hadamard gates to the state in (10.71) with $e_2 = 0$; since the Hadamard gate is self-inverse this takes us back to the state in (10.68) with $e_2 = 0$:

$$\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x + y\rangle, \tag{10.73}$$

which is the original encoded state!
One important application of CSS codes is to prove a quantum version of the GilbertVarshamov bound, guaranteeing the existence of good quantum codes. This states that
in the limit as n becomes large, an $[n, k]$ quantum code protecting against errors on up to t qubits exists for some k such that

$$\frac{k}{n} \geq 1 - 2H\left(\frac{2t}{n}\right) \tag{10.74}$$

Thus, good quantum error-correcting codes exist, provided one doesn't try to pack too many qubits k into an n qubit code. The proof of the Gilbert-Varshamov bound for CSS codes is rather more complex than the proof of the classical Gilbert-Varshamov bound, due to the constraints on the classical codes C_1 and C_2, and is left as an end of chapter problem.

Summarizing, suppose C_1 and C_2 are $[n, k_1]$ and $[n, k_2]$ classical linear codes, respectively, such that $C_2 \subset C_1$, and both C_1 and $C_2^\perp$ can correct errors on up to t bits. Then $\mathrm{CSS}\,(C_1, C_2)$ is an $[n, k_1 - k_2]$ quantum error-correcting code which can correct arbitrary errors on up to t qubits. Furthermore, the error-detection and correction steps require only the application of Hadamard and controlled-not gates, in each case a number linear in the size of the code. Encoding and decoding can also be performed using a number of gates linear in the size of the code, but we won't discuss that here; it's discussed later in more generality in Section 10.5.8.

Exercise 10.27: Show that the codes defined by

$$|x + C_2\rangle \equiv \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{u \cdot y} |x + y + v\rangle \tag{10.75}$$

and parameterized by u and v are equivalent to $\mathrm{CSS}\,(C_1, C_2)$ in the sense that they have the same error-correcting properties. These codes, which we'll refer to as $\mathrm{CSS}_{u,v}\,(C_1, C_2)$, will be useful later in our study of quantum key distribution, in Section 12.6.5.

The Steane code

An important example of a CSS code may be constructed using the [7,4,3] Hamming code whose parity check matrix we recall here:

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \tag{10.76}$$

Suppose we label this code C and define $C_1 \equiv C$ and $C_2 \equiv C^{\perp}$. To use these codes to define a CSS code we need first to check that $C_2 \subset C_1$. By definition the parity check matrix of $C_2 = C^{\perp}$ is equal to the transposed generator matrix of $C_1 = C$:

$$H\,[C_2] = G\,[C_1]^T = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \tag{10.77}$$

Exercise 10.28: Verify that the transpose of the matrix in (10.77) is the generator of the [7, 4, 3] Hamming code.

Comparing with (10.76) we see that the span of the rows of $H\,[C_2]$ strictly contains the span of the rows of $H\,[C_1]$, and since the corresponding codes are the kernels of $H\,[C_2]$ and $H\,[C_1]$ we conclude that $C_2 \subset C_1$. Furthermore, $C_2^{\perp} = \left(C^{\perp}\right)^{\perp} = C$, so both C_1 and $C_2^{\perp}$ are distance 3 codes which can correct errors on 1 bit. Since C_1 is a $[7, 4]$ code and C_2 is a $[7, 3]$ code it follows that $\mathrm{CSS}\,(C_1, C_2)$ is a $[7, 1]$ quantum code which can correct errors on a single qubit.

This [7,1] quantum code has nice properties that make it easy to work with, and will be used in many of the examples for the remainder of this chapter. It is known as the Steane code, after its inventor. The codewords of C_2 are easily determined from (10.77) and Exercise 10.28. Rather than write them out explicitly, we write them out implicitly as the entries in the logical $|0_L\rangle$ for the Steane code, $|0 + C_2\rangle$:

$$|0_L\rangle = \frac{1}{\sqrt{8}}[|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle + |0001111\rangle + |1011010\rangle + |0111100\rangle + |110100 \tag{10.78}$$

To determine the other logical codeword we need to find an element of C_1 that is not in C_2. An example of such an element is $(1, 1, 1, 1, 1, 1, 1)$, giving:

$$|1_L\rangle = \frac{1}{\sqrt{8}}[|1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle + |1110000\rangle + |0100101\rangle + |1000011\rangle + |001011 \tag{10.79}$$

9.3.13 10.5 Stabilizer codes

> We cannot clone, perforce; instead, we split Coherence to protect it from that wrong That would destroy our valued quantum bit And make our computation take too long.
>
> Correct a flip and phase - that will suffice. If in our code another error's bred, We simply measure it, then God plays dice, Collapsing it to X or Y or zed.
>
> We start with noisy seven, nine, or five And end with perfect one. To better spot Those flaws we must avoid, we first must strive To find which ones commute and which do not.
>
> With group and eigenstate, we've learned to fix Your quantum errors with our quantum tricks. - 'Quantum Error Correction Sonnet', by Daniel Gottesman

Stabilizer codes, sometimes known as additive quantum codes, are an important class of quantum codes whose construction is analogous to classical linear codes. In order to understand stabilizer codes it is useful to first develop the stabilizer formalism, a powerful method for understanding a wide class of operations in quantum mechanics. The applications of the stabilizer formalism extend far beyond quantum error-correction; however, in this book our main concern is with this specific application. After defining the stabilizer formalism, we explain how unitary gates and measurements may be described using it, and an important theorem which quantifies the limitations of stabilizer operations. We then present stabilizer constructions for stabilizer codes, along with explicit examples, a useful standard form, and circuits for encoding, decoding, and correction.

9.3.14 10.5.1 The stabilizer formalism

The central insight of the stabilizer formalism is easily illustrated by an example. Consider the EPR state of two qubits

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{10.80}$$

It is easy to verify that this state satisfies the identities $X_1X_2|\psi\rangle = |\psi\rangle$ and $Z_1Z_2|\psi\rangle = |\psi\rangle$; we say that the state $|\psi\rangle$ is stabilized by the operators X_1X_2 and Z_1Z_2. A little less obviously, the state $|\psi\rangle$ is the unique quantum state (up to a global phase) which is stabilized by these operators X_1X_2 and Z_1Z_2. The basic idea of the stabilizer formalism is that many quantum states can be more easily described by working with the operators that stabilize them than by working explicitly with the state itself. This claim is perhaps rather surprising at first sight; nevertheless it is true. It turns out that many quantum codes (including CSS codes and the Shor code) can be much more compactly described using stabilizers than in the state vector description. Even more importantly, errors on the qubits and operations such as the Hadamard gate, phase gate, and even the controllednot gate and measurements in the computational basis are all easily described using the stabilizer formalism!

The key to the power of the stabilizer formalism lies in the clever use of group theory, whose basic elements are reviewed in Appendix 2. The group of principal interest is the Pauli group G_n on n qubits. For a single qubit, the Pauli group is defined to consist of all the Pauli matrices, together with multiplicative factors $\pm 1, \pm i$:

$$G_1 \equiv \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\} \tag{10.81}$$

This set of matrices forms a group under the operation of matrix multiplication. You might wonder why we don't omit the multiplicative factors ± 1 and $\pm i$; the reason these are included is to ensure that G_1 is closed under multiplication, and thus forms a legitimate group. The general Pauli group on n qubits is defined to consist of all n-fold tensor products of Pauli matrices, and again we allow multiplicative factors $\pm 1, \pm i$.

We can now define stabilizers a little more precisely. Suppose S is a subgroup of G_n and define V_S to be the set of n qubit states which are fixed by every element of S.V_S is the vector space stabilized by S, and S is said to be the stabilizer of the space V_S, since every element of V_S is stable under the action of elements in S. You should convince yourself of the truth of the following simple exercise:

Exercise 10.29: Show that an arbitrary linear combination of any two elements of V_S is also in V_S. Therefore, V_S is a subspace of the n qubit state space. Show that V_S is the intersection of the subspaces fixed by each operator in S (that is, the eigenvalue one eigenspaces of elements of S).

Let's look at a simple example of the stabilizer formalism in action, a case with $n = 3$ qubits and $S \equiv \{I, Z_1Z_2, Z_2Z_3, Z_1Z_3\}$. The subspace fixed by Z_1Z_2 is spanned by $|000\rangle$, $|001\rangle, |110\rangle$ and $|111\rangle$, and the subspace fixed by Z_2Z_3 is spanned by $|000\rangle, |100\rangle, |011\rangle$ and $|111\rangle$. Note that the elements $|000\rangle$ and $|111\rangle$ are common to both these lists. With these observations and a little thought one realizes that V_S must be the subspace spanned by the states $|000\rangle$ and $|111\rangle$.

In this example we determined V_S simply by looking at the subspaces stabilized by two of the operators in S. This is a manifestation of an important general phenomenon the description of a group by its generators. As explained in Appendix 2 a set of elements $g_1, \ldots, g_l$ in a group G is said to generate the group G if every element of G can be written as a product of elements from the list $g_1, \ldots, g_l$, and we write $G = \langle g_1, \ldots, g_l \rangle$. In the example $S = \langle Z_1Z_2, Z_2Z_3 \rangle$ as $Z_1Z_3 = (Z_1Z_2)(Z_2Z_3)$ and $I = (Z_1Z_2)^2$. The great advantage of using generators to describe groups is that they provide a compact means of describing the group. Indeed, in Appendix 2 we show that a group G with size $|G|$ has a set of at most $\log(|G|)$ generators. Furthermore, to see that a particular vector is stabilized by a group S we need only check that the vector is stabilized by the generators, since it is then automatically stabilized by products of the generators, making this a most convenient representation. (The notation $\langle \cdots \rangle$ which we use for group generators may potentially be confused with the notation for observable averages introduced in Section 2.2.5 beginning on page 87; however, in practice, it is always clear from context how the notation is being used.)

Not just any subgroup S of the Pauli group can be used as the stabilizer for a nontrivial vector space. For example, consider the subgroup of G_1 consisting of $\{\pm I, \pm X\}$. Obviously the only solution to $(-I)|\psi\rangle = |\psi\rangle$ is $|\psi\rangle = 0$, and thus $\{\pm I, \pm X\}$ is the stabilizer for the trivial vector space. What conditions must be satisfied by S in order that it stabilize a non-trivial vector space, V_S ? Two conditions easily seen to be necessary are that (a) the elements of S commute, and (b) $-I$ is not an element of S. We don't yet have all the tools to prove it, but will show later that these two conditions are also sufficient for V_S to be non-trivial.

Exercise 10.30: Show that $-I \notin S$ implies $\pm iI \notin S$.

To see that these two conditions are necessary, suppose V_S is non-trivial, so it contains a non-zero vector $|\psi\rangle$. Let M and N be elements of S. Then M and N are tensor products of Pauli matrices, possibly with an overall multiplicative factor; because the Pauli matrices all commute or anti-commute with one another, it follows that M and N must either commute or anti-commute. To establish condition (a), that they commute, we suppose that M and N anti-commute and show that this leads to a contradiction. By assumption $-NM = MN$ so we have $-|\psi\rangle = -NM|\psi\rangle = MN|\psi\rangle = |\psi\rangle$, where the first and last equalities follow from the fact that M and N stabilize $|\psi\rangle$. So we have $-|\psi\rangle = |\psi\rangle$, which implies that $|\psi\rangle$ is the zero vector,

which is the desired contradiction. To establish condition (b), that $-I \notin S$ just note that if $-I$ is an element of S then we have $-I|\psi\rangle = |\psi\rangle$, which again leads to a contradiction.

Exercise 10.31: Suppose S is a subgroup of G_n generated by elements $g_1, \ldots, g_l$. Show that all the elements of S commute if and only if g_i and g_j commute for each pair i, j.

A beautiful example of the stabilizer formalism is provided by the seven qubit Steane

Name	Operator
g_1	$IIIXXXX$
g_2	$IXXIIXX$
g_3	$XIXIXIX$
g_4	$IIIZZZZ$
g_5	$IZZIIZZ$
g_6	$ZIZIZIZ$

Figure 10.6. Stabilizer generators for the Steane seven qubit code. The entries represent tensor products on the respective qubits; for example, $Z I Z I Z I Z=Z \otimes I \otimes Z \otimes I \otimes Z \otimes I \otimes Z=Z_{1 Z_{3} Z_{5} Z_{7}$.}

code. It turns out that the six generators g_1 through g_6 listed in Figure 10.6 generate a stabilizer for the code space of the Steane code. Observe how clean and compact this description is when compared with the rather messy specification in terms of state vectors, (10.78) and (10.79); even further advantages will manifest when we examine quantum error-correction from this viewpoint. Note also the similarity in structure between the generators in Figure 10.6 and the parity check matrices for the classical linear codes C_1 and $C_2^\perp$ used in the construction of the Steane code. (Recall that for the Steane code $C_1 = C_2^\perp$ is the Hamming [7,4,3] code with parity check matrix given by (10.76).) The first three generators of the stabilizer have X s in locations corresponding to the locations of the 1 s in the parity check matrix for C_1, while the final three generators g_4 through g_6 have Z s in locations corresponding to the locations of the 1 s in the parity check matrix for $C_2^\perp$. With these observations in hand the solution to the following exercise becomes almost self-evident.

Exercise 10.32: Verify that the generators in Figure 10.6 stabilize the codewords for the Steane code, as described in Section 10.4.2.

This use of the stabilizer formalism to describe a quantum code foreshadows our later use of stabilizers to describe a wide class of quantum codes, but for now it is important to appreciate that there is nothing special about the Steane code's status as a quantum code - it is merely a subspace of a vector space which happens to have a description using stabilizers.

In practice, we want our generators $g_1, \ldots, g_l$ to be independent in the sense that removing any generator g_i makes the group generated smaller,

$$\langle g_1, \ldots, g_{i-1}, g_{i+1}, \ldots, g_l \rangle \neq \langle g_1, \ldots, g_l \rangle . \tag{10.82}$$

Determining whether a particular set of generators is independent or not is rather time-consuming with our current understanding; fortunately, there is a simple way this can be done based on an idea known as the check matrix, so-named because it plays a role in the theory of stabilizer codes analogous to the parity check matrix in classical linear codes.

Suppose $S = \langle g_1, \ldots, g_l \rangle$. There is an extremely useful way of presenting the generators $g_1, \ldots, g_l$ of S using the check matrix. This is an $l \times 2n$ matrix whose rows correspond to the generators g_1 through g_l; the left hand side of the matrix contains 1 s to indicate which generators contain X s, and the right hand side contains 1s to indicate

which generators contain Z s; the presence of a 1 on both sides indicates a Y in the generator. More explicitly, the i th row is constructed as follows. If g_i contains an I on the j th qubit then the j th and $n+j$ th column elements are 0 ; if it contains an X on the j th qubit then the j th column element is a 1 and the $n+j$ th column element is a 0 ; if it contains a Z on the j th qubit then the j th column element is 0 and the $n+j$ th column element is 1 ; if it contains a Y on the j th qubit then both the j th and $n+j$ th columns are 1. In the case of the Steane seven qubit code we can read the check matrix off from Figure 10.6:

$$\left[\begin{array}{ccccccc|ccccccc} 0&0&0&1&1&1&1&0&0&0&0&0&0&0\\ 0&1&1&0&0&1&1&0&0&0&0&0&0&0\\ 1&0&1&0&1&0&1&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&1&1&1&1\\ 0&0&0&0&0&0&0&0&1&1&0&0&1&1\\ 0&0&0&0&0&0&0&1&0&1&0&1&0&1 \end{array}\right]. \tag{10.83}$$

The check matrix doesn't contain any information about the multiplicative factors out the front of the generators, but it does contain much other useful information, so much so that we use $r(g)$ to denote the $2n$-dimensional row vector representation of an element g of the Pauli group. Suppose we define a $2n \times 2n$ matrix Λ by

$$\Lambda = \left[\begin{array}{cc} 0 & I \\ I & 0 \end{array}\right] \tag{10.84}$$

where the I matrices on the off-diagonals are $n \times n$. Elements g and g' of the Pauli group are easily seen to commute if and only if $r(g)\Lambda r\left(g'\right)^T = 0$; the formula $x\Lambda y^T$ defines a sort of 'twisted' inner product between row matrices x and y expressing whether the elements of the Pauli group corresponding to x and y commute or not.

Exercise 10.33: Show that g and g' commute if and only if $r(g)\Lambda r\left(g'\right)^T = 0$. (In the check matrix representation, arithmetic is done modulo two.)

Exercise 10.34: Let $S = \langle g_1, \ldots, g_l \rangle$. Show that $-I$ is not an element of S if and only if $g_j^2 = I$ for all j, and $g_j \neq -I$ for all j.

Exercise 10.35: Let S be a subgroup of G_n such that $-I$ is not an element of S. Show that $g^2 = I$ for all $g \in S$, and thus $g^\dagger = g$.

A useful connection between independence of the generators and the check matrix is established by means of the following proposition:

Proposition 10.3: Let $S = \langle g_1, \ldots, g_l \rangle$ be such that $-I$ is not an element of S. The generators g_1 through g_l are independent if and only if the rows of the corresponding check matrix are linearly independent.

Proof

We prove the contrapositive. Note first that g_i^2 must equal I for all i, by Exercise 10.35 . Observe that $r(g) + r\left(g'\right) = r\left(gg'\right)$, so addition in the row vector representation corresponds to multiplication of group elements. Thus the rows of the check matrix are linearly dependent, $\sum_i a_i r\left(g_i\right) = 0$, and $a_j \neq 0$ for some j, if and only if $\prod_i g_i^{a_i}$ is equal to the identity, up to an overall multiplicative factor. But $-I \notin S$ so the multiplicative factor must be 1 , and the last condition corresponds to the condition $g_j = g_j^{-1} = \prod_{i \neq j} g_i^{a_i}$, and thus $g_1, \ldots, g_l$ are not independent generators. $\square$

The following innocuous looking proposition is surprisingly useful, and can be immediately leveraged into a proof that V_S is of dimension 2^k when S is generated by $l = n-k$ independent commuting generators, and $-I \notin S$. We will use the proposition repeatedly throughout the remainder of this chapter. Once again the tool of choice in the proof is the check matrix representation.

Proposition 10.4: Let $S = \langle g_1, \ldots, g_l \rangle$ be generated by l independent generators and satisfy $-I \notin S$. Fix i in the range $1, \ldots, l$. Then there exists $g \in G_n$ such that $g g_i g^\dagger = -g_i$ and $g g_j g^\dagger = g_j$ for all $j \neq i$.

Proof

Let G be the check matrix associated to $g_1, \ldots, g_l$. The rows of G are linearly independent by Proposition 10.3, so there exists a $2n$-dimensional vector x such that $G \Lambda x = e_i$, where e_i is the l-dimensional vector with a 1 in the i th position and 0 s elsewhere. Let g be such that $r(g) = x^T$. Then by definition of x we have $r(g_j) \Lambda r(g)^T = 0$ for $j \neq i$ and $r(g_i) \Lambda r(g)^T = 1$, and thus $g g_i g^\dagger = -g_i$ and $g g_j g^\dagger = g_j$ for $j \neq i$. □

We conclude our look at the most basic elements of the stabilizer formalism by fulfilling our earlier promise that V_S is non-trivial provided S is generated by independent commuting generators and $-I \notin S$. Indeed, if there are $l = n-k$ generators, then it is at least plausible (and we will prove) that V_S is 2^k-dimensional, based on the intuitive argument that each additional generator for the stabilizer cuts the dimension of V_S by a factor of 1/2, as we might naively expect because the +1 and -1 eigenspaces for a tensor product of Pauli matrices divide the total Hilbert space into two subspaces of equal dimension.

Proposition 10.5: Let $S = \langle g_1 \ldots, g_{n-k} \rangle$ be generated by $n-k$ independent and commuting elements from G_n, and such that $-I \notin S$. Then V_S is a 2^k-dimensional vector space.

In all our later discussion of the stabilizer formalism we use the convention that stabilizers are always described in terms of independent commuting generators such that $-I \notin S$.

Proof

Let $x = (x_1, \ldots, x_{n-k})$ be a vector of $n-k$ elements of $\mathbf{Z}_2$. Define

$$P_S^x \equiv \frac{\prod_{j=1}^{n-k} (I + (-1)^{x_j} g_j)}{2^{n-k}}. \tag{10.85}$$

Because $(I + g_j)/2$ is the projector onto the +1 eigenspace of g_j, it is easy to see that $P_S^{(0,\ldots,0)}$ must be the projector onto V_S. By Proposition 10.4 for each x there exists g_x in G_n such that $g_x P_S^{(0,\ldots,0)} (g_x)^\dagger = P_S^x$, and therefore the dimension of P_S^x is the same as the dimension of V_S. Furthermore, for distinct x the P_S^x are easily seen to be orthogonal.

The proof is concluded with the algebraic observation that

$$I = \sum_x P_S^x \tag{10.86}$$

The left hand side is a projector onto a 2^n-dimensional space, while the right hand side is a sum over 2^{n-k} orthogonal projectors of the same dimension as V_S, and thus the dimension of V_S must be 2^k.

9.3.15 10.5.2 Unitary gates and the stabilizer formalism

We have been discussing the use of the stabilizer formalism to describe vector spaces. The formalism can also be used to describe the dynamics of those vector spaces in the larger state space, under a variety of interesting quantum operations. Aside from the intrinsic interest of understanding quantum dynamical operations, this goal is especially relevant because we will describe quantum error-correcting codes using the stabilizer formalism, and would like an elegant means for understanding the effects of noise and other dynamical processes on those codes. Suppose we apply a unitary operation U to a vector space V_S stabilized by the group S. Let $|\psi\rangle$ be any element of V_S. Then for any element g of S,

$$U|\psi\rangle = Ug|\psi\rangle = UgU^\dagger U|\psi\rangle, \tag{10.87}$$

and thus the state $U|\psi\rangle$ is stabilized by $UgU^\dagger$, from which we deduce that the vector space UV_S is stabilized by the group $USU^\dagger \equiv \left\{UgU^\dagger \mid g \in S\right\}$. Furthermore, if $g_1, \ldots, g_l$ generate S, then $Ug_1U^\dagger, \ldots, Ug_lU^\dagger$ generate $USU^\dagger$, so to compute the change in the stabilizer we need only compute how it affects the generators of the stabilizer.

The great advantage of this approach to dynamics is that for certain special unitary operations U this transformation of the generators takes on a particularly appealing form. Suppose, for example, that we apply a Hadamard gate to a single qubit. Note that

$$HXH^\dagger = Z; \quad HYH^\dagger = -Y; \quad HZH^\dagger = X. \tag{10.88}$$

As a consequence we correctly deduce that after a Hadamard gate is applied to the quantum state stabilized by $Z(|0\rangle)$, the resulting state will be stabilized by $X(|+\rangle)$.

Not very impressive, you may think! Imagine though that we had n qubits in a state whose stabilizer is $\langle Z_1, Z_2, \ldots, Z_n\rangle$. It is easy to see that this is the state $|0\rangle^{\otimes n}$. Applying the Hadamard gate to each of the n qubits we see that the state afterwards has a stabilizer $\langle X_1, X_2, \ldots, X_n\rangle$; again it is easy to see that this is just the familiar state which is an equal superposition of all computational basis states. What is remarkable about this example is that the usual (state vector) description of the final state requires 2^n amplitudes to be specified, compared with the description provided by the generators: $\langle X_1, \ldots, X_n\rangle$, which is linear in n! Still, you might say, after applying the Hadamard gate to each of the n qubits there is no entanglement in the quantum computer, so it is not so surprising that a compact description can be obtained. But much more is possible within the stabilizer formalism, including an efficient description of the controlled-not, which together with the Hadamard gate is capable of generating entanglement. To understand how this works, consider how the operators X_1, X_2, Z_1 and Z_2 behave under conjugation by the controlled-not. Denoting by U the controlled-not gate with qubit 1 as control

Operation	Input	Output
controlled-NOT	X_1	X_1X_2
	X_2	X_2
	Z_1	Z_1
	Z_2	Z_1Z_2
H	X	Z
	Z	X
S	X	Y
	Z	Z
X	X	X
	Z	$-Z$
Y	X	$-X$
	Z	$-Z$
Z	X	$-X$
	Z	Z

Figure 10.7. Transformation properties of elements of the Pauli group under conjugation by various common operations. The controlled-not has qubit 1 as the control and qubit 2 as the target.

and qubit 2 as the target, we have

$$
\begin{aligned}
UX_1U^\dagger &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \\
&= \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \\
&= X_1X_2. \qquad (10.89)
\end{aligned}
$$

Similar calculations show that $UX_2U^\dagger = X_2, UZ_1U^\dagger = Z_1$ and $UZ_2U^\dagger = Z_1Z_2$. To see how U conjugates other operators in the two qubit Pauli group we need only take products of the facts we already know. For example, to calculate $UX_1X_2U^\dagger$ we observe that $UX_1X_2U^\dagger = UX_1U^\dagger UX_2U^\dagger = (X_1X_2)\, X_2 = X_1$. The Y Pauli matrices may be dealt with similarly, as for example $UY_2U^\dagger = iUX_2Z_2U^\dagger = iUX_2U^\dagger UZ_2U^\dagger = iX_2\,(Z_1Z_2) = Z_1Y_2$.

Exercise 10.36: Explicitly verify that $UX_1U^\dagger = X_1X_2, UX_2U^\dagger = X_2, UZ_1U^\dagger = Z_1$, and $UZ_2U^\dagger = Z_1Z_2$. These and other useful conjugation relations for the Hadamard, phase, and Pauli gates are summarized in Figure 10.7.

Exercise 10.37: What is $UY_1U^\dagger$?

As an example of using the stabilizer formalism to understand unitary dynamics, consider the swap circuit introduced in Section 1.3.4 on page 23; for convenience, the circuit is illustrated in Figure 10.8. Consider the way the operators Z_1 and Z_2 transform
by conjugation by the gates in the circuit. The operator Z_1 transforms through the sequence $Z_1 \rightarrow Z_1 \rightarrow Z_1Z_2 \rightarrow Z_2$ and the operator Z_2 transforms through the sequence $Z_2 \rightarrow Z_1Z_2 \rightarrow Z_1 \rightarrow Z_1$. Similarly, $X_1 \rightarrow X_2$ and $X_2 \rightarrow X_1$ under the circuit. Of course, if we take U to be the swap operator then it is obvious that $UZ_1U^\dagger = Z_2$ and $UZ_2U^\dagger = Z_1$, and similarly for X_1 and X_2, just as for the circuit in Figure 10.8. Proving that this implies that the circuit implements U is left as an exercise:

Exercise 10.38: Suppose U and V are unitary operators on two qubits which transform Z_1, Z_2, X_1, and X_2 by conjugation in the same way. Show this implies that $U = V$.

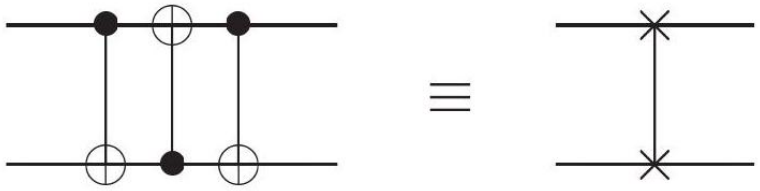


Figure 10.8. Circuit swapping two qubits.

The example of the swap circuit is interesting but doesn't do justice to the feature of the stabilizer formalism which makes it truly useful - the ability to describe certain types of quantum entanglement. We've already seen that the stabilizer formalism can be used to describe Hadamard gates and controlled-NOT gates, and of course these gates together can be used to create entangled states (compare Section 1.3.6). We will see that the stabilizer formalism can in fact be used to describe a wide class of entangled states, including many quantum error-correcting codes.

What gates other than the Hadamard and controlled-NOT gates can be described within the stabilizer formalism? The most important addition to this set is the phase gate, a single qubit gate whose definition we now recall,

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}. \tag{10.90}$$

The action of the phase gate by conjugation on the Pauli matrices is easily computed:

$$SXS^\dagger = Y; \quad SZS^\dagger = Z. \tag{10.91}$$

Exercise 10.39: Verify (10.91).

Indeed, it turns out that any unitary operation taking elements of G_n to elements of G_n under conjugation can be composed from the Hadamard, phase and controlled-NOT gates. By definition, we say the set of U such that $UG_nU^\dagger = G_n$ is the normalizer of G_n, and denote it by $N(G_n)$, so we are claiming that the normalizer of G_n is generated by the Hadamard, phase and controlled-not gates, in view of which the Hadamard, phase and controlled-NOT gates are sometimes referred to simply as the normalizer gates. The proof of this result is simple but instructive, and you will work through it in Exercise 10.40 on page 462.

Theorem 10.6: Suppose U is any unitary operator on n qubits with the property that if $g \in G_n$ then $UgU^\dagger \in G_n$. Then up to a global phase U may be composed from $O(n^2)$ Hadamard, phase and controlled-not gates.

Exercise 10.40: Provide an inductive proof of Theorem 10.6 as follows.

(1) Prove that the Hadamard and phase gates can be used to perform any normalizer operation on a single qubit.

(2) Suppose U is an $n+1$ qubit gate in $N(G_{n+1})$ such that $UZ_1U^\dagger = X_1 \otimes g$ and $UX_1U^\dagger = Z_1 \otimes g'$ for some $g, g' \in G_n$. Define U' on n qubits by $U'|\psi\rangle \equiv \sqrt{2}\langle 0|U(|0\rangle \otimes |\psi\rangle)$. Use the inductive hypothesis to show that the construction for U in Figure 10.9 may be implemented using $O(n^2)$ Hadamard, phase and controlled-not gates.

(3) Show that any gate $U \in N(G_{n+1})$ may be implemented using $O(n^2)$ Hadamard, phase and controlled-not gates.

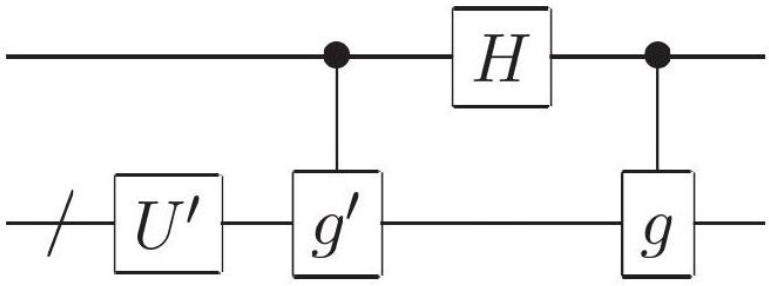


Figure 10.9. Construction used to prove that the Hadamard, phase and controlled-not gates generate the normalizer $N\left(G_{n}\right)$.

We've seen that many interesting quantum gates are in the normalizer $N(G_n)$; are there any gates which aren't? It turns out that most quantum gates are outside the normalizer. Two gates of particular interest which are not in the normalizer are the $\pi/8$ and Toffoli gates. Letting U denote the Toffoli gate with qubits 1 and 2 as controls and qubit 3 as the target, and recalling that T denotes the $\pi/8$ gate, we can easily calculate the action by conjugation of the $\pi/8$ and Toffoli gates on Pauli matrices as

$$TZT^\dagger = Z \quad TXT^\dagger = \frac{X+Y}{\sqrt{2}} \tag{10.92}$$

and

$$\begin{array}{rlrl} UZ_1U^\dagger & = Z_1 & UX_1U^\dagger & = X_1 \otimes \frac{I+Z_2+X_3-Z_2X_3}{2} \\ UZ_2U^\dagger & = Z_2 & UX_2U^\dagger = X_2 \otimes \frac{I+Z_1+X_3-Z_1X_3}{2} & \\ UX_3U^\dagger = X_3 & UZ_3U^\dagger = Z_3 \otimes \frac{I+Z_1+Z_2-Z_1Z_2}{2}. & & \end{array} \tag{10.95}$$

Unfortunately, this makes analyzing quantum circuits including $\pi/8$ and Toffoli gates via the stabilizer formalism much less convenient than circuits which only contain Hadamard, phase and controlled-not gates. Fortunately, encoding, decoding, error-detection and recovery for stabilizer quantum codes can all be accomplished using only such normalizer gates, so the stabilizer formalism is very convenient for the analysis of such codes!

Exercise 10.41: Verify Equations (10.92) through (10.95).

9.3.16 10.5.3 Measurement in the stabilizer formalism

We have explained how a limited class of unitary gates may be conveniently described within the stabilizer formalism, but even more is true! Measurements in the computational basis may also be easily described within the stabilizer formalism. To understand how this works, imagine we make a measurement of $g \in G_n$ (recall that g is a Hermitian operator, and can thus be regarded as an observable in the sense of Section 2.2.5). For convenience we assume without loss of generality that g is a product of Pauli matrices with no multiplicative factor of -1 or $\pm i$ out the front. The system is assumed to be in a state $|\psi\rangle$ with stabilizer $\langle g_1, \ldots, g_n \rangle$. How does the stabilizer of the state transform under this measurement? There are two possibilities:

- g commutes with all the generators of the stabilizer.
- g anti-commutes with one or more of the generators of the stabilizer. Suppose the stabilizer has generators $g_1, \ldots, g_n$, and that g anti-commutes with g_1. Without loss of generality we may assume that g commutes with $g_2, \ldots, g_n$, since if it does not commute with one of these elements (say g_2) then it is easy to verify that g does commute with $g_1 g_2$, and we simply replace the generator g_2 by $g_1 g_2$ in our list of generators for the stabilizer.

In the first instance it follows that either g or $-g$ is an element of the stabilizer by the following argument. Since $g_j g|\psi\rangle = g g_j|\psi\rangle = g|\psi\rangle$ for each stabilizer generator, $g|\psi\rangle$ is in V_S and is thus a multiple of $|\psi\rangle$. Because $g^2 = I$ it follows that $g|\psi\rangle = \pm|\psi\rangle$, whence either g or $-g$ must be in the stabilizer. We assume that g is in the stabilizer, with the discussion for $-g$ proceeding analogously. In this instance $g|\psi\rangle = |\psi\rangle$ and thus a measurement of g yields $+1$ with probability one, and the measurement does not disturb the state of the system, and thus leaves the stabilizer invariant.

What about the second instance, when g anti-commutes with g_1 and commutes with all the other generators of the stabilizer? Note that g has eigenvalues ± 1 and so the projectors for the measurement outcomes ± 1 are given by $(I \pm g)/2$, respectively, and thus the measurement probabilities are given by

$$p(+1) = \mathrm{tr}\left(\frac{I+g}{2}|\psi\rangle\langle\psi|\right) \tag{10.96}$$

$$p(-1) = \mathrm{tr}\left(\frac{I-g}{2}|\psi\rangle\langle\psi|\right). \tag{10.97}$$

Using the facts that $g_1|\psi\rangle = |\psi\rangle$ and $gg_1 = -g_1 g$ gives

$$p(+1) = \mathrm{tr}\left(\frac{I+g}{2} g_1 |\psi\rangle\langle\psi|\right) \tag{10.98}$$

$$= \mathrm{tr}\left(g_1 \frac{I-g}{2} |\psi\rangle\langle\psi|\right). \tag{10.99}$$

Applying the cyclic property of trace we may take g_1 to the right hand end of the trace and absorb it into $\langle\psi|$ using $g_1 = g_1^\dagger$ (Exercise 10.35 on page 457), giving

$$p(+1) = \mathrm{tr}\left(\frac{I-g}{2}|\psi\rangle\langle\psi|\right) = p(-1). \tag{10.100}$$

Since $p(+1) + p(-1) = 1$ we deduce that $p(+1) = p(-1) = 1/2$. Suppose the result $+1$ occurs. In this instance the new state of the system is $|\psi^+\rangle \equiv (I+g)|\psi\rangle/\sqrt{2}$, which has stabilizer $\langle g, g_2, \ldots, g_n\rangle$. Similarly, if the result -1 occurs the posterior state is stabilized by $\langle -g, g_2, \ldots, g_n\rangle$.

9.3.17 10.5.4 The Gottesman-Knill theorem

The results about using stabilizers to describe unitary dynamics and measurements may be summarized in the remarkable Gottesman-Knill theorem:

Theorem 10.7: (Gottesman-Knill theorem) Suppose a quantum computation is performed which involves only the following elements: state preparations in the computational basis, Hadamard gates, phase gates, controlled-not gates, Pauli gates, and measurements of observables in the Pauli group (which includes measurement in the computational basis as a special case), together with the possibility of classical control conditioned on the outcome of such measurements. Such a computation may be efficiently simulated on a classical computer.

We have already implicitly proved the Gottesman-Knill theorem. The way the classical computer performs the simulation is simply to keep track of the generators of the stabilizer as the various operations are being performed in the computation. For example, to simulate a Hadamard gate we simply update each of the n generators describing the quantum state. Similarly, simulation of the state preparation, phase gate, controllednot gate, Pauli gates, and measurements of observables in the Pauli group may all be done using $O(n^2)$ steps on a classical computer, so that a quantum computation involving m operations from this set can be simulated using $O(n^2 m)$ operations on a classical computer.

The Gottesman-Knill theorem highlights how subtle is the power of quantum computation. It shows that some quantum computations involving highly entangled states may be simulated efficiently on classical computers. Of course, not all quantum computations (and therefore, not all types of entanglement) can be described efficiently within the stabilizer formalism, but an impressive variety can be. Consider that interesting quantum information processing tasks such as quantum teleportation (Section 1.3.7) and superdense coding (Section 2.3) can be performed using only the Hadamard gate, controllednot gate, and measurements in the computational basis, and can therefore be efficiently simulated on a classical computer, by the Gottesman-Knill theorem. Moreover, we will shortly see that a wide variety of quantum error-correcting codes can be described within the stabilizer formalism. There is much more to quantum computation than just the power bestowed by quantum entanglement!

Exercise 10.42: Use the stabilizer formalism to verify that the circuit of Figure 1.13 on page 27 teleports qubits, as claimed. Note that the stabilizer formalism restricts the class of states being teleported, so in some sense this is not a complete description of teleportation, nevertheless it does allow an understanding of the dynamics of teleportation.

9.3.18 10.5.5 Stabilizer code constructions

The stabilizer formalism is ideally suited to the description of quantum codes. In this section we describe how this may be done, and use it to illustrate several important codes, such as Shor's nine qubit code, CSS codes, and a five qubit code which is the smallest
code that can be used to protect against the effects of arbitrary errors on a single qubit. The basic idea is very simple: an $[n, k]$ stabilizer code is defined to be the vector space V_S stabilized by a subgroup S of G_n such that $-I \notin S$ and S has $n-k$ independent and commuting generators, $S = \langle g_1, \ldots, g_{n-k} \rangle$. We denote this code $C(S)$.

What are the logical basis states for the code $C(S)$? In principle, given $n-k$ generators for the stabilizer S we can choose any 2^k orthonormal vectors in the code $C(S)$ to act as our logical computational basis states. In practice it makes a great deal more sense to choose the states in a more systematic way. One method is as follows. First, we choose operators $\bar{Z}_1, \ldots, \bar{Z}_k \in G_n$ such that $g_1, \ldots, g_{n-k}, \bar{Z}_1, \ldots, \bar{Z}_k$ forms an independent and commuting set. (We explain in detail how this may be done a little later.) The $\bar{Z}_j$ operator plays the role of a logical Pauli sigma z operator on logical qubit number j, so the logical computational basis state $|x_1, \ldots, x_k\rangle_L$ is therefore defined to be the state with stabilizer

$$\left\langle g_1, \ldots, g_{n-k}, (-1)^{x_1} \bar{Z}_1, \ldots, (-1)^{x_k} \bar{Z}_k \right\rangle \tag{10.101}$$

Similarly, we define $\bar{X}_j$ to be that product of Pauli matrices which takes $\bar{Z}_j$ to $-\bar{Z}_j$ under conjugation, and leaves all other $\bar{Z}_i$ and g_i alone when acting by conjugation. Clearly $\bar{X}_j$ has the effect of a quantum not gate acting on the j th encoded qubit. The operator $\bar{X}_j$ satisfies $\bar{X}_j g_k \bar{X}_j^\dagger = g_k$, and thus commutes with all the generators of the stabilizer. It is also easy to check that $\bar{X}_j$ commutes with all the $\bar{Z}_i$ except for $\bar{Z}_j$, with which it anti-commutes.

How are the error-correcting properties of a stabilizer code related to the generators of its stabilizer? Suppose we encode a state using an $[n, k]$ stabilizer code $C(S)$ with stabilizer $S = \langle g_1, \ldots, g_{n-k} \rangle$, and an error E occurs corrupting the data. In three stages of analysis we are going to determine what types of errors can be detected using $C(S)$ and when recovery can be performed. First, we'll take a look at the effect different types of errors have on the code space, simply to gain some intuition about what types of errors can be detected and corrected; there will be no proofs, as this stage is simply to build intuition. The second stage is the statement and proof of a general theorem telling us what kinds of errors can be detected and corrected by a stabilizer code, based upon the quantum error-correction conditions. The third stage of our analysis is to give a practical prescription for performing error-detection and recovery, using notions such as error syndrome.

Suppose $C(S)$ is a stabilizer code corrupted by an error $E \in G_n$. What happens to the code space when E anti-commutes with an element of the stabilizer? In this case E takes $C(S)$ to an orthogonal subspace, and the error can in principle be detected (and perhaps corrected after detection) by performing an appropriate projective measurement. If $E \in S$ we don't need to worry since the 'error' E doesn't corrupt the space at all. The real danger comes when E commutes with all the elements of S but is not actually in S, that is, $Eg = gE$ for all $g \in S$. The set of $E \in G_n$ such that $Eg = gE$ for all $g \in S$ is known as the centralizer of S in G_n and is denoted $Z(S)$. In fact, for the stabilizer groups S of concern to us, the centralizer is identical to a more familiar group, the normalizer of S, denoted $N(S)$, which is defined to consist of all elements E of G_n such that $EgE^\dagger \in S$ for all $g \in S$.

Exercise 10.43: Show that $S \subseteq N(S)$ for any subgroup S of G_n.

Exercise 10.44: Show that $N(S) = Z(S)$ for any subgroup S of G_n not containing $-I$.

These observations about the effect of various types of error operator E motivate the statement and proof of the following theorem, which is essentially just a translation of the quantum error-correction conditions (Theorem 10.1) into the terms of stabilizer codes.

Theorem 10.8: (Error-correction conditions for stabilizer codes) Let S be the stabilizer for a stabilizer code $C(S)$. Suppose $\{E_j\}$ is a set of operators in G_n such that $E_j^\dagger E_k \notin N(S) - S$ for all j and k. Then $\{E_j\}$ is a correctable set of errors for the code $C(S)$.

Without loss of generality we can restrict ourselves to considering errors E_j in G_n such that $E_j^\dagger = E_j$, which reduces the error-correction conditions for stabilizer codes to having $E_j E_k \notin N(S) - S$ for all j and k.

Proof

Let P be the projector onto the code space $C(S)$. For given j and k there are two possibilities: either $E_j^\dagger E_k$ in S or $E_j^\dagger E_k$ in $G_n - N(S)$. Consider the first case. Then $P E_j^\dagger E_k P = P$ since P is invariant under multiplication by elements of S. Suppose $E_j^\dagger E_k \in G_n - N(S)$ so that $E_j^\dagger E_k$ must anticommute with some element g_1 of S. Let $g_1, \ldots, g_{n-k}$ be a set of generators of S, so that

$$P = \frac{\prod_{l=1}^{n-k} (I + g_l)}{2^{n-k}} \tag{10.102}$$

Using the anti-commutativity gives

$$E_j^\dagger E_k P = (I - g_1) E_j^\dagger E_k \frac{\prod_{l=2}^{n-k} (I + g_l)}{2^{n-k}}. \tag{10.103}$$

But $P(I - g_1) = 0$ since $(I + g_1)(I - g_1) = 0$ and therefore $P E_j^\dagger E_k P = 0$ whenever $E_j^\dagger E_k \in G_n - N(S)$. It follows that the set of errors $\{E_j\}$ satisfies the quantum errorcorrection conditions, and thus forms a correctable set of errors. $\square$

The statement and proof of Theorem 10.8 are wonderful theoretical results, but they don't explicitly tell us how to perform the error-correction operation when it is in fact possible! To understand how this is achieved, suppose $g_1, \ldots, g_{n-k}$ is a set of generators for the stabilizer of an $[n, k]$ stabilizer code, and that $\{E_j\}$ is a set of correctable errors for the code. Error-detection is performed by measuring the generators of the stabilizer g_1 through g_{n-k} in turn, to obtain the error syndrome, which consists of the results of the measurements, β_1 through β_{n-k}. If the error E_j occurred then the error syndrome is given by β_l such that $E_j g_l E_j^\dagger = \beta_l g_l$. In the case when E_j is the unique error operator having this syndrome recovery may be achieved simply by applying $E_j^\dagger$. In the case when there are two distinct errors E_j and $E_{j'}$ giving rise to the same error syndrome, it follows that $E_j P E_j^\dagger = E_{j'} P E_{j'}^\dagger$, where P is the projector onto the code space, so $E_j^\dagger E_{j'} P E_{j'}^\dagger E_j = P$, whence $E_j^\dagger E_{j'} \in S$, and thus applying $E_j^\dagger$ after the error $E_{j'}$ has occurred results in a successful recovery. Thus, for each possible error syndrome we simply pick out a single error E_j with that syndrome, and apply $E_j^\dagger$ to achieve recovery when that syndrome is observed.

Theorem 10.8 motivates the definition of a notion of distance for a quantum code analogous to the distance for a classical code. We define the weight of an error $E \in G_n$ to be the number of terms in the tensor product which are not equal to the identity. For example, the weight of $X_1 Z_4 Y_8$ is three. The distance of a stabilizer code $C(S)$ is defined to be the minimum weight of an element of $N(S) - S$, and if $C(S)$ is an $[n, k]$ code with distance d then we say that $C(S)$ is an $[n, k, d]$ stabilizer code. By Theorem 10.8 a code with distance at least $2t + 1$ is able to correct arbitrary errors on any t qubits, just as in the classical case.

Exercise 10.45: (Correcting located errors) Suppose $C(S)$ is an $[n, k, d]$ stabilizer code. Suppose k qubits are encoded in n qubits using this code, which is then subjected to noise. Fortunately, however, we are told that only $d - 1$ of the qubits are affected by the noise, and moreover, we are told precisely which $d - 1$ qubits have been affected. Show that it is possible to correct the effects of such located errors.

9.3.19 10.5.6 Examples

We now give a few simple examples of stabilizer codes, including already familiar codes such as the Shor nine qubit code and CSS codes, but from the new point of view of the stabilizer formalism. In each case, the properties of the codes follow easily by applying Theorem 10.8 to the generators of the stabilizer. With the examples under our belt we will turn our attention to finding quantum circuits for performing encoding and decoding.

The three qubit bit flip code

Consider the familiar three qubit bit flip code spanned by the states $|000\rangle$ and $|111\rangle$, with stabilizer generated by Z_1Z_2 and Z_2Z_3. By inspection we see that every possible product of two elements from the error set $\{I, X_1, X_2, X_3\} - I, X_1, X_2, X_3, X_1X_2, X_1X_3, X_2X_3$ - anti-commutes with at least one of the generators of the stabilizer (except for I, which is in S), and thus by Theorem 10.8 the set $\{I, X_1, X_2, X_3\}$ forms a correctable set of errors for the three qubit bit flip code with stabilizer $\langle Z_1Z_2, Z_2Z_3\rangle$.

Error-detection for the bit flip code is effected by measuring the stabilizer generators, Z_1Z_2 and Z_2Z_3. If, for example, the error X_1 occurred, then the stabilizer is transformed to $\langle -Z_1Z_2, Z_2Z_3\rangle$, so the syndrome measurement gives the results -1 and +1 . Similarly, the error X_2 gives error syndrome -1 and -1 , the error X_3 gives error syndrome +1 and -1 , and the trivial error I gives error syndrome +1 and +1 . In each instance recovery is effected in the obvious way simply by applying the inverse operation to the error indicated by the error syndrome. The error-correction operation for the bit flip code is summarized in Figure 10.10.

Of course, the procedure we have outlined is exactly the same as that described earlier for the three qubit bit flip code! All this group-theoretic analysis would hardly be worthwhile if this was all the insight we gained. The real utility of the stabilizer formalism only starts to become apparent as we move to more complex examples.

Exercise 10.46: Show that the stabilizer for the three qubit phase flip code is generated by X_1X_2 and X_2X_3.

Z_1Z_2	Z_2Z_3	Error type	Action
+1	+1	no error	no action
+1	-1	bit 3 flipped	flip bit 3
-1	+1	bit 1 flipped	flip bit 1
-1	-1	bit 2 flipped	flip bit 2

Figure 10.10. Error-correction for the three qubit bit flip code in the language of stabilizer codes.

Name	Operator
g_1	$ZZIIIIIIIII$
g_2	$IZIIIIIIIII$
g_3	$IIIIZIIIIII$
g_4	$IIIIIIZZIIII$
g_5	$IIIIIIIIZII$
g_6	$IIIIIIIIIZI$
g_7	$XXXXXXIIII$
g_8	$IIIIXXXXXX$
$\bar{Z}$	$XXXXXXXXX$
$\bar{X}$	$ZZZZZZZZ$

Figure 10.11. The eight generators for the Shor nine qubit code, and the logical Z and logical X operations. (Yes, they really are the reverse of what one might naively expect!)

The nine qubit Shor code

The stabilizer for the Shor code has eight generators, as illustrated in Figure 10.11. It is easy to check the conditions of Theorem 10.8 for the error set containing I and all single qubit errors. Consider, for example, single qubit errors like X_1 and Y_4. The product X_1Y_4 anti-commutes with Z_1Z_2, and thus is not in $N(S)$. Similarly, all other products of two errors from this error set are either in S or else anti-commute with at least one element of S and thus are not in $N(S)$, implying that the Shor code can be used to correct an arbitrary single qubit error.

Exercise 10.47: Verify that the generators of Figure 10.11 generate the two codewords of Equation (10.13).

Exercise 10.48: Show that the operations $\bar{Z} = X_1X_2X_3X_4X_5X_6X_7X_8X_9$ and $\bar{X} = Z_1Z_2Z_3Z_4Z_5Z_6Z_7Z_8Z_9$ act as logical Z and X operations on a Shor-code encoded qubit. That is, show that this $\bar{Z}$ is independent of and commutes with the generators of the Shor code, and that $\bar{X}$ is independent of and commutes with the generators of the Shor code, and anti-commutes with $\bar{Z}$.

The five qubit code

What is the minimum size for a quantum code which encodes a single qubit so that any error on a single qubit in the encoded state can be detected and corrected? It turns out that the answer to this question is five qubits. (See Section 12.4.3). The stabilizer for

Name	Operator
g_1	$XZZXI$
g_2	$IXZZX$
g_3	$XIXZZ$
g_4	$ZXIXZ$
$\bar{Z}$	$ZZZZZ$
$\bar{X}$	$XXXXX$

Figure 10.12. The four generators for the five qubit code, and the logical Z and logical X operations. Note that the last three generators may be obtained by shifting the first right.

the five qubit code has the generators given in Figure 10.12. Because the five qubit code is the smallest capable of protecting against a single error it might be thought that it is the most useful code; however, for many applications it is more transparent to use the Steane seven qubit code.

Exercise 10.49: Use Theorem 10.8 to verify that the five qubit code can protect against an arbitrary single qubit error.

The logical codewords for the five qubit code are

$$\begin{aligned}|0_L\rangle = \frac{1}{4}[&|00000\rangle + |10010\rangle + |01001\rangle + |10100\rangle \\ &+ |01010\rangle - |11011\rangle - |00110\rangle - |11000\rangle \\ &- |11101\rangle - |00011\rangle - |11110\rangle - |01111\rangle \\ &- |10001\rangle - |01100\rangle - |10111\rangle + |00101\rangle] \end{aligned} \tag{10.104}$$

$$\begin{aligned}|1_L\rangle = \frac{1}{4}[&|11111\rangle + |01101\rangle + |10110\rangle + |01011\rangle \\ &+ |10101\rangle - |00100\rangle - |11001\rangle - |00111\rangle \\ &- |00010\rangle - |11100\rangle - |00001\rangle - |10000\rangle \\ &- |01110\rangle - |10011\rangle - |01000\rangle + |11010\rangle] \end{aligned} \tag{10.105}$$

Exercise 10.50: Show that the five qubit code saturates the quantum Hamming bound, that is, it satisfies the inequality of (10.51) with equality.

CSS codes and the seven qubit code

The CSS codes are an excellent example of a class of stabilizer codes, demonstrating beautifully how easy the stabilizer formalism makes it to understand quantum code construction. Suppose C_1 and C_2 are $[n, k_1]$ and $[n, k_2]$ classical linear codes such that $C_2 \subset C_1$ and C_1 and $C_2^\perp$ both correct t errors. Define a check matrix with the form

$$\left[\begin{array}{c|c} H\left(C_2^\perp\right) & 0 \\ 0 & H\left(C_1\right) \end{array}\right]. \tag{10.106}$$

To see that this defines a stabilizer code, we need the check matrix to satisfy the commutativity condition $H\left(C_2^\perp\right) H\left(C_1\right)^T = 0$. But we have $H\left(C_2^\perp\right) H\left(C_1\right)^T = \left[H\left(C_1\right) G\left(C_2\right)\right]^T = 0$ because of the assumption $C_2 \subset C_1$. Indeed, it's an easy exercise to see that this code is exactly $\mathrm{CSS}\left(C_1, C_2\right)$, and that it is capable of correcting arbitrary errors on any t qubits.

The seven qubit Steane code is an example of a CSS code, whose check matrix we have already seen, in Equation (10.83). Encoded Z and X operators may be defined for the Steane code as

$$\bar{Z} \equiv Z_1 Z_2 Z_3 Z_4 Z_5 Z_6 Z_7; \quad \bar{X} \equiv X_1 X_2 X_3 X_4 X_5 X_6 X_7. \tag{10.107}$$

Exercise 10.51: Verify that the check matrix defined in (10.106) corresponds to the stabilizer of the CSS code $\mathrm{CSS}\left(C_1, C_2\right)$, and use Theorem 10.8 to show that arbitrary errors on up to t qubits may be corrected by this code.

Exercise 10.52: Verify by direct operation on the codewords that the operators of (10.107) act appropriately, as logical Z and X.

9.3.20 10.5.7 Standard form for a stabilizer code

The construction of the logical Z and X operators for a stabilizer code is made much easier to understand if we put the code into standard form. To understand what the standard form is, consider the check matrix for an $[n, k]$ stabilizer code C :

$$G = [G_1 \mid G_2]\,. \tag{10.108}$$

This matrix has $n - k$ rows. Swapping rows of this matrix corresponds to relabeling generators, swapping corresponding columns on both sides of the matrix to relabeling qubits, and adding two rows corresponds to multiplying generators; it is easy to see that we may always replace a generator g_i by $g_i g_j$ when $i \neq j$. Thus there is an equivalent code with a different set of generators whose corresponding check matrix corresponds to the matrix G where Gaussian elimination has been done on G_1, swapping qubits as necessary:

$$n-k-r\left\{\left[\begin{array}{cc|cc} r & \overbrace{I}^{r} & \overbrace{A}^{n-r} & \overbrace{B}^{r} \\ 0 & 0 & \overbrace{C}^{r} & E \end{array}\right]\right., \tag{10.109}$$

where r is the rank of G_1. Next, swapping qubits as necessary we perform a Gaussian elimination on E to obtain

$$n-k-r-s\left\{\left[\begin{array}{ccc|ccc} & \overbrace{}^{r} & \overbrace{}^{n-k-r-s} & \overbrace{}^{k+s} & \overbrace{}^{r} & \overbrace{}^{n-k-s} \\ r & I & A_1 & A_2 & B & C_1 \\ & & & \overbrace{}^{k+s} & & \\ s\{ & 0 & 0 & C_2 & & \\ 0 & 0 & 0 & I & E_2 & \\ D_2 & 0 & 0 & & & \end{array}\right]\right.. \tag{10.110}$$

The last s generators cannot commute with the first r generators unless $D_2 = 0$, and thus we may assume that $s = 0$. Furthermore, we may also set $C_1 = 0$ by taking appropriate linear combinations of rows, so our check matrix has the form:

$$n-k-r\left\{\left[\begin{array}{ccc|ccc} \overbrace{I}^{r} & \overbrace{A_1}^{n-k-r} & \overbrace{A_2}^{k} & \overbrace{B}^{r} & \overbrace{0}^{n} & \overbrace{C}^{k} \\ 0 & 0 & 0 & D & I & E \end{array}\right]\right., \tag{10.111}$$

where we have relabeled E_2 as E and D_1 as D. It is not difficult to see that this procedure is not unique; however, we will say that any code with check matrix in the form (10.111) is in standard form.

Given the standard form for a quantum code it is easy to define encoded Z operations for the code. That is, we have to pick k operators independent of the generators of the stabilizer and of one another, yet commuting with one another, and also with the generators of the stabilizer. Suppose we write the check matrix for these k encoded Z operators in the form $G_z = [F_1 F_2 F_3 \mid F_4 F_5 F_6]$, where all the matrices have k rows, and the respective column sizes are $r, n-k-r, k, r, n-k-r$ and k. We choose these matrices such that $G_z = \left[000 \mid A_2^T 0 I\right]$. The commutativity of these encoded Z operations with the elements of the stabilizer follows from the equation $I \times \left(A_2^T\right)^T + A_2 = 0$, and it is clear that the encoded Z operations commute with one another since they only contain products of Z operators. The independence of the encoded Z operators from the first r generators of the stabilizer follows from the fact that no X terms appear in the definition of the encoded Z operators, the independence from the set of $n-k-r$ generators follows from the $(n-k-r) \times (n-k-r)$ identity matrix appearing in the check matrix for those generators, and the lack of any corresponding terms in the check

matrix for the encoded Z operators. In a similar way we may pick the encoded X operators, with $k \times 2n$ check matrix $\left[0E^T I \mid C^T 00\right]$.

Exercise 10.53: Prove that the encoded Z operators are independent of one another.
Exercise 10.54: Prove that with the check matrix for the encoded X operators defined as above, the encoded X operators are independent of one another and of the generators, commute with the generators of the stabilizer, with each other, and $\bar{X}_j$ commutes with all the $\bar{Z}_k$ except $\bar{Z}_j$, with which it anti-commutes.

As an example we bring the check matrix for the Steane code (Equation 10.83) into standard form. We have $n = 7$ and $k = 1$ for this code, and inspection of the check matrix shows that the rank of the σ_x part is $r = 3$. The matrix may be brought into standard form by swapping qubits 1 and 4,3 and 4 , and 6 and 7 , then by adding row 6 to row 4 , then row 6 to row 5 , and finally adding rows 4 and 5 to row 6 . The resulting standard form is:

$$\left[\begin{array}{ccccccc|ccccccc} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \end{array}\right]. \tag{10.112}$$

We read off $A_2 = (1, 1, 0)$ and thus the encoded Z has check matrix $[0000000 \mid 1100001]$, which corresponds to $\bar{Z} = Z_1 Z_2 Z_7$. Recalling that qubits 1 and 4, 3 and 4, 6 and 7 were swapped, this corresponds to an encoded Z of $\bar{Z} = Z_2 Z_4 Z_6$ in the original code. This may appear rather puzzling in the light of Equation (10.107), which states that the encoded Z is $\bar{Z} = Z_1 Z_2 Z_3 Z_4 Z_5 Z_6 Z_7$; however, the puzzle is resolved by noting that the two 'different' encoded Z operations differ only by a factor $Z_1 Z_3 Z_5 Z_7$, which is an element of the stabilizer of the Steane code, and thus both have the same effect on Steane code states.

Exercise 10.55: Find the $\bar{X}$ operator for the standard form of the Steane code.
Exercise 10.56: Show that replacing an encoded X or Z operator by g times that operator, where g is an element of the stabilizer, does not change the action of the operator on the code.

Exercise 10.57: Give the check matrices for the five and nine qubit codes in standard form.

9.3.21 10.5.8 Quantum circuits for encoding, decoding, and correction

One of the features of stabilizer codes is that their structure enables systematic construction of procedures for encoding, decoding, and error-correction. We describe the general method first, then present some explicit circuit constructions as examples. Let us begin with a general case, an $[n, k]$ stabilizer code with generators $g_1, \ldots, g_{n-k}$, and logical Z operators $Z_1, \ldots, \bar{Z}_k$.

Preparing an encoded $|0\rangle^{\otimes k}$ state, which is the standard state for beginning a quantum computation, is quite simple. To do this we can start with any easily-prepared state say, the state $|0\rangle^{\otimes n}$ - and measure each of the observables $g_1, \ldots, g_{n-k}, Z_1, \ldots, Z_k$ in turn. Depending on the measurement outcomes the resulting quantum state will have stabilizer $\langle \pm g_1, \ldots, \pm g_{n-k}, \pm Z_1, \ldots, \pm Z_k \rangle$, with the various signs being determined by the respective measurement outcomes. The signs of all the stabilizer generators and the $\bar{Z}_j$ can then be fixed up by applying products of Pauli operators, as described in the proof of Proposition 10.4, resulting in a state with stabilizer $\left\langle g_1, \ldots, g_{n-k}, \bar{Z}_1, \ldots, \bar{Z}_k \right\rangle$, that is, to the encoded $|0\rangle^{\otimes k}$. Once this state is prepared it is possible to change it to an arbitrary encoded computational basis state $|x_1, \ldots, x_k\rangle$ by applying the appropriate operators from the set $\bar{X}_1, \ldots, \bar{X}_k$. Of course, this approach to encoding has the disadvantage that it is not unitary. To obtain fully

unitary encoding a different approach based upon the standard form of the check matrix may be used; this approach is outlined in Problem 10.3. Also, if you wish to encode an unknown state, this can also be done systematically, starting from an encoded $|0\rangle^{\otimes k}$ state, as explained in Problem 10.4. For our purposes it will be sufficient to prepare encoded $|0\rangle^{\otimes k}$ states.

Decoding quantum codes is also quite simple, however it is worth explaining why, for many purposes, a full decoding is not necessary. It turns out that the techniques of fault-tolerant quantum computation can be used to perform logical operations directly on encoded data, without the need to decode the data. Furthermore, the output of a computation performed in this way can be directly determined simply by measuring the logical Z operators, without the need to decode and measure in the computational basis. Thus, doing a fully unitary decoding which preserves the encoded quantum information is not so important for our purposes. If such a decoding procedure is desired for some reason - perhaps one is using quantum error-correcting codes to transmit information over a noisy communication channel - then it may be achieved by running the unitary encoding circuit found in Problem 10.3 backwards.

The error-correction procedure for a stabilizer code has already been described in Section 10.5.5, and is much like the encoding procedure: simply measure each of the generators $g_1, \ldots g_{n-k}$ in turn, obtaining the error syndrome $\beta_1, \ldots, \beta_{n-k}$. Classical computation is then used to determine from β_j the required recovery operations $E_j^\dagger$.

The key to constructing encoding, decoding, and error-correction circuits in each of the above descriptions is understanding how to measure operators. Recall that this is a generalization of the normal projective measurements we have widely used, in which the objective is to project a state into an eigenstate of the operator and to obtain both
the projected state, and an indicator of the eigenvalue. If this reminds you of the phase estimation algorithm of Chapter 5, it's no coincidence! Recall from that chapter, and from Exercise 4.34 on page 188, that the circuit shown in Figure 10.13 can be used to measure the single qubit operator M (with eigenvalues ± 1), given a gate which performs a controlled- M operation. Two useful versions of this circuit, which measure X and Z, are given in Figures 10.14 and 10.15.

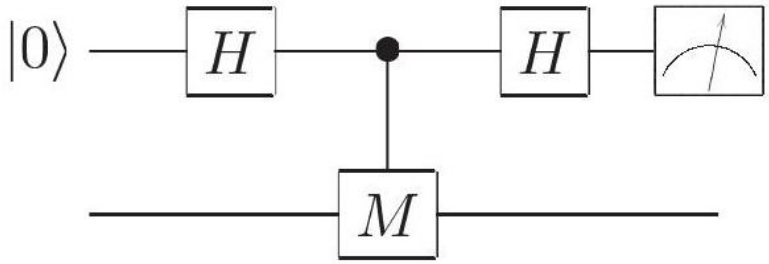


Figure 10.13. Quantum circuit for measuring a single qubit operator M with eigenvalues ± 1. The top qubit is the ancilla used for the measurement, and the bottom qubit is being measured.

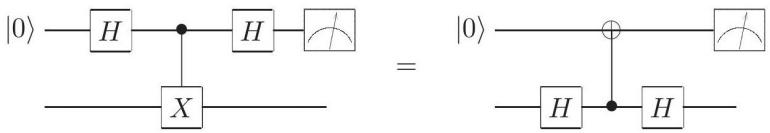


Figure 10.14. Quantum circuit for measuring the X operator. Two equivalent circuits are given; the one on the left is the usual construction (as in Figure 10.13), and the one on the right is a useful equivalent circuit.

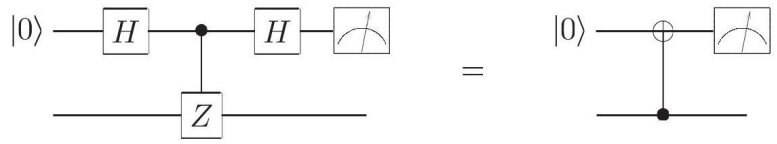


Figure 10.15. Quantum circuit for measuring the Z operator. Two equivalent circuits are given; the one on the left is the usual construction (as in Figure 10.13), and the one on the right is a useful simplification.

Of course, there is nothing special about the fact that M is a single qubit operator: the circuit in Figure 10.13 works just as well if we replace the second qubit with a bundle of qubits, and M is an arbitrary Hermitian operator with eigenvalues ± 1. Such operators include, for example, the products of Pauli operators we need to measure during the encoding, decoding and error-correction procedures for stabilizer codes.

As a concrete example, consider the syndrome measurement and encoding procedures for the seven qubit Steane code. A convenient starting point is the standard form of the check matrix for the code, Equation (10.112), because we can immediately read off the generators we need to measure directly from this matrix. Specifically, recall that the left block corresponds to X generators, and the right, Z, so the quantum circuit shown in Figure 10.16 immediately results. Note how the location of the zeroes and ones in the matrix corresponds to the location of the targets for the gates in the left half (which measure X), and the targets in the right half (which measure Z). This circuit can be used to perform error-correction by following the measurement results with products of Pauli operators on the code qubits to correct the errors. Or, by adding an additional
measurement of $\bar{Z}$ and fixing the signs in the generators of the stabilizer, as described earlier, the circuit can be used to prepare the encoded logical state $|0_L\rangle$.

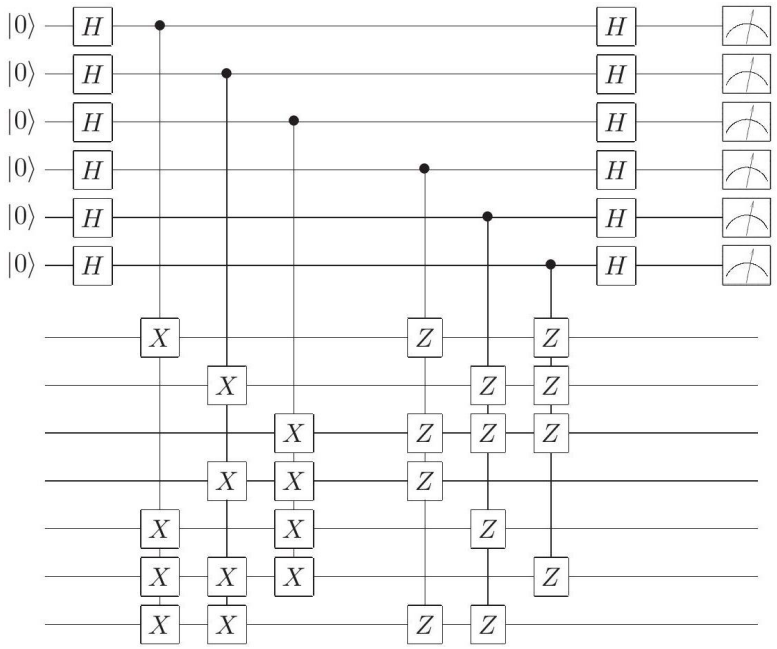


Figure 10.16. Quantum circuit for measuring the generators of the Steane code, to give the error syndrome. The top six qubits are the ancilla used for the measurement, and the bottom seven are the code qubits.

Exercise 10.58: Verify that the circuits in Figures 10.13-10.15 work as described, and check

the claimed circuit equivalences.

Exercise 10.59: Show that by using the identities of Figures 10.14 and 10.15, the syndrome circuit of Figure 10.16 can be replaced with the circuit of Figure 10.17

Exercise 10.60: Construct a syndrome measuring circuit analogous to that in Figure 10.16, but for the nine and five qubit codes.

Exercise 10.61: Describe explicit recovery operations $E_j^\dagger$ corresponding to the different possible error syndromes that may be measured using the circuit in Figure 10.16.

9.3.22 10.6 Fault-tolerant quantum computation

One of the most powerful applications of quantum error-correction is not merely the protection of stored or transmitted quantum information, but the protection of quantum information as it dynamically undergoes computation. Remarkably, it turns out that arbitrarily good quantum computation can be achieved even with faulty logic gates, provided only that the error probability per gate is below a certain constant threshold. Over

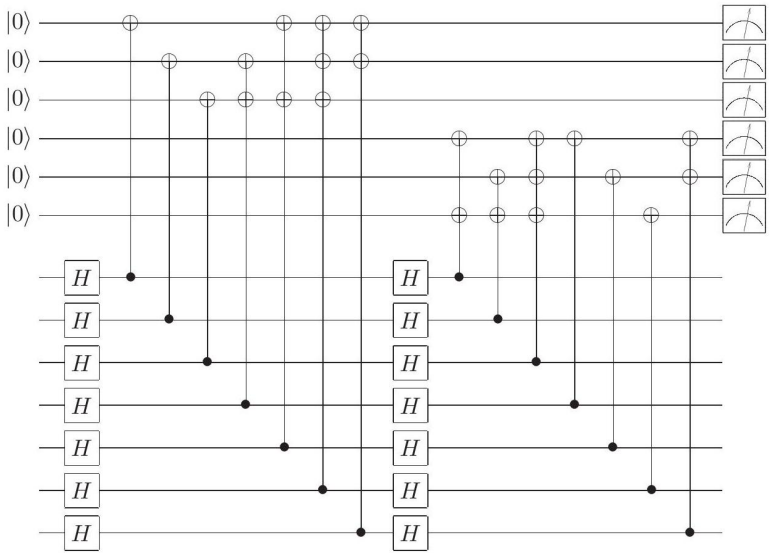


Figure 10.17. Quantum circuit equivalent to the one in Figure 10.16.

the next few sections we explain the techniques of fault-tolerant quantum computation which are used to achieve this remarkable result. We look first at the big picture in Section 10.6.1, before examining in detail the various elements of fault-tolerant quantum computation in Sections 10.6.2 and 10.6.3, and conclude in Section 10.6.4 with a discussion of some of the limitations and possible extensions of the fault-tolerant constructions. Note that a rigorous discussion of the many subtleties of fault-tolerant quantum computation lies somewhat beyond our scope; the interested reader is referred to the end of chapter 'History and further reading'.

9.3.23 10.6.1 Fault-tolerance: the big picture

The theory of fault-tolerant quantum computation integrates many different ideas en route to the threshold condition. We now describe each of these ideas in turn. We begin with the notion of computing on encoded data, and explain how the fundamental problems of error propagation and error accumulation require that our circuits for computing on encoded data satisfy certain fault-tolerance criteria. We then introduce our fundamental noise model for quantum circuits, which allows us to give more precise definitions for the notion of a fault-tolerant operation. We work through a specific example of a faulttolerant operation in action -

the fault-tolerant controlled-NOT - explaining how it can be used to prevent the propagation and accumulation of errors. We conclude by explaining how fault-tolerant operations can be combined with a procedure known as concatenation to obtain the threshold theorem for quantum computation, and give a simple estimate for the threshold.

Fundamental issues

The basic idea of fault-tolerant quantum computation is to compute directly on encoded quantum states in such a manner that decoding is never required. Suppose we are given a simple quantum circuit such as that shown in Figure 10.18. Unfortunately, noise afflicts each of the elements used to build this circuit - the state preparation procedures, quantum logic gates, measurement of the output, and even the simple transmission of quantum information along the quantum wires. To combat the effect of this noise we replace each qubit in the original circuit with an encoded block of qubits, using an error-correcting code such as the seven qubit Steane code, and replace each gate in the original circuit with a procedure for performing an encoded gate acting on the encoded state, as shown in Figure 10.19. By performing error-correction periodically on the encoded state we prevent accumulation of errors in the state. Of course, merely performing error-correction periodically is not sufficient to prevent the build-up of errors, even if it is applied after every encoded gate. The reasons for this are two-fold. First, and most importantly, the encoded gates can cause errors to propagate. For example, the encoded controlled-not illustrated in Figure 10.20 may cause an error on the encoded control qubit to propagate to the encoded target qubit. Thus errors in the qubits forming the encoded control qubit can propagate to become errors in the encoded target qubit. Encoded gates should therefore be designed very carefully so that a failure anywhere during the procedure for performing the encoded gate can only propagate to a small number of qubits in each block of the encoded data, in order that error-correction will be effective at removing the errors. Such procedures for performing encoded gates are referred to as fault-tolerant procedures, and we will show that it is possible to perform a universal set of logical operations - the Hadamard, phase, controlled-not and $\pi/8$ gates - using fault-tolerant procedures. The second issue that must be addressed is that error-correction itself can introduce errors on the encoded qubits, so we must be careful to design error-correction procedures that do not introduce too many errors into the encoded data. This can be achieved using techniques similar to those used to prevent propagation of errors by encoded gates, by taking care to ensure that failures during the procedure for errorcorrection do not propagate to cause too many errors in the encoded data.

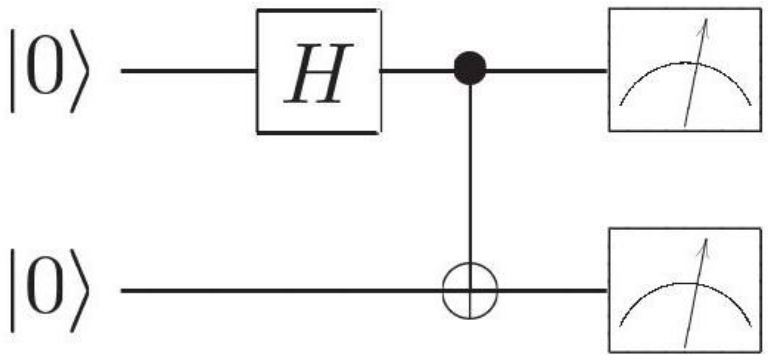


Figure 10.18. A simple quantum circuit. If each component in the circuit fails with probability p then the probability of an error at the output is $O(p)$.

Fault-tolerant operations: definitions

Let's pin down a little more precisely what it means for a particular procedure implementing an encoded quantum gate to be fault-tolerant. We define the fault-tolerance of a procedure to be the property that if only one component in the procedure fails then the failure causes at most one error in each encoded block of qubits output from the procedure. For example, the failure of a single component in a fault-tolerant recovery

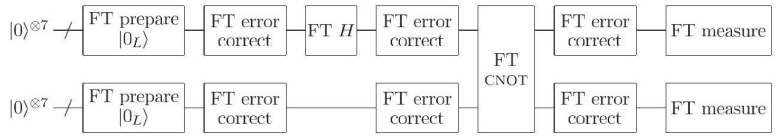


Figure 10.19. A simulation of the circuit in Figure 10.18, using encoded qubits and encoded logical operations. If fault-tolerant procedures are used to perform all the operations then the probability of error at the output is $O\left(p^{2
\right)$, where p is the probability for any individual component in the circuit to fail. An interesting feature is the second error-correction step performed on the second qubit. The 'operation' being error-corrected by this step appears to be trivial: nothing happens to the qubit at all! Nevertheless, simply storing qubits for a period of time introduces errors into the qubits, and should be periodically error-corrected in order to prevent the accumulation of errors.}

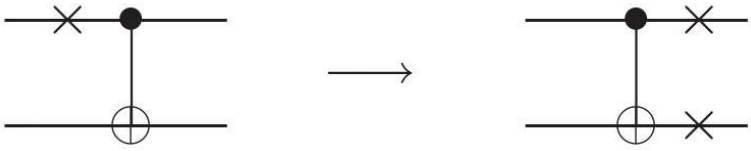


Figure 10.20. A controlled-NOT gate can cause an error to propagate so that instead of affecting one qubit, it affects two. This is also true when encoded qubits are used, and an encoded controlled-not is implemented, as discussed in the text.

procedure for quantum error-correction results in the recovery procedure being performed correctly, up to an error on a single qubit of the output. By 'component' we mean any of the elementary operations used in the encoded gate, which might include noisy gates, noisy measurements, noisy quantum wires, and noisy state preparations. This definition of a fault-tolerant procedure for a quantum gate is sometimes generalized in the literature to cope with some of the more subtle issues that arise in the theory of fault-tolerant computation, but at our level of detail it is sufficient.

Of course, encoded quantum gates aren't all we wish to perform during our quantum computations. It is also useful to define the notions of a fault-tolerant measurement procedure, and fault-tolerant state preparation. A procedure for measuring an observable on a set of encoded qubits is said to be fault-tolerant if the failure of any single component in the procedure results in an error in at most one qubit in each encoded block of qubits at the output of the procedure. Furthermore, we require that if only one component fails then the measurement result reported must have probability of error of $O\left(p^2\right)$, where p is the (maximum) probability of a failure in any one of the components used to implement the measurement procedure. A procedure for preparing a fixed encoded state is said to be fault-tolerant if, given that a single component

failed during the procedure, there is at most a single qubit in error in each encoded block of qubits output from the procedure.

To make these notions of fault-tolerance more precise, we need to be a little more specific about our error model. One of the major simplifications we are going to make in our analysis is to describe errors on qubits as being of one of four types: I, X, Y or Z, occurring stochastically with appropriate probabilities. We allow correlated errors to occur on two qubits, when performing gates such as the controlled-not, but again will assume that they are of the form of a tensor product of Pauli matrices, occurring with some probability. This probabilistic analysis enables us to use familiar concepts from classical probability theory to determine the total probability that the output from a circuit is correct or not. In more sophisticated presentations of fault-tolerance (see
'History and further reading') much more general error models can be considered, for example, allowing correlated errors of arbitrary type across several qubits. Nevertheless, the techniques used in those more sophisticated analyses are essentially generalizations of those we describe, combined with the deep insight we obtained earlier in the chapter that to perform error-correction of a continuum of possible errors it suffices to correct a discrete set of errors.

With our noise model at hand, we can be more precise about what we mean when we say that an error 'propagates' through the circuit. Consider, for example, the CNOT gate in Figure 10.20. Imagine that an X error on the first qubit occurs just before the CNOT is applied. If the unitary operator for the CNOT gate is denoted U, then the effective action of the circuit is $UX_1 = UX_1U^\dagger U = X_1X_2U$, that is, it is as though the controlled-not was applied correctly, but an X error occurred on both qubits after the CNOT. Over the remainder of this chapter we repeatedly use this trick of conjugating errors through gates to study how errors propagate through our circuits. A slightly more challenging example of error propagation is to suppose it is the CNOT gate itself which fails. What happens then? Suppose our noisy CNOT gate implements the quantum operation $\mathcal{E}$. Then this may be rewritten as $\mathcal{E} = \mathcal{E} \circ \mathcal{U}^{-1} \circ \mathcal{U}$, where $\mathcal{U}$ is the quantum operation implementing a perfect cNOT gate. Thus, the noisy CNOT gate is equivalent to applying a perfect CNOT followed by the operation $\mathcal{E} \circ \mathcal{U}^{-1}$, which is approximately the identity if our noisy CNOT is reasonably good, and can be understood in our usual error model of tensor products such as $X \otimes Z$ occurring on the two qubits with some small probability p.

Over the next few sections we explain in detail procedures for performing each class of fault-tolerant operations we have described - fault-tolerant quantum logic with a universal set of gates, fault-tolerant measurement, and fault-tolerant state preparation. The actual constructions we describe are for the Steane code, but they generalize fairly easily to the case of more general stabilizer codes. For now, however, we imagine that we have all of these procedures at our disposal. How can we put them together to perform quantum computation?

Example: fault-tolerant controlled-NOT

Let's examine a procedure for implementing a fault-tolerant controlled-NOT gate, followed by a fault-tolerant error-correction step, as illustrated in Figure 10.21. Our analysis of this circuit proceeds in 4 steps. Step 1 is the point of entry into the circuit, step 2 is after the encoded CNOT has been performed, step 3 is after the syndrome measurement, and step 4 is after the recovery operation has been applied. Our goal is to show that the probability that this circuit introduces two or more errors in the first encoded block behaves as $O(p^2)$, where p is the probability of failure of individual components in the circuit. Because a (hypothetical) perfect decoding of the first block of qubits only fails if there are two or more errors in the block, it follows that the probability that a perfectly decoded state contains errors is at most $O(p^2)$ larger after the action of this circuit than it was before.

To show that this procedure introduces two errors into the first encoded block with prob-

ability $O(p^2)$, let's identify all the possible ways this circuit can introduce two or more errors into the first encoded block of qubits at the output:
(1) There is a single pre-existing error entering the circuit at step 1 in each encoded block of qubits. This can cause two errors in the output from the first block because,

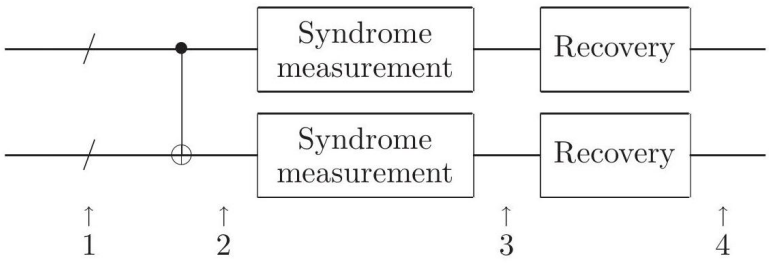


Figure 10.21. Block diagram of the fault-tolerant procedure construction, including error-correction.

for example, the error on the second block may propagate through the encoded CNOT circuit to cause an error on the first block of qubits. Provided the operations up to this stage have been done fault-tolerantly, we can argue that the probability of such an error entering on the first block is at most $c_0 p$ for some constant c_0, since such an error must have occurred during either the syndrome measurement or recovery stages in the previous stage of the quantum circuit. c_0 is the total number of places at which a failure may occur during syndrome measurement or recovery in the previous stage of the circuit. If we assume for simplicity that the probability of a single pre-existing error entering at step 1 on the second block is also $c_0 p$, and that these two errors occur independently, then the probability of this event is at most $c_0^2 p^2$. For the Steane code construction described below, there are contributions to c_0 from the six separate syndrome measurements, each of which has approximately 10^1 locations at which a failure may occur, together with a recovery operation involving seven components, for a total of approximately $c_0 \approx 70$.
(2) A single pre-existing error enters in step 1 on either the first or second block of qubits, and a single failure occurs during the fault-tolerant controlled-not. The probability of this is $c_1 p^2$, where c_1 is a constant defined to be the number of pairs of points at which a failure may occur. For the Steane code construction described below, we argued previously that there are roughly 70 locations times two blocks where a failure may have occurred causing an error to enter the circuit, for a total of 140 locations. There are a further 7 locations at which a failure may occur during the circuit, for a total of $c_1 \approx 7 \times 140 \approx 10^3$ locations at which a pair of failures may occur.
(3) Two failures occur during the fault-tolerant cNOT. This happens with probability at most $c_2 p^2$, where c_2 is the number of pairs of points at which a failure may occur. For the Steane code, $c_2 \approx 10^2$.
(4) A failure occurs during the CNOT and during the syndrome measurement. The only way two or more errors can occur at the output is if the syndrome measurement gives the incorrect result, which occurs with probability $c_3 p^2$ for some constant c_3 (for the Steane code, $c_3 \approx 10^2$). Another case which appears to be of interest, but which does not actually matter, is when the syndrome measurement gives the correct result, in which case the error introduced by the CNOT is correctly diagnosed and corrected by recovery, leaving only a single error at the output, introduced during syndrome measurement.
(5) Two or more failures occur during the syndrome measurement. This happens with probability at most $c_4 p^2$, where c_4 is the number of pairs of points at which a failure may occur. For the Steane code, $c_4 \approx 70^2 \approx 5 \times 10^3$.

(6) A failure occurs during syndrome measurement and a failure during recovery. This happens with probability at most $c_5 p^2$, where c_5 is the number of pairs of points at which a failure may occur. For the Steane code, $c_5 \approx 70 \times 7 \approx 500$.
(7) Two or more failures occur during recovery. This happens with probability at most $c_6 p^2$, where c_6 is the number of pairs of points at which a failure may occur. For the Steane code, $c_6 \approx 7^2 \approx 50$.

Thus, the probability that this circuit introduces two or more errors into the encoded first block of qubits is at most cp^2 for some constant $c = c_0^2 + c_1 + c_2 + c_3 + c_4 + c_5 + c_6$ which is approximately equal to 10^4 for the Steane code. If a perfect decoding were to be performed at the end of the circuit, the probability of an error would therefore be at most cp^2. This is a truly remarkable result: we have managed to find an implementation for the CNOT with the property that individual components may fail with probability p, but the encoded procedure succeeds with probability $1 - cp^2$, and thus, provided p is small enough, in the example, $p < 10^{-4}$, there is a net gain to be had by using the encoded procedure! Similar conclusions can be drawn for all the other operations one might wish to do during a quantum computation, so that by doing any of our operations fault-tolerantly we can reduce our probability of a failure from p to cp^2, for some constant c. We have estimated c for the CNOT, however estimates for other fault-tolerant operations do not differ all that greatly, and we will continue to use $c \approx 10^4$ in our numerical estimates.

Concatenated codes and the threshold theorem

There is a beautiful construction based on concatenated codes which can be used to reduce the effective error rate achieved by the computation even further! The idea is to recursively apply the scheme described above for simulating a circuit using an encoded circuit, constructing a hierarchy of quantum circuits C_0 (the original circuit we wish to simulate), $C_1, C_2, \ldots$. In the first stage of this construction, each qubit in the original circuit is encoded in a quantum code whose qubits are themselves encoded in a quantum code, whose own qubits are encoded yet again, and so forth ad infinitum, as illustrated in Figure 10.22. In the second stage of this construction, any given gate in the original circuit C_0, such as a Hadamard gate, is replaced in the circuit C_1 by a fault-tolerant procedure implementing an encoded Hadamard gate and error-correction. Each of the components used in the circuit C_1 is then replaced in the circuit C_2 by a fault-tolerant procedure implementing an encoded version of the component and error-correction, and so on, ad infinitum. Suppose we do two levels of concatenation, as illustrated. If the failure probability of components at the lowest level of the code - the actual physical qubits - is p, then the failure probability at the middle level (one level of encoding) is at most cp^2, and at the highest level (two levels of encoding) - the level at which the circuit must function correctly if the computation is to produce the correct output - is $c\left(cp^2\right)^2$. Thus, if we concatenate k times, the failure probability for a procedure at the highest level is $(cp)^{2^k}/c$, while the size of the simulating circuit goes as d^k times the size of the original circuit, where d is a constant representing the maximum number of operations used in a fault-tolerant procedure to do an encoded gate and error-correction.

Suppose then that we wish to simulate a circuit containing $p(n)$ gates, where n specifies the size of some problem, and $p(n)$ is a polynomial function in n. This might be, for

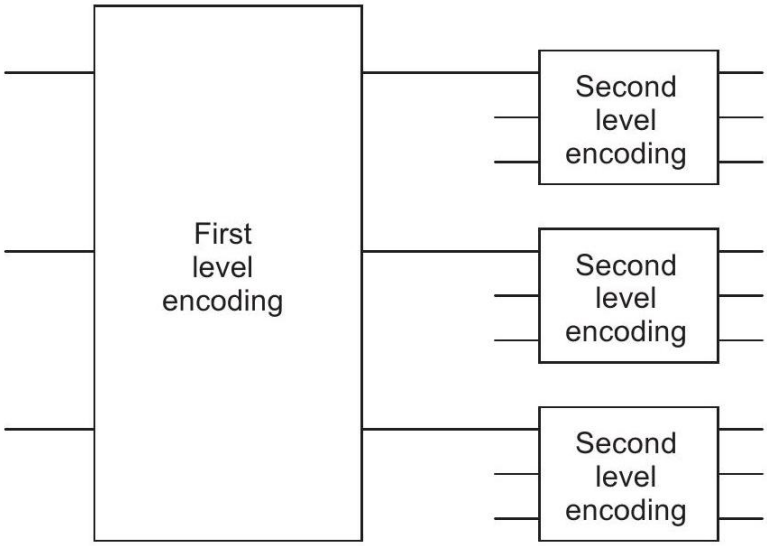


Figure 10.22. A two level concatenated code, encoding a single qubit in nine qubits. We use a three qubit code merely to keep the figure simple; in practice a code such as the Steane code which can correct arbitrary errors on one or more qubits would be used.

example, the circuit for the quantum factoring algorithm. Suppose we wish to achieve a final accuracy of ϵ in our simulation of this algorithm. To do so our simulation of each gate in the algorithm must be accurate to $\epsilon/p(n)$, so we must concatenate a number of times k such that

$$\frac{(cp)^{2^k}}{c} \leq \frac{\epsilon}{p(n)}. \tag{10.113}$$

Provided $p < p_{\rm th} \equiv 1/c$ such a k can be found. This condition - that $p < p_{\rm th}$ − is known as the threshold condition for quantum computation, since provided it is satisfied we can achieve arbitrary accuracy in our quantum computations. How large a simulating circuit is required to achieve this level of accuracy? Note that we have

$$d^k = \left(\frac{\log(p(n)/c\epsilon)}{\log(1/pc)} \right)^{\log d} = O(\mathrm{poly}(\log p(n)/\epsilon)), \tag{10.114}$$

where poly indicates a polynomial of fixed degree, and thus the simulating circuit contains

$$O(\mathrm{poly}(\log p(n)/\epsilon)p(n)) \tag{10.115}$$

gates, which is only polylogarithmically larger than the size of the original circuit. Summarizing, we have the threshold theorem for quantum computation:

Threshold theorem for quantum computation: A quantum circuit containing $p(n)$ gates may be simulated with probability of error at most ϵ using

$$O(\mathrm{poly}(\log p(n)/\epsilon)p(n)) \tag{10.116}$$

gates on hardware whose components fail with probability at most p, provided p is below some constant threshold, $p < p_{\rm th}$, and given reasonable assumptions about the noise in the underlying hardware.

What is the value of $p_{\rm th}$? For the Steane code, $c \approx 10^4$ according to our counting, so a very rough estimate gives $p_{\rm th} \approx 10^{-4}$. It needs to be emphasized that our estimates are (very) far from rigorous, however much more sophisticated calculations for the threshold have

typically yielded values in the range $10^{-5} - 10^{-6}$. Note that the precise value of the threshold depends greatly on the assumptions made about the computational capabilities! For example, if parallel operations are not possible, then the threshold condition is impossible to achieve, because errors accumulate in the circuit too quickly for errorcorrection to cope with. Classical computation is also required in addition to the quantum operations, to process the measured syndromes and determine what quantum gates to apply to correct errors. Some discussion of limitations on estimates of the threshold are given in Section 10.6.4.

Exercise 10.62: Show by explicit construction of generators for the stabilizer that concatenating an $[n_1, 1]$ stabilizer code with an $[n_2, 1]$ stabilizer code gives an $[\ n_1 n_2, 1\ ]$ stabilizer code.

9.3.24 10.6.2 Fault-tolerant quantum logic

A key technique in the construction of fault-tolerant quantum circuits is the method of constructing fault-tolerant operations to do logic on encoded states. In Section 4.5.3 of Chapter 4 we learned that the Hadamard, phase, controlled-not and $\pi/8$ gates form a universal set in terms of which any quantum computation may be expressed. We now explain how each of these gates can be implemented fault-tolerantly.

Normalizer operations

We begin with fault-tolerant constructions for the normalizer operations - the Hadamard, phase and controlled-not gates - for the specific case of the Steane code. By understanding the basic principles underlying the constructions for this concrete example it is easy to generalize them to any stabilizer code. Recall from Equation (10.107) that for the Steane code the Pauli $\bar{Z}$ and $\bar{X}$ operators on the encoded states can be written in terms of operators on the unencoded qubits, as

$$Z = Z_1 Z_2 Z_3 Z_4 Z_5 Z_6 Z_7; \quad \bar{X} = X_1 X_2 X_3 X_4 X_5 X_6 X_7. \tag{10.117}$$

An encoded Hadamard gate $\bar{H}$ should interchange $\bar{Z}$ and $\bar{X}$ under conjugation, just as the Hadamard gate interchanges Z and X under conjugation. $\bar{H} = H_1 H_2 H_3 H_4 H_5 H_6 H_7$ accomplishes this task, so that a Hadamard on the encoded qubit can be implemented as shown in Figure 10.23.

Exercise 10.63: Suppose U is any unitary operation mapping the Steane code into itself, and such that $U\bar{Z}U^\dagger = \bar{X}$ and $U\bar{X}U^\dagger = \bar{Z}$. Prove that up to a global phase the action of U on the encoded states $|0_L\rangle$ and $|1_L\rangle$ is $|0_L\rangle \rightarrow (|0_L\rangle + |1_L\rangle)/\sqrt{2}$ and $|1_L\rangle \rightarrow (|0_L\rangle - |1_L\rangle)/\sqrt{2}$.

This is a good first step, but just doing logic on the encoded state is not sufficient to make this operation fault-tolerant! We also need to understand how errors propagate. Because the circuit implementing $\bar{H} = H^{\otimes 7}$ does not involve more than one qubit in the encoded block in interaction, it seems physically reasonable to assume that the failure of a single component in the circuit can cause at most one error in the block of qubits output

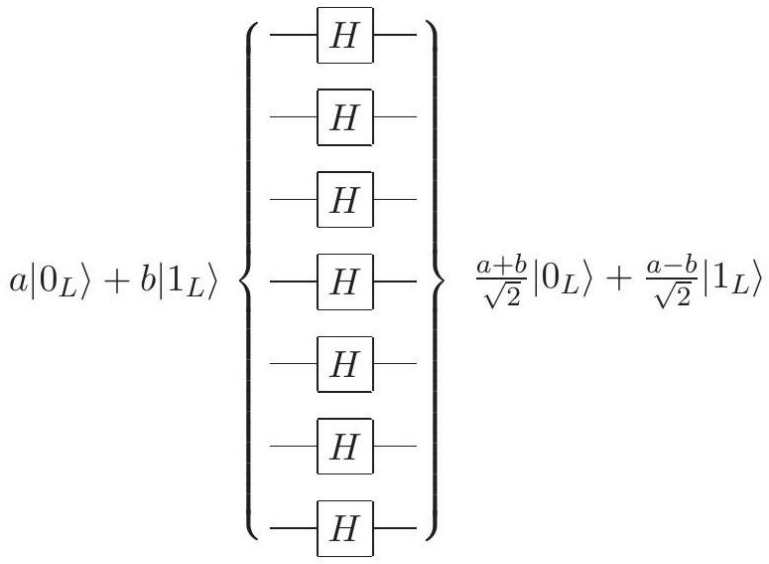


Figure 10.23. Transversal Hadamard gate on a qubit encoded in the Steane code.

from the procedure. To see that this is true, imagine an error on the first qubit occurred just before the encoded H gate was applied. For the sake of definiteness, suppose that the error is a Z error, so the combined operation on the qubit is HZ. As in our earlier analysis of error propagation for the CNOT gate, inserting the identity $H^\dagger H = I$ gives $HZ = HZH^\dagger H = XH$, so such an error is equivalent to first applying H then the error X occurring. Similarly, a failure during the gate operation itself is equivalent to a perfect gate, followed by a small amount of noise acting on the qubit, which we can think of in terms of our usual model of X, Y and Z all occurring with some small probability. The circuit in Figure 10.23 thus really is a fault-tolerant operation, because a single failure occurring anywhere in the procedure doesn't propagate to affect other qubits, and thus causes at most one error in the block of qubits output from the procedure.

Are there any general principles we can distill from the circuit in Figure 10.23? One useful observation is that encoded gates are automatically fault-tolerant if they can be implemented in a bitwise fashion, since that property ensures that a single failure anywhere in the encoded gate introduces at most one error per block of the code, and thus error probabilities do not grow out of the control of the error-correcting code. This property, that an encoded gate can be implemented in a bitwise fashion, is known as the transversality property of an encoded quantum gate. Transversality is interesting because it offers a general design principle for finding fault-tolerant quantum circuits, and we see below that many gates other than the Hadamard gate can be given transversal implementations. Keep in mind, though, that it is possible to find fault-tolerant constructions which aren't transversal, as we'll see below with the example of the fault-tolerant $\pi/8$ gate.

Using the Steane code, many gates other than the Hadamard gate are easily given transversal (and thus fault-tolerant) implementations. Three of the most interesting, in addition to the Hadamard, are the phase gate and the Pauli X and Z gates. Suppose we apply the X gates bitwise to each of the seven qubits of the Steane code. This transforms each Z operator to $-Z$ under conjugation, so $Z \rightarrow (-1)^7 Z = -Z$ and $\bar{X} \rightarrow \bar{X}$ under conjugation by the bitwise application of X, and thus this circuit effects an encoded X operation on the states of the Steane code. This circuit is transversal, and thus is automatically fault-tolerant. In a similar way, applying Z bitwise to the states of the Steane code gives a fault-tolerant implementation of an encoded Z. The transversal
implementation of the phase gate is a little more challenging. Under conjugation, $\bar{S}$ must take

$\bar{Z}$ to $\bar{Z}$ and $\bar{X}$ to $\bar{Y} = i\bar{X}\bar{Z}$. However, applying the obvious guess $\bar{S} = S_1 S_2 S_3 S_4 S_5 S_6 S_7$ takes $\bar{Z}$ to $\bar{Z}$ under conjugation, and $\bar{X}$ to $-\bar{Y}$. The minus sign in front of the $-\bar{Y}$ may be fixed up by applying $\bar{Z}$. Thus, applying the operation ZS to each qubit in the code effects an encoded phase gate, which is transversal and thus fault-tolerant.

In contrast to the Hadamard, Pauli, and phase gates, implementing the controllednot fault-tolerantly appears at first to be a challenge, because it involves two separate code blocks of seven qubits. How can we realize a CNOT which does not introduce more than one error per block of the code? Fortunately, this turns out to be very simple when using the Steane code, as illustrated in Figure 10.24: it is easily seen to be effected by seven CNOT gates applied pairwise between the seven qubits in the two blocks! You might worry that this transversal construction violates our own rules; after all, can't the controlled-NOT gates we are doing cause errors to propagate beyond a single qubit? This is correct, but there is no problem, because the error propagation only ever affects at most one qubit in another block; it does not adversely affect qubits within the same block. Remember that affecting qubits in other blocks is okay because each block can handle errors on single qubits!

More precisely, suppose that an X error on the first qubit occurs just before the controlled-not between the first qubit of each block, which we'll label qubits 1 and 8 . If this controlled-NOT gate is denoted U, then the effective action is $UX_1 = UX_1U^\dagger U = X_1X_8U$, that is, it is as though the controlled-NOT was applied correctly, but an X error occurred on the first qubit of both blocks of encoded qubits! Slightly more challenging, suppose one of the cNOT gates fails. What happens then? Suppose our noisy cNOT gate implements the quantum operation $\mathcal{E}$. Then this may be rewritten as $\mathcal{E} = \mathcal{E} \circ \mathcal{U}^{-1} \circ \mathcal{U}$, where $\mathcal{U}$ is the quantum operation implementing a perfect cNOT gate. Thus, the noisy CNOT gate is equivalent to applying a perfect CNOT followed by the operation $\mathcal{E} \circ \mathcal{U}^{-1}$, which is approximately the identity if our noisy CNOT is reasonably good, and can be understood in our usual error model of tensor products such as $X \otimes Z$ occurring on the two qubits with some small probability. Fortunately, while such errors involve two qubits, they only involve a single qubit in each block of encoded qubits. Similar conclusions about error propagation apply to errors at other locations. It follows that the failure of a single component anywhere within the procedure we have described propagates to cause no more than one error in each block of encoded qubits, and thus this implementation of the encoded controlled-NOT is fault-tolerant.

Having found fault-tolerant implementations of the Hadamard, phase and controllednot gates, it follows from Theorem 10.6 that any operation in the normalizer can be realized fault-tolerantly. Of course, normalizer operations do not exhaust the complete set of unitary gates required to do quantum computation, but this is a promising start!

Exercise 10.64: (Back propagation of errors) It is clear that an X error on the control qubit of a CNOT gate propagates to the target qubit. In addition, it turns out that a Z error on the target propagates back to the control! Show this using the stabilizer formalism, and also directly using quantum circuit identities. You may find Exercise 4.20 on page 179 useful.

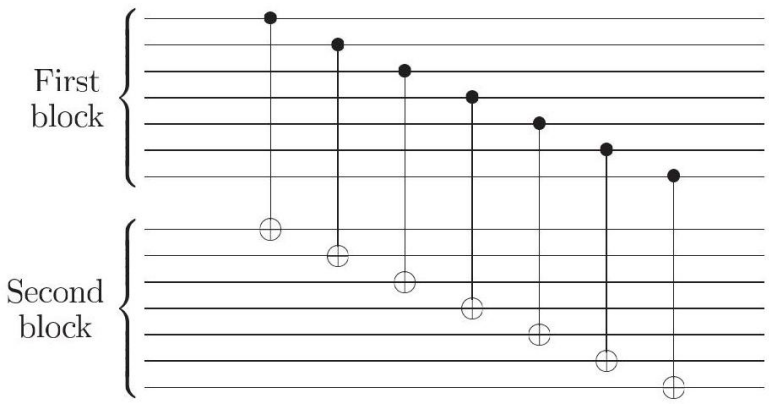


Figure 10.24. Transversal controlled-not between two qubits encoded in separate blocks with the Steane code.

Fault-tolerant $\pi/8$ gate

The one remaining gate we require to complete the standard set of gates for universal quantum computation is the $\pi/8$ gate. Alternatively, as was noted in Section 4.5.3, adding a fault-tolerant Toffoli gate to our current set of fault-tolerant Hadamard, phase and controlled-NOT gates would also give us a universal set, allowing us to perform all the gates required by a quantum computer in a fault-tolerant manner. It turns out that the fault-tolerant $\pi/8$ gate is very simple to realize, and using a similar but more elaborate construction a fault-tolerant Toffoli gate can be realized.

Our basic strategy in constructing the fault-tolerant $\pi/8$ gate is to split the construction into three parts. The first part of the construction is a simple circuit to simulate the $\pi/8$ gate using elements we already know how to do fault-tolerantly, such as the controllednot, phase and X gates. There are, however, two parts of this circuit which we don't yet know how to make fault-tolerant. The first is the preparation of an ancilla state for input into the circuit. In order that this ancilla be adequate, we require that the failure of any component during the ancilla preparation should lead to at most a single error in the block of qubits making up the ancilla. We explain how such fault-tolerant ancilla preparation can be done later in this section. The second operation we need is measurement. In order to make the measurement fault-tolerant, we require that the failure of a single component during the procedure for measurement should not affect the measurement outcome. If it did, then the error would propagate to cause errors on many qubits in the first block, since whether the encoded SX operation is performed or not is determined by the measurement result. How to do such a fault-tolerant measurement is described in the next section. (Strictly speaking, for the fault-tolerant measurement procedure we describe the measurement outcome may actually be incorrect with probability $O(p^2)$, where p is the probability of failure of a single component. We will ignore this for the purposes of the present discussion; it is easily dealt with by a slightly more sophisticated analysis along similar lines.)

Figure 10.25 shows a circuit implementing a $\pi/8$ gate. All elements in the circuit can be performed fault-tolerantly, except perhaps those in the dashed box and the measurement. The circuit starts with two encoded qubits, one of which is the qubit $|\psi\rangle = a|0\rangle + b|1\rangle$ we wish to operate on (let $|0\rangle$ and $|1\rangle$ denote logical states here). The other qubit is prepared

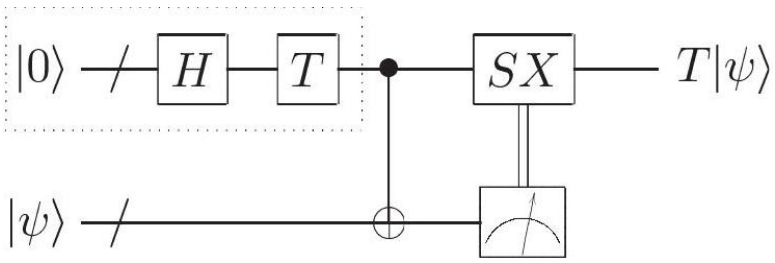


Figure 10.25. Quantum circuit which fault-tolerantly implements a $\pi/8$ gate. The dashed box represents a (non-fault-tolerant) preparation procedure for the ancilla state $(|0\rangle+\exp(i \pi / 4)|1\rangle) / \sqrt{2}$; how to do this preparation fault-tolerantly is explained in the text. The slash on the wire denotes a bundle of seven qubits, and the double-line wire represents the classical bit resulting from the measurement. Note that the final SX operation is controlled by the measurement result.}

in the state

$$|\Theta\rangle = \frac{|0\rangle + \exp(i\pi/4)|1\rangle}{\sqrt{2}}, \tag{10.118}$$

which is the state generated by the circuit in the dotted box in the figure. We explain how this ancilla preparation step may be done fault-tolerantly in a moment. Next, perform a fault-tolerant controlled-NOT operation, giving

$$\begin{aligned} &\frac{1}{\sqrt{2}}[|0\rangle(a|0\rangle + b|1\rangle) + \exp(i\pi/4)|1\rangle(a|1\rangle + b|0\rangle)] \\ &\quad = \frac{1}{\sqrt{2}}[(a|0\rangle + b\exp(i\pi/4)|1\rangle)|0\rangle + (b|0\rangle + a\exp(i\pi/4)|1\rangle)|1\rangle]. \end{aligned} \tag{10.119}$$

Finally, measure the second qubit, and if it is 0 then we are done. Otherwise, perform the operation

$$SX = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{10.120}$$

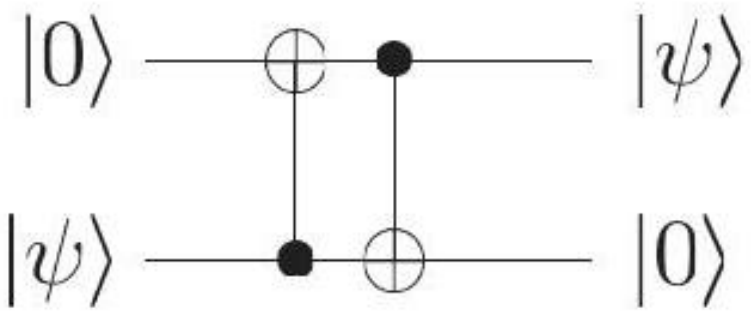
to the remaining qubit. Either way, we are left with the state $a|0\rangle + b\exp(i\pi/4)|1\rangle$ up to an irrelevant global phase, as required for a $\pi/8$ gate. This wonderful result may seem to have come out of nowhere, but in fact it is the result of a systematic construction which is explained in the exercises below. The same construction is used to realize a fault-tolerant Toffoli gate, as shown in Exercise 10.68.

The construction of the fault-tolerant $\pi/8$ gate requires a fault-tolerant method to produce the ancilla state $|\Theta\rangle$. This preparation can be achieved using the techniques for fault-tolerant measurements, as explained in detail in the next section. For now we explain the connection to fault-tolerant measurement. As shown in Figure 10.25, $|\Theta\rangle$ may be produced by applying a Hadamard gate and then a $\pi/8$ gate to the state $|0\rangle$. The state $|0\rangle$ is a $+1$ eigenstate of Z, so it follows that $|\Theta\rangle$ is a $+1$ eigenstate of $THZHT^\dagger = TXT^\dagger = e^{-i\pi/4}SX$.$|\Theta\rangle$ can therefore be prepared by first preparing an encoded $|0\rangle$, and then fault-tolerantly measuring $e^{-i\pi/4}SX$. If the result $+1$ is obtained we conclude that the state has been correctly prepared. If the result -1 is obtained, we have one of two options. We can either start over, repeating the procedure until the fault-tolerant measurement of $e^{-i\pi/4}SX$ gives the result $+1$, or we can use the more elegant and efficient observation that since $ZSXZ = -SX$, applying a fault-tolerant

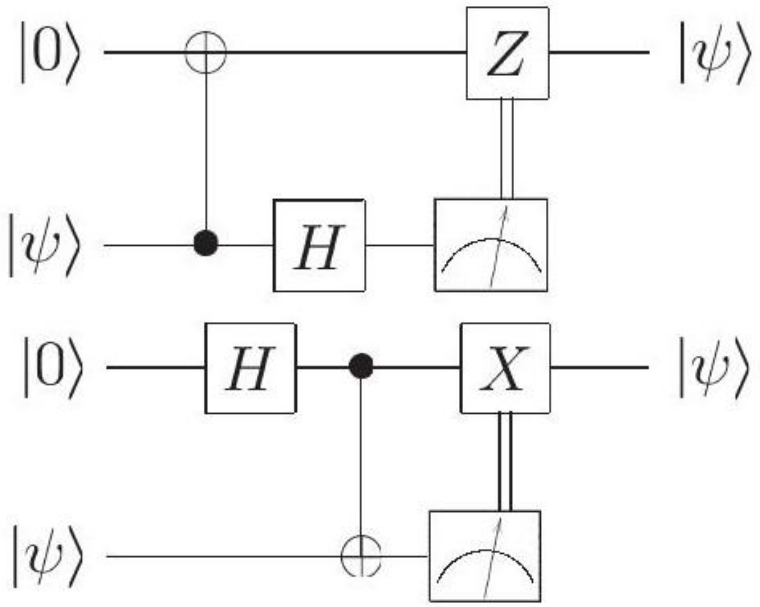
Z operation changes the state from the -1 eigenstate of $e^{-i\pi/4}SX$ to the $+1$ eigenstate of $e^{-i\pi/4}SX$, $|\Theta\rangle$. Whichever procedure is used, a single failure anywhere in the procedure produces an error in at most one qubit in the ancilla state $|\Theta\rangle$.

It is not difficult to see that the procedure we have described is fault-tolerant as a whole; however, it may be useful to look at an explicit example to see this. Suppose a single component failure occurred during ancilla construction, leading to an error on a single qubit in the ancilla. This propagates through the encoded controlled-not gate to cause one error in each of the first and second blocks of qubits. Fortunately, an error on a single qubit in the second encoded qubit doesn't affect the result of our fault-tolerant measurement procedure, so SX is applied or not applied as appropriate, and thus the error on the first block of qubits propagates through to cause a single error in the output from the encoded gate. Similarly, it is not difficult to convince yourself that a single failure anywhere else in this procedure for an encoded $\pi/8$ gate leads to an error on only a single qubit in the output block of encoded qubits.

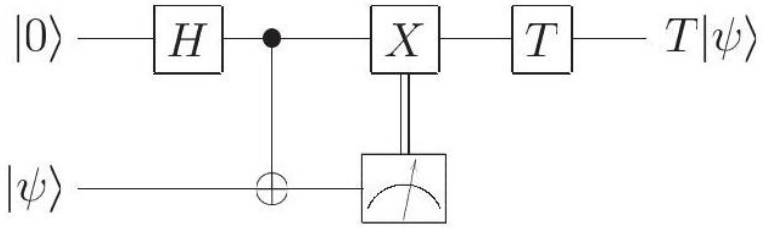
Exercise 10.65: An unknown qubit in the state $|\psi\rangle$ can be swapped with a second qubit which is prepared in the state $|0\rangle$ using only two controlled-not gates, with the circuit



Show that the two circuits below, which use only a single cNOT gate, with measurement and a classically controlled single qubit operation, also accomplish the same task:



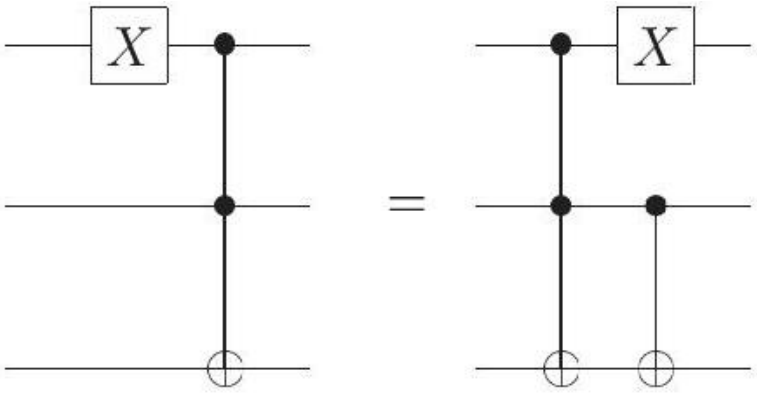
Exercise 10.66: (Fault-tolerant $\pi/8$ gate construction) One way to implement a $\pi/8$ gate is to first swap the qubit state $|\psi\rangle$ you wish to transform with some known state $|0\rangle$, then to apply a $\pi/8$ gate to the resulting qubit. Here is a quantum circuit which does that:



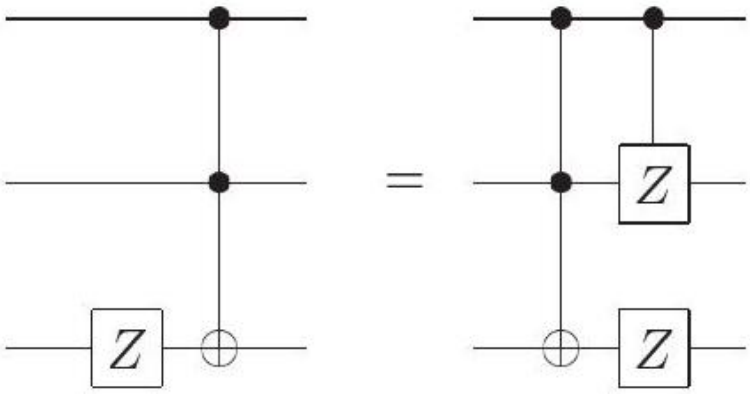
Doing this does not seem particularly useful, but actually it leads to something which is! Show that by using the relations $TX = \exp(-i\pi/4)SX$ and $TU = UT$ (U is the controlled-NOT gate, and T acts on the control qubit) we may obtain the circuit of Figure 10.25.

Exercise 10.67: Show that the following circuit identities hold:

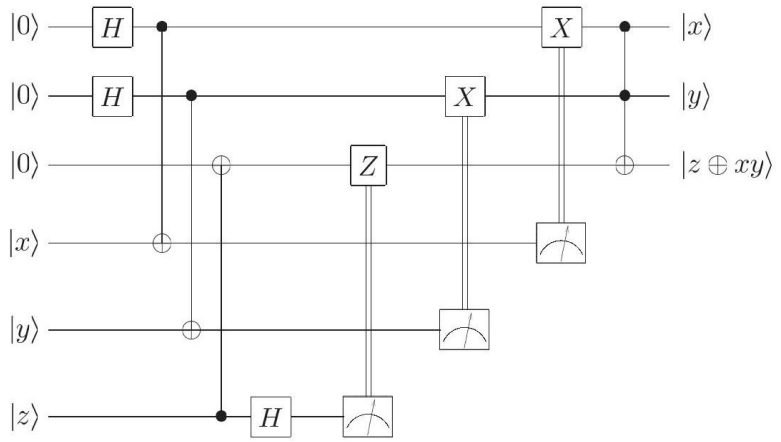
(a)



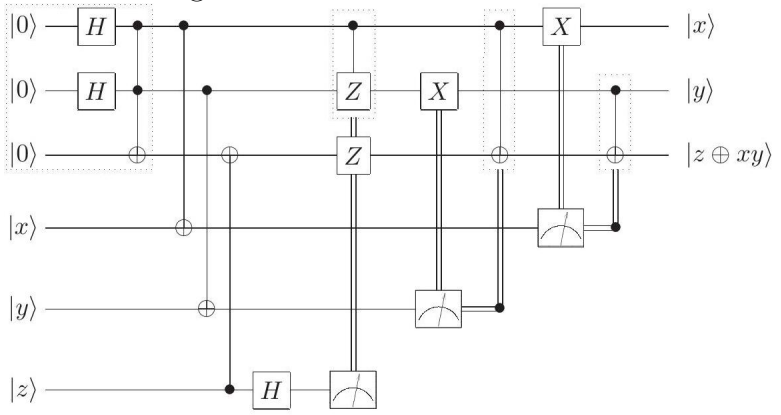
(b)



Exercise 10.68: (Fault-tolerant Toffoli gate construction) A procedure similar to the above sequence of exercises for the $\pi/8$ gate gives a fault-tolerant Toffoli gate.
(1) First, swap the three qubit state $|xyz\rangle$ you wish to transform with some known state $|000\rangle$, then apply a Toffoli gate to the resulting qubits. Show that the following circuit accomplishes this task:



(2) Using the commutation rules from Exercise 10.67, show that moving the final Toffoli gate all the way back to the left side gives the circuit



(3) Assuming the ancilla preparation shown in the leftmost dotted box can be done fault-tolerantly, show that this circuit can be used to give a fault-tolerant implementation of the Toffoli gate using the Steane code.

9.3.25 10.6.3 Fault-tolerant measurement

An extremely useful and important tool in the construction of fault-tolerant circuits is the ability to measure an operator M. Measurements are used to do encoding, read out the result of a quantum computation, to diagnose the syndrome in error-correction, and to do ancilla state preparation in the construction of the fault-tolerant $\pi/8$ and Toffoli gates, and thus are absolutely crucial to fault-tolerant quantum computation. In order that a procedure for performing an encoded measurement be considered to be fault-tolerant, we require that two things be true in order to prevent the propagation of errors. First, a single failure anywhere in the procedure should lead to at most one error in any block of qubits at the end of the procedure. Second, even if a single failure occurs during the procedure, we require that the measurement result be correct with probability $1 - O(p^2)$. This latter requirement is extremely important, since the measurement result may be used to control other operations in the quantum computer, and if it is incorrect then it may propagate to affect many qubits in other blocks of encoded qubits.

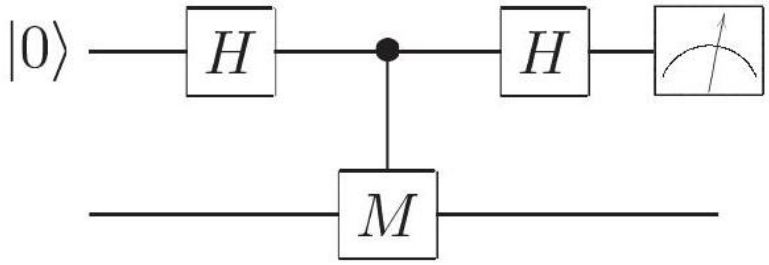


Figure 10.26. Quantum circuit for measuring a single qubit operator M with eigenvalues ± 1. The top qubit is the ancilla used for the measurement, and the bottom qubit is being measured.

Recall that measurement of a single qubit observable M may be performed using the circuit shown in Figure 10.26. Suppose M can be given a transversal encoded implementation on a quantum code as bitwise application of a gate M' to each qubit of the code. For example, for the Steane code, $M = H$ can be given a transversal implementation as bitwise application of $M' = H$, while a transversal implementation of $M = S$ uses bitwise application of $M' = ZS$. This suggests a possible circuit for measuring the encoded M on the encoded data, as shown schematically in Figure 10.27. Note that a real quantum code, such as the Steane code, would require more qubits. Unfortunately, the circuit in Figure 10.27 is not fault-tolerant. To see this, imagine a single failure occurs at the very beginning of the circuit, on the ancilla qubit. This will propagate forward to affect all the encoded qubits, so the circuit is not fault-tolerant.

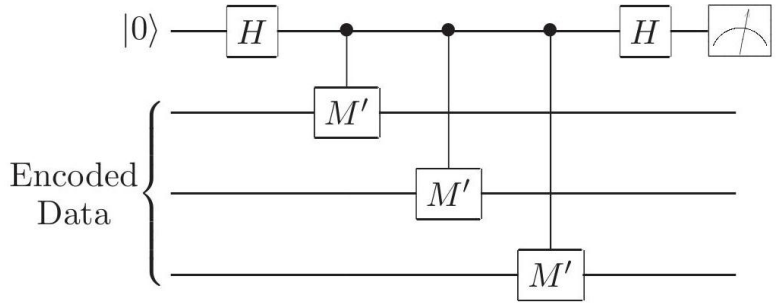


Figure 10.27. Schematic procedure for performing a measurement of an encoded observable M with a transversal implementation as bitwise application of $M^{\prime}$. The circuit is not fault-tolerant. Note that a real code would require more than three qubits.

A nice way to make the measurement circuit fault-tolerant is schematically illustrated in Figure 10.28. For simplicity, this figure shows the data to be measured encoded in only three qubits; in practice more qubits will be used, such as the seven qubit Steane code, and for concreteness we imagine that it is the Steane code which is being used here. In addition to the encoded data, the circuit introduces one ancilla qubit for each data qubit, initially each in the state $|0\rangle$. The first step is to prepare the ancilla in a 'cat' state, $|00\ldots0\rangle + |11\ldots1\rangle$. (Note that the cat state is not encoded in any code.) The circuit used to do this preparation is not itself fault-tolerant, because a single failure during the circuit can cause errors on multiple qubits in the cat state. Nevertheless, this does not affect the fault-tolerance of the entire procedure, because we follow the ancilla preparation by several verification steps (only a single verification step is shown in the Figure).

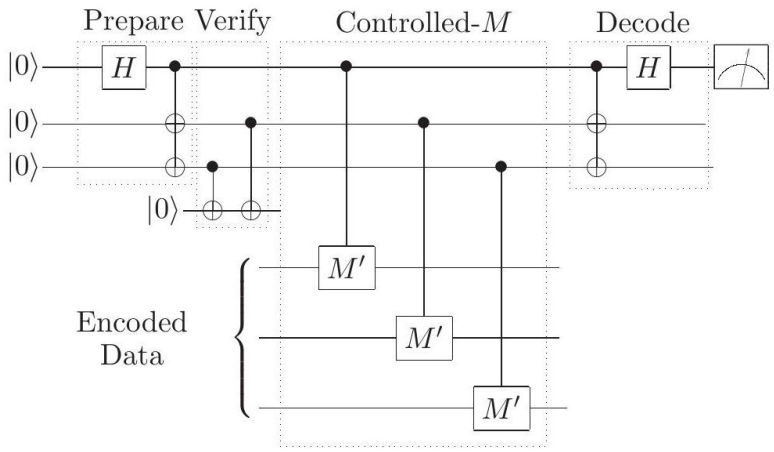


Figure 10.28. Schematic procedure for fault-tolerant measurement of an observable M, which is performed on encoded data. This procedure is repeated three times and a majority vote of the measurement outcomes taken, with the result that the measurement result is wrong with probability \$O\left(p\^{}{2
\right)\$, where p is the failure probability of any individual component, and a single error anywhere in the circuit produces at most one error in the data.}

The verification works as follows. The basic idea is that to verify that the state is a cat state it is sufficient to show that measurement of $Z_i Z_j$ for all pairs of qubits i and j in the cat state will give 1 ; that is, the parity of any pair of qubits in the cat state is even. To verify this for a particular pair $Z_i Z_j$ ($Z_2 Z_3$ in the example) we introduce an extra qubit, initially in the state $|0\rangle$. We compute the parity of two of the qubits in the ancilla by implementing two controlled-nots with the ancilla qubits as controls, and the extra qubit as the target, before measuring the extra qubit. If the measured parity is 1 then we know that the ancilla is not in the cat state, discard it, and start again. Suppose a single component failure occurs somewhere during this sequence of parity checks. This procedure is not fault-tolerant, because it is easy to show that there are single component failures which lead to more than one phase flip in the ancilla state. For example, if there is a Z error on the extra qubit between the CNOT gates then this can propagate forward to cause Z errors on two of the ancilla qubits. Fortunately, it is easy to show that multiple Z errors in the ancilla qubits do not propagate to the encoded data, although they may cause the final measurement result to be incorrect. To cope with this problem, and as described in more detail below, we repeat this procedure for measurement three times
and take a majority vote, so the probability that the measurement will be wrong two or more times in this way is at most $O(p^2)$, where p is the probability of failure for a single component. What about X or Y errors? Well, these can propagate to cause errors in the encoded data, but it is a fortunate fact that a single failure during the cat state preparation and verification can cause at most one X or Y error in the ancilla after verification, and thus at most one error in the encoded data, ensuring fault-tolerance!

Exercise 10.69: Show that a single failure anywhere in the ancilla preparation and verification can lead to at most one X or Y error in the ancilla output.

Exercise 10.70: Show that Z errors in the ancilla do not propagate to affect the encoded data, but result in an incorrect measurement result being observed.

After the cat state has been verified, controlled- M' gates are performed between pairs of ancilla and data qubits, with no ancilla qubit being used more than once. Thus, if the ancilla is in the state $|00\ldots0\rangle$ this results in nothing being done to the encoded data, while if the ancilla is in the state $|11\ldots1\rangle$ the encoded M operation is applied to the data. The value of

the cat state is that it ensures errors do not propagate from one controlled- M' gate to another, so a single error in the verification stage or the sequence of controlled $-M'$ gates results in at most a single error in the encoded data. Finally, the measurement result is obtained by decoding the cat state with a series of CNOT gates and a Hadamard; the resulting qubit is 0 or 1 depending on the eigenvalue of the state of the data. These final gates do not involve the data, and thus an error in these gates does not propagate to affect the data at all. But what if an error in this final sequence of gates results in an incorrect measurement result? By repeating the measurement procedure three times and taking a majority vote of the results, we can ensure that the probability of an error in the measurement result is $O(p^2)$, where p is the probability of failure in an individual component.

We have described a method for performing fault-tolerant measurements such that the measurement gives an erroneous result with probability $O(p^2)$, where p is the failure probability for the individual components, and a single failure anywhere in the procedure results in an error on at most one qubit in the encoded data. The construction can be applied for any single qubit observable M which can be implemented in a transversal fashion. For the Steane code, this includes the Hadamard, phase and Pauli gates, and with a slight modification, the observable $M = e^{-i\pi/4}SX$. To perform the controlled$M$ operation on the Steane code for this choice of M we apply controlled- ZSX gates transversally for each pair of qubits in the ancilla and the code, followed by seven T gates applied transversally to the ancilla qubits. As described in Section 10.6.2, a fault-tolerant measurement of this observable can be used to create the ancilla used in the fault-tolerant circuit for the $\pi/8$ gate.

Exercise 10.71: Verify that when $M = e^{-i\pi/4}SX$ the procedure we have described gives a fault-tolerant method for measuring M.

Exercise 10.72: (Fault-tolerant Toffoli ancilla state construction) Show how to fault-tolerantly prepare the state created by the circuit in the dotted box of

Exercise 10.68, that is,

$$\frac{|000\rangle + |010\rangle + |100\rangle + |111\rangle}{2}. \tag{10.121}$$

You may find it helpful to first give the stabilizer generators for this state.

Measurement of stabilizer generators

We have described the fault-tolerant measurement procedure when M is an encoded observable for a single qubit, however the techniques immediately generalize to other cases. For our purposes it is sufficient to be able to measure stabilizer generators, which take the form of a tensor product of Pauli matrices. Such measurements allow us to perform fault-tolerant error-correction, the initial encoding for the quantum computer, and to measure encoded Z operators for the final readout stage of the computation.

As a simple example, suppose we wished to measure an operator like $X_1Z_2X_3$ on the first three qubits of a block of seven qubits encoded using the Steane code. An obvious generalization of Figure 10.28 can be used to perform this measurement, as shown in Figure 10.29. Once again, we perform verified cat state preparations before applying transversal controlled operations on the encoded data, in order to achieve a fault-tolerant measurement procedure for the operator $X_1Z_2X_3$. With the ability to fault-tolerantly measure such observables we automatically obtain the ability to perform the steps of encoding, syndrome measurement and measurement in the (logical) computational basis that are required to perform quantum computation. For the purposes of encoding, it suffices for quantum computation to prepare an encoded $|0\rangle$ state. For a stabilizer code such as the Steane code, such a preparation can be achieved by fault-tolerantly measuring all the stabilizer generators and the encoded $\bar{Z}$ operator, and then fixing the signs of the stabilizer generators and the encoded Z by applying appropriate fault-tolerant operations,

according to the prescription in the proof of Proposition 10.4 in Section 10.5.1. An example illustrating how the Steane code encoded $|0\rangle$ state may be prepared faulttolerantly is explained in Exercise 10.73. Syndrome measurement for error-correction and final read-out in the encoded computational basis of the quantum computer are realized fault-tolerantly along similar lines.

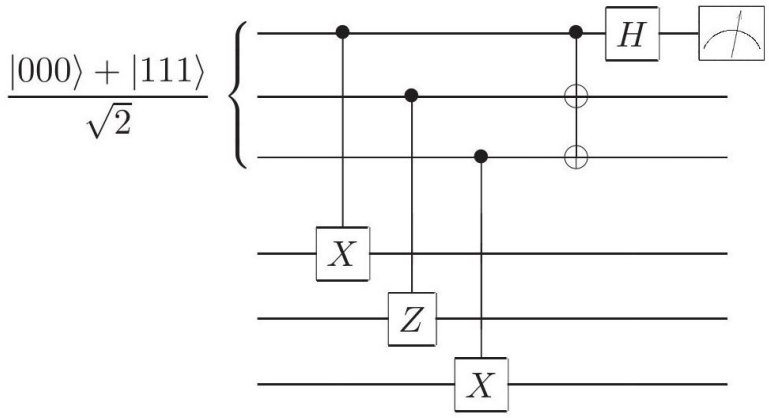


Figure 10.29. Schematic procedure for performing a fault-tolerant measurement of the operator XZX on three qubits.

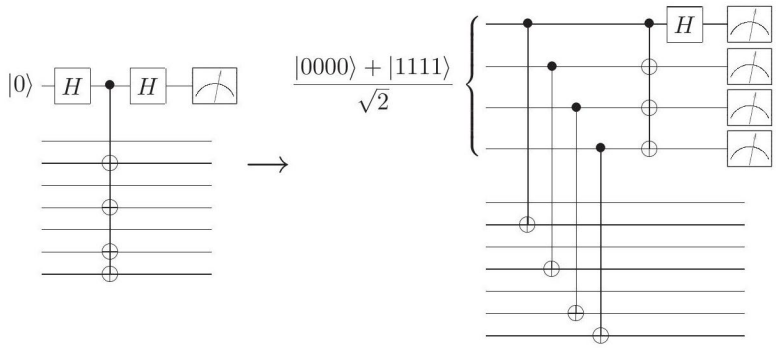


Figure 10.30. One step in fault-tolerantly producing the Steane code encoded $|0\rangle$ state.

Exercise 10.73: (Fault-tolerant encoded state construction) Show that the Steane code encoded $|0\rangle$ state can be constructed fault-tolerantly in the following manner.
(1) Begin with the circuit of Figure 10.16, and replace the measurement of each generator, as shown in Figure 10.30, with each ancilla qubit becoming a cat state $|00\ldots0\rangle + |11\ldots1\rangle$, and the operations rearranged to have their controls on different qubits, so that errors do not propagate within the code block.
(2) Add a stage to fault-tolerantly measure Z.
(3) Calculate the error probability of this circuit, and of the circuit when the generator measurements are repeated three times and majority voting is done.
(4) Enumerate the operations which should be performed conditioned on the measurement results and show that they can be done fault-tolerantly.

Exercise 10.74: Construct a quantum circuit to fault-tolerantly generate the encoded $|0\rangle$ state for the five qubit code (Section 10.5.6).

9.3.26 10.6.4 Elements of resilient quantum computation

The most spectacular success of quantum error-correcting codes - the threshold for quantum computation - is that provided the noise in individual quantum gates is below a certain constant threshold it is possible to efficiently perform an arbitrarily large quantum computation. Stated another way, noise is not a serious problem in principle for quantum computation. The basic idea in the proof of the threshold, as was outlined in Section 10.6.1, is to perform fault-tolerant operations directly on encoded states, interleaved with error-correction steps, resulting in a net reduction in error probability from p to $O(p^2)$. By concatenating our codes multiple times and creating hierarchical fault-tolerant procedures, the error probability can be reduced further to $O(p^4)$, then $O(p^8)$ and so on, ultimately being reduced to as low a level as desired, so long as the the original error p is less than some threshold value p_{th} . Using the procedures we have described, we estimate a threshold of approximately $p_{\text{th}} \sim 10^{-5} - 10^{-6}$.

A bold claim such as the threshold theorem obviously needs qualifiers. It is not the case that it is possible to protect a quantum computation against the effect of completely arbitrary noise. The threshold theorem relies for its functioning on a small number of physically reasonable assumptions about the type of noise occurring in the quantum computer, and the quantum computer architecture available in order to reach its powerful conclusion. The error model we have considered is rather simplistic, and it is certainly the case that real quantum computers will experience more varied types of noise than we have considered here. Nevertheless, it seems plausible that the techniques introduced here when coupled with more sophisticated quantum error-correcting codes and with more sophisticated tools for analysis, can result in a threshold for quantum computation applicable in a much wider variety of circumstances than those we have considered.

We have not the space here to dive into a more sophisticated analysis, but several observations are in order. First, it is interesting to note that the threshold result requires a high degree of parallelism in our circuits. Even if all we wish to do is store quantum information in a quantum memory this operation will require periodic error-correction that demands a high degree of parallelism. Thus, a desirable goal for would-be designers of quantum computers is to develop architectures which are parallelizable, in order that the techniques of fault-tolerant quantum computation may be applied. Second, we note that our presentation of the threshold has completely neglected the cost of the classical computations and communication that are done during state preparation, syndrome measurement, and recovery. The cost of these could potentially be quite high; for example, to do recovery at the highest levels of the concatenated code requires communication between all parts of the quantum system. If this communication cannot be accomplished much faster than the time scale over which errors occur in the system then errors will begin to creep back in, negating the effect of the error-correction. More sophisticated analyses can deal with this problem; however, as with other complications there is a concomitant cost in the form of a more stringent threshold for quantum computation. Third, our fault-tolerant constructions for measurement and the $\pi/8$ gate made use of ancilla qubits in the state $|0\rangle$, perhaps with some slight additional noise. It can be shown that in fact a constant supply of such fresh ancilla qubits is necessary for the threshold theorem to apply, and thus quantum computer designers must provide architectures which are not only parallelizable, but which also allow fresh ancilla qubits to be brought up on a regular basis.

Our presentation has focused on basic principles, not on optimizing the methods used, and it is likely that in practice much more streamlined versions of our constructions would be used. A simple but important guiding principle is to choose your codes well. We have focused on the Steane code because it is easy to work with and demonstrates all the fundamental principles; however, in practice other codes may work much better. For example, it may pay handsome dividends at the first level of concatenation to use a code optimized to protect against the type of noise known to occur in the particular physical system being used for implementation.

Although the theoretical ideas behind the threshold theorem can be adapted in a variety of different ways, depending upon the noise prevalent in a specific implementation of quantum computation, a skeptic might still claim that all such noise models for which a threshold may be proved are overly restrictive, and will not be realized within any real physical system. Such skepticism is, finally, only answerable in the laboratory with a demonstration of large-scale fault-tolerant quantum computation. The marvel of the present result is that it proves that, to the best of our current knowledge, no principle of physics will limit quantum computers from being realized someday.

Summarizing, in this chapter we have outlined the basic principles by which quantum information processing may be performed in a resilient manner, focusing on the specific example of quantum computation. The same basic techniques apply also to any other system in which quantum information processing may be performed, such as quantum communications channels for performing tasks such as quantum cryptography. The extreme fragility of quantum information in all known systems makes it likely that some form of quantum error-correction will need to be used in any practical quantum information processing system, but surprisingly, these techniques work so well that arbitrarily reliable quantum computations can be performed using noisy components, provided the error probability in those components is less than some constant threshold.

Problem 10.1: Channels $\mathcal{E}_1$ and $\mathcal{E}_2$ are said to be equivalent if there exist unitary channels $\mathcal{U}$ and $\mathcal{V}$ such that $\mathcal{E}_2 = \mathcal{U} \circ \mathcal{E}_1 \circ \mathcal{V}$.
(1) Show that the relation of channel equivalence is an equivalence relation.
(2) Show how to turn an error-correcting code for $\mathcal{E}_1$ into an error-correcting code for $\mathcal{E}_2$. Assume that the error-correction procedure for $\mathcal{E}_1$ is performed as a projective measurement followed by a conditional unitary operation, and explain how the error-correction procedure for $\mathcal{E}_2$ can be performed in the same fashion.

Problem 10.2: (Gilbert-Varshamov bound) Prove the Gilbert-Varshamov bound for CSS codes, namely, that an $[n, k]$ CSS code correcting t errors exists for some k such that

$$\frac{k}{n} \geq 1 - 2H\left(\frac{2t}{n}\right). \tag{10.122}$$

As a challenge, you may like to try proving the Gilbert-Varshamov bound for a general stabilizer code, namely, that there exists an $[n, k]$ stabilizer code correcting errors on t qubits, with

$$\frac{k}{n} \geq 1 - \frac{2\log(3)t}{n} - H\left(\frac{2t}{n}\right). \tag{10.123}$$

Problem 10.3: (Encoding stabilizer codes) Suppose we assume that the generators for the code are in standard form, and that the encoded Z and X operators have been constructed in standard form. Find a circuit taking the $n \times 2n$ check matrix corresponding to a listing of all the generators for the code together with the encoded Z operations from

$$G = \left[\begin{array}{ccc|ccc} 0 & 0 & 0 & I & 0 & 0 \\ 0 & 0 & 0 & 0 & I & 0 \\ 0 & 0 & 0 & 0 & 0 & I \end{array}\right] \tag{10.124}$$

to the standard form

$$\left[\begin{array}{ccc|ccc} I & A_1 & A_2 & B & 0 & C_2 \\ 0 & 0 & 0 & D & I & E \\ 0 & 0 & 0 & A_2^T & 0 & I \end{array}\right]. \tag{10.125}$$

Problem 10.4: (Encoding by teleportation) Suppose you are given a qubit $|\psi\rangle$ to encode in a stabilizer code, but you are not told anything about how $|\psi\rangle$ was constructed: it is an unknown state. Construct a circuit to perform the encoding in the following manner:
(1) Explain how to fault-tolerantly construct the partially encoded state

$$\frac{|0\rangle |0_L\rangle + |1\rangle |1_L\rangle}{\sqrt{2}}, \tag{10.126}$$

by writing this as a stabilizer state, so it can be prepared by measuring stabilizer generators.
(2) Show how to fault-tolerantly perform a Bell basis measurement with $|\psi\rangle$ and the unencoded qubit from this state.
(3) Give the Pauli operations which you need to fix up the remaining encoded qubit after this measurement, so that it becomes $|\psi\rangle$, as in the usual quantum teleportation scheme.
Compute the probability of error of this circuit. Also show how to modify the circuit to perform fault-tolerant decoding.

Problem 10.5: Suppose $C(S)$ is an $[n, 1]$ stabilizer code capable of correcting errors on a single qubit. Explain how a fault-tolerant implementation of the controlled-not gate may be implemented between two logical qubits encoded using this code, using only fault-tolerant stabilizer state preparation, fault-tolerant measurement of elements of the stabilizer, and normalizer gates applied transversally.

9.3.27 Summary of Chapter 10: Quantum error-correction

- Quantum error-correcting code: An $[n, k, d]$ quantum error-correcting code uses n qubits to encode k qubits, with distance d.

- Quantum error-correction conditions: Let C be a quantum error-correcting code and P be the projector onto C. Then the code can correct the error set $\{E_i\}$ if and only if

$$PE_i^\dagger E_j P = \alpha_{ij} P, \tag{10.127}$$

for some Hermitian matrix α of complex numbers.

- Stabilizer codes: Let S be the stabilizer for a stabilizer code $C(S)$ and suppose $\{E_j\}$ is a set of errors in the Pauli group such that $E_j^\dagger E_k \notin N(S) - S$ for all j and k. Then $\{E_j\}$ is a correctable set of errors for the code $C(S)$.

- Fault-tolerant quantum computation: A universal set of logical operations on encoded quantum states can be performed in such a way that the effective failure probability in the encoded states scales like $O(p^2)$, where p is the failure probability in the underlying gates.

- The threshold theorem: Provided the noise in individual quantum gates is below a certain constant threshold and obeys certain physically reasonable assumptions, it is possible to reliably perform an arbitrarily long quantum computation, with only a small overhead in the size of the circuit necessary to ensure reliability.

History and further reading

There are many excellent texts on error-correcting codes in classical information theory. We especially recommend the wonderful text of MacWilliams and Sloane[MS77]. This begins at a very elementary level, but quickly and smoothly moves into more advanced topics, covering

an enormous range of material. A more recent introduction, also very good, is the text by Welsh[Wel88].

Quantum error-correction was independently discovered by Shor [Sho95] , who found the nine qubit code presented in Section 10.2, and by Steane [Ste96a], who used a different approach, in which he studied the interference properties of multiple particle entangled states. The quantum error-correction conditions were proved independently by Bennett, DiVincenzo, Smolin and Wootters [BDSW96], and by Knill and Laflamme[KL97], building upon earlier work by Ekert and Macchiavello [EM96]. The five qubit code was discovered by Bennett, DiVincenzo, Smolin and Wootters[BDSW96], and independently by Laflamme, Miquel, Paz and Zurek [LMPZ96].

Calderbank and Shor [CS96], and Steane [Ste96b] used ideas from classical error-correction to develop the CSS (Calderbank-Shor-Steane) codes. Calderbank and Shor also stated and proved the Gilbert-Varshamov bound for CSS codes. Gottesman [Got96] invented the stabilizer formalism, and used it to define stabilizer codes, and investigated some of the properties of some specific codes. Independently, Calderbank, Rains, Shor and Sloane [CRSS97] invented an essentially equivalent approach to quantum error-correction
based on ideas from classical coding theory. They were able to classify almost all known quantum codes using a $GF(4)$ orthogonal geometry approach [CRSS98] , and also provided the first proof of the quantum Gilbert-Varshamov bound for general stabilizer codes, which had earlier been stated by Ekert and Macchiavello[EM96]. The Gottesman-Knill theorem seems to have first been stated by Gottesman in [Got97], where he attributes the result to Knill, with the proof based upon the stabilizer formalism Gottesman had introduced. Gottesman has applied the stabilizer formalism to a wide variety of problems with considerable success; see for example [Got97] for a sample and further references. Our presentation of the stabilizer formalism is based primarily upon [Got97], wherein may be found most of the results we describe, including the result that the Hadamard, phase and controlled-not generate the normalizer $N(G_n)$.

Many constructions for specific classes of quantum codes are known; we point to just a few here. Rains, Hardin, Shor and Sloane [RHSS97] have constructed interesting examples of quantum codes lying outside the stabilizer codes we have considered. Many people have considered quantum codes based on systems other than qubits; we mention especially the work of Gottesman [Got98a] and Rains [Rai99b] which construct non-binary codes and consider fault-tolerant computation with such codes. Aharonov and Ben-Or [ABO99] construct non-binary codes using interesting techniques based on polynomials over finite fields, and also investigate fault-tolerant computation with such codes. Approximate quantum error-correction is another topic we have not touched; that approximate quantum error-correction can lead to improved codes was shown by Leung, Nielsen, Chuang and Yamamoto [LNCY97].

A large and interesting class of quantum error-correcting codes (but beyond the scope of this chapter) are known variously by the names noiseless quantum codes and decoherence free subspaces. A substantial body of work exists on these subjects (and clarifying the connections between them). An entry into the literature may be found through the work of Zanardi and Rasetti[ZR98, Zan99], Lidar, Chuang, and Whaley[LCW98], Bacon, Kempe, Lidar and Whaley [BKLW99, LBW99], and of Knill, Laflamme and Viola[KLV99].

Many bounds on quantum error-correcting codes are known, often adapted from similar classical bounds. Ekert and Macchiavello [EM96] pointed out the possibility of proving a quantum analogue to the Hamming bound; this construction and the role of 'degenerate' quantum codes was subsequently clarified by Gottesman [Got96] . Shor and Laflamme [SL97] proved a quantum analogue of a result in classical coding theory, the MacWilliams identities, which touched off a great deal of work studying the properties of certain polynomials related to quantum codes (the weight enumerators) as well as more general work on the problem of bounds for quantum codes, by Ashikhmin [Ash97] , Ashikhmin and Lytsin [AL99] , and several papers on the topic by Rains[Rai98, Rai99c, Rai99a].

The theory of fault-tolerant computation for classical computers was worked out by von Neumann [von56], and is discussed in the monograph by Winograd and Cowan [WC67]. Shor [*Sho*96] introduced the idea of fault-tolerance into quantum computation, and showed how to perform all the basic fault tolerant steps (state preparation, quantum logic, errorcorrection, and measurement). Kitaev[Kit97b, Kit97c] independently developed many similar ideas, including fault-tolerant constructions for many basic quantum logic gates. Cirac, Pellizzari and Zoller [CPZ96], and Zurek and Laflamme [ZL96], also took early steps toward fault-tolerant quantum computation. DiVincenzo and Shor generalized Shor's original construction to show how fault-tolerant measurement of syndromes for any stabilizer code could be performed [DS96], and Gottesman [Got98b] generalized all the fault-tolerant
constructions, showing how to perform fault-tolerant computation with any stabilizer code. A general review of this work as well as much other survey material may be found in [Got97]; this includes a construction to solve Problem 10.5. The fault-tolerant $\pi/8$ and Toffoli gate constructions are based on a line of thought developed by Gottesman and Chuang [*GC*99], and Zhou and Chuang [*ZLC*00]; the circuit for the fault-tolerant Toffoli described in Exercise 10.68 is actually Shor's original construction [Sho96]. Steane [Ste99] has developed many ingenious constructions for fault-tolerant procedures.

Kitaev[Kit97a, Kit97b] has introduced a beautiful set of ideas for implementing faulttolerance, using topological methods to assist in the performance of quantum errorcorrection. The basic idea is that if information is stored in the topology of a system, then that information will naturally be very robust against the effects of noise. These and many other elegant ideas have been developed in further papers by Bravyi and Kitaev [BK98 b] and by Freedman and Meyer [FM98]. Preskill [Pre97] is an excellent review of the field of quantum error-correction as a whole, and contains an especially beautiful description of topological quantum error-correction, as well as a provocative discussion of whether topological error-correction can be used to gain insight into fundamental questions about black holes and quantum gravity!

Many different groups proved threshold results for quantum computation. These results hold for a wide variety of assumptions, giving essentially different threshold theorems. Aharonov and Ben-Or [ABO97, *ABO*99] and Kitaev's [Kit97c, Kit97b] threshold proofs do not require fast or reliable classical computation. Aharonov and Ben-Or also showed that in order for a threshold result to hold, there must be constant parallelism in the quantum computer at each timestep [ABO97]. In their threshold proofs, Gottesman [Got97] and Preskill [Pre98c, GP10] have an especially detailed optimization of the value of the threshold. Knill, Laflamme and Zurek [KLZ98a, KLZ98b]'s results concentrate on proving the threshold theorem for a wide class of error models. Aharonov, Ben-Or, Impagliazzo, and Nisan have also shown that a supply of fresh qubits is necessary for the threshold [*ABOIN*96]. Further references and historical material may be found within the cited works. In particular, each group built on Shor's pioneering work [Sh96] on fault-tolerant quantum computation.

Numerous excellent reviews of fault-tolerant quantum computation have been written, developing the basic ideas in much greater detail than we have here, from a variety of different points of view. Aharonov's thesis [Aha99a] develops the threshold theorem and much material of related interest in a self-contained way. Gottesman's thesis [Got 97] also provides a review of fault-tolerant quantum computation, with more emphasis on properties of quantum codes, and developing fault-tolerant constructions for a wide variety of different codes. Knill, Laflamme and Zurek have written a semi-popular overview of the threshold result [*KLZ*98]. Finally, Preskill has written two superb articles [Pre98c, Pre98a] explaining quantum error-correction and fault-tolerant quantum computation.

9.4 11 Entropy and information

Entropy is a key concept of quantum information theory. It measures how much uncertainty there is in the state of a physical system. In this chapter we review the basic definitions and properties of entropy in both classical and quantum information theory. In places the chapter contains rather detailed and lengthy mathematical arguments. On a first reading these sections may be read lightly and returned to later for reference purposes.

9.4.1 11.1 Shannon entropy

The key concept of classical information theory is the Shannon entropy. Suppose we learn the value of a random variable X. The Shannon entropy of X quantifies how much information we gain, on average, when we learn the value of X. An alternative view is that the entropy of X measures the amount of uncertainty about X before we learn its value. These two views are complementary; we can view the entropy either as a measure of our uncertainty before we learn the value of X, or as a measure of how much information we have gained after we learn the value of X.

Intuitively, the information content of a random variable should not depend on the labels attached to the different values that may be taken by the random variable. For example, we expect that a random variable taking the values 'heads' and 'tails' with respective probabilities $1/4$ and $3/4$ contains the same amount of information as a random variable that takes the values 0 and 1 with respective probabilities $1/4$ and $3/4$. For this reason, the entropy of a random variable is defined to be a function of the probabilities of the different possible values the random variable takes, and is not influenced by the labels used for those values. We often write the entropy as a function of a probability distribution, $p_1, \ldots, p_n$. The Shannon entropy associated with this probability distribution is defined by

$$H(X) \equiv H(p_1, \ldots, p_n) \equiv -\sum_x p_x \log p_x. \tag{11.1}$$

We justify this definition shortly. Note that in the definition - and throughout this book logarithms indicated by 'log' are taken to base two, while 'ln' indicates a natural logarithm. It is conventional to say that entropies are measured in 'bits' with this convention for the logarithm. You may wonder what happens when $p_x = 0$, since $\log 0$ is undefined. Intuitively, an event which can never occur should not contribute to the entropy, so by convention we agree that $0 \log 0 \equiv 0$. More formally, note that $\lim_{x \to 0} x \log x = 0$, which provides further support for our convention.

Why is the entropy defined in this way? Later in this section, Exercise 11.2 gives an intuitive justification for this definition of the entropy, based on certain 'reasonable' axioms which might be expected of a measure of information. This intuitive justification
is reassuring but it is not the whole story. The best reason for this definition of entropy is that it can be used to quantify the resources needed to store information. More concretely, suppose there is some source (perhaps a radio antenna) which is producing information of some sort, say in the form of a bit string. Let's consider a very simple model for a source: we model it as producing a string $X_1, X_2, \ldots$ of independent, identically distributed random variables. Most real information sources don't behave quite this way, but it's often a good approximation to reality. Shannon asked what minimal physical resources are required to store the information being produced by the source, in such a way that at a later time the information can be reconstructed? The answer to this question turns out to be the entropy, that is, $H(X)$ bits are required per source symbol, where $H(X) \equiv H(X_1) = H(X_2) = \ldots$ is the entropy of each random variable modeling the source. This result is known as Shannon's noiseless coding theorem, and we prove both classical and quantum versions of it in Chapter 12.

For a concrete example of Shannon's noiseless channel coding theorem, suppose an information source produces one of four symbols, $1, 2, 3$ or 4 . Without compression two bits of storage space corresponding to the four possible outputs are consumed for each use of the source. Suppose however that the symbol 1 is produced by the source with probability $1/2$, the symbol 2 with probability $1/4$, and the symbols 3 and 4 both with probability $1/8$. We can make use of the bias between the source outputs to compress the source, using fewer bits to store commonly occurring symbols such as 1 , and more bits to store rarely occurring symbols like 3 and 4 . One possible compression scheme is to encode 1 as the bit string 0,2 as the bit string 10,3 as the bit string 110 , and 4 as the bit string 111 . Notice that the average length of the compressed string is $\frac{1}{2} \cdot 1 + \frac{1}{4} \cdot 2 + \frac{1}{8} \cdot 3 + \frac{1}{8} \cdot 3 = 7/4$ bits of information per use of the source. This is less than is required in the naive approach to storing this source! Amazingly, this matches the entropy of the source, $H(X) = -1/2 \log(1/2) - 1/4 \log(1/4) - 1/8 \log(1/8) - 1/8 \log(1/8) = 7/4$! Moreover, it turns out that any attempt to compress the source further results in data being irretrievably lost; the entropy quantifies the optimal compression that may be achieved.

This operational motivation for the definition of entropy in terms of data compression expresses a key philosophy of information theory, both quantum and classical: fundamental measures of information arise as the answers to fundamental questions about the physical resources required to solve some information processing problem.

Exercise 11.1: (Simple calculations of entropy) What is the entropy associated with the toss of a fair coin? With the roll of a fair die? How would the entropy behave if the coin or die were unfair?

Exercise 11.2: (Intuitive justification for the definition of entropy) Suppose we are trying to quantify how much information is provided by an event E which may occur in a probabilistic experiment. We do this using an 'information function' $I(E)$ whose value is determined by the event E. Suppose we make the following assumptions about this function:
(1) $I(E)$ is a function only of the probability of the event E, so we may write $I = I(p)$, where p is a probability in the range 0 to 1.
(2) I is a smooth function of probability.
(3) $I(pq) = I(p) + I(q)$ when $p, q > 0$. (Interpretation: The information gained when two independent events occur with individual probabilities p and q is the sum of the information gained from each event alone.)
Show that $I(p) = k \log p$, for some constant, k. It follows that the average information gain when one of a mutually exclusive set of events with probabilities $p_1, \ldots, p_n$ occurs is $k \sum_i p_i \log p_i$, which is just the Shannon entropy, up to a constant factor.

9.4.2 11.2 Basic properties of entropy

9.4.3 11.2.1 The binary entropy

The entropy of a two-outcome random variable is so useful that we give it a special name, the binary entropy, defined as

$$H_{\text{bin}}(p) \equiv -p \log p - (1-p) \log(1-p) \tag{11.8}$$

where p and $1-p$ are the probabilities of the two outcomes. Where context makes the meaning clear we write $H(p)$ rather than $H_{\text{bin}}(p)$. The binary entropy function is plotted in Figure 11.1. Notice that $H(p) = H(1-p)$ and that $H(p)$ attains its maximum value of 1 at $p = 1/2$.

The binary entropy is an excellent testing ground for the understanding of more general properties of entropy. One property of particular interest is how the entropy behaves when we mix two or more probability distributions. Imagine, for example, that Alice has in her

possession two coins, one a quarter from the US, the other a dollar coin from Australia. Both coins have been altered to exhibit bias, with the probability of heads on the US coin being $p_{\rm U}$, and the probability of heads on the Australian coin being $p_{\rm A}$. Suppose Alice flips the US coin with probability q and the Australian coin with probability $1-q$, telling Bob whether the result was heads or tails. How much information does Bob gain on average? Intuitively it is clear that Bob should gain at least as much information as the average of the information he would have gained from a US coin flip or an Australian coin flip. As an equation this intuition may be expressed as:

$$H\left(qp_{\rm U} + (1-q)p_{\rm A}\right) \geq qH\left(p_{\rm U}\right) + (1-q)H\left(p_{\rm A}\right). \tag{11.9}$$

Sometimes the inequality can be strict, because Bob gains information not only about the value (heads or tails) of the coin, but also some additional information about the identity of the coin. For instance, if $p_{\rm U} = 1/3$ and $p_{\rm A} = 5/6$, and heads comes up, then Bob has received a pretty good indicator that the coin was Australian.

Equation (11.9) is easily shown to be correct. It is an example of a broader concept, that of concavity, which we met in Chapter 9 when discussing distance measures. Recall that a real-valued function f is said to be concave if for any p in the range 0 to 1 ,

$$f(px + (1-p)y) \geq pf(x) + (1-p)f(y). \tag{11.10}$$

The binary entropy is easily seen to be concave, as can be grasped visually by examining Figure 11.1 and observing that the graph of the binary entropy goes above any line cutting the graph. We will be much concerned with concavity properties of the entropy, both classical and quantum. Don't let the simplicity of the above intuitive argument beguile you into a false complacency: many of the deepest results in quantum information have their roots in skilful application of concavity properties of classical or quantum entropies.

Box 11.1: Entropic quantum uncertainty principle

There is an elegant entropic way of reformulating the uncertainty principle of quantum mechanics. Recall the Heisenberg uncertainty principle from Box 2.4 on page 89 . This states that the standard deviations $\Delta(C)$ and $\Delta(D)$ for observables C and D must satisfy the relation

$$\Delta(C)\Delta(D) \geq \frac{|\langle\psi|[C,D]|\psi\rangle\ |}{2} \tag{11.2}$$

for a quantum system in the state $|\psi\rangle$.

Let $C = \sum_c c|c\rangle\langle c|$ and $D = \sum_d d|d\rangle\langle d|$ be spectral decompositions for C and D. Define $f(C,D) \equiv \max_{c,d} |\langle c \mid d\rangle|$ to be the maximum fidelity between any two eigenvectors of $|c\rangle$ and $|d\rangle$. For example, $f(X,Z) = 1/\sqrt{2}$ for the Pauli matrices X and Z.

Suppose the quantum system is prepared in a state $|\psi\rangle$, and let $p(c)$ be the probability distribution associated with a measurement of C, with associated entropy $H(C)$, and $q(d)$ the probability distribution associated with a measurement of D, with associated entropy $H(D)$. The entropic uncertainty principle states that

$$H(C) + H(D) \geq 2\log\left(\frac{1}{f(C,D)}\right) \tag{11.3}$$

A full proof of this result would take us too far afield (see 'History and further reading' for references); however, we can give a simple proof of the weaker result:

$$H(C) + H(D) \geq -2\log\frac{1+f(C,D)}{2} \tag{11.4}$$

To prove this, note that

$$H(C) + H(D) = -\sum_{cd} p(c)q(d)\log(p(c)q(d)) \tag{11.5}$$

We aim to bound $p(c)q(d) = |\langle c \mid \psi\rangle\langle\psi \mid d\rangle|^2$ from above. To do this, let $|\tilde{\psi}\rangle$ be the projection of $|\psi\rangle$ into the plane spanned by $|c\rangle$ and $|d\rangle$, so $|\tilde{\psi}\rangle$ has norm λ less than or equal to one. If θ is the angle $|d\rangle$ makes with $|c\rangle$ in this plane, and φ is the angle $|\tilde{\psi}\rangle$ makes with $|d\rangle$, then we see $p(c)q(d) = |\langle c \mid \tilde{\psi}\rangle\langle\tilde{\psi} \mid d\rangle|^2 = \lambda^2\cos^2(\theta-\varphi)\cos^2(\varphi)$. Calculus implies that the maximum is reached when $\lambda = 1$ and $\varphi = \theta/2$, at which point $p(c)q(d) = \cos^4(\theta/2)$, which can be put in the form

$$p(c)q(d) = \left(\frac{1 + |\langle c \mid d\rangle|}{2}\right)^2 \tag{11.6}$$

Combining this with Equation (11.5) gives

$$H(C) + H(D) \geq -2\log\frac{1 + f(C,D)}{2} \tag{11.7}$$

as claimed.

Moreover, for quantum entropies it is sometimes rather difficult to justify our intuitive beliefs about what concavity properties entropy ought to have.

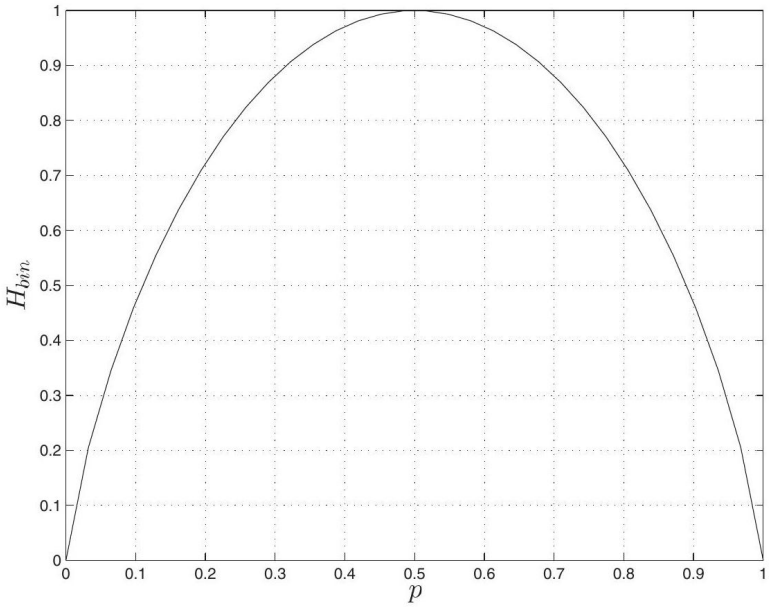


Figure 11.1. Binary entropy function $H(p)$.

Exercise 11.3: Prove that the binary entropy $H_{\text{bin}}(p)$ attains its maximum value of one at $p = 1/2$.

Exercise 11.4: (Concavity of the binary entropy) From Figure 11.1 it appears that the binary entropy is a concave function. Prove that this is so, that is:

$$H_{\text{bin}}\left(px_1 + (1-p)x_2\right) \geq pH_{\text{bin}}(x_1) + (1-p)H_{\text{bin}}(x_2), \tag{11.11}$$

where $0 \leq p, x_1, x_2 \leq 1$. Prove in addition that the binary entropy is strictly concave, that is, the above inequality is an equality only for the trivial cases $x_1 = x_2$, or $p = 0$, or $p = 1$.

9.4.4 11.2.2 The relative entropy

The relative entropy is a very useful entropy-like measure of the closeness of two probability distributions, $p(x)$ and $q(x)$, over the same index set, x. Suppose $p(x)$ and $q(x)$ are two probability distributions on the same index set, x. Define the relative entropy of $p(x)$ to $q(x)$ by

$$H(p(x)\|q(x)) \equiv \sum_x p(x) \log \frac{p(x)}{q(x)} \equiv -H(X) - \sum_x p(x) \log q(x). \tag{11.12}$$

We define $-0 \log 0 \equiv 0$ and $-p(x) \log 0 \equiv +\infty$ if $p(x) > 0$.
It is not immediately obvious what the relative entropy is good for, or even why it is a good measure of distance between two distributions. The following theorem gives some motivation as to why it is regarded as being like a distance measure.

Theorem 11.1: (Non-negativity of the relative entropy) The relative entropy is non-negative, $H(p(x)\|q(x)) \geq 0$, with equality if and only if $p(x) = q(x)$ for all x.

Proof

A very useful inequality in information theory is $\log x \ln 2 = \ln x \leq x - 1$, for all positive x, with equality if and only if $x = 1$. Here we need to rearrange the result slightly, to $-\log x \geq (1 - x)/\ln 2$, and then note that

$$\begin{aligned} H(p(x)\|q(x)) &= -\sum_x p(x) \log \frac{q(x)}{p(x)} && (11.13)\\ &\geq \frac{1}{\ln 2} \sum_x p(x) \left(1 - \frac{q(x)}{p(x)}\right) && (11.14)\\ &= \frac{1}{\ln 2} \sum_x (p(x) - q(x)) && (11.15)\\ &= \frac{1}{\ln 2}(1 - 1) = 0, && (11.16) \end{aligned}$$

which is the desired inequality. The equality conditions are easily deduced by noting that equality occurs in the second line if and only if $q(x)/p(x) = 1$ for all x, that is, the distributions are identical.

The relative entropy is often useful, not in itself, but because other entropic quantities can be regarded as special cases of the relative entropy. Results about the relative entropy then give as special cases results about other entropic quantities. For example, we can use the non-negativity of the relative entropy to prove the following fundamental fact about entropies. Suppose $p(x)$ is a probability distribution for X, over d outcomes. Let $q(x) \equiv 1/d$ be the uniform probability distribution over those outcomes. Then

$$H(p(x)\|q(x)) = H(p(x)\|1/d) = -H(X) - \sum_x p(x) \log(1/d) = \log d - H(X) \tag{11.17}$$

From the non-negativity of the relative entropy, Theorem 11.1, we see that $\log d - H(X) \geq 0$, with equality if and only if X is uniformly distributed. This is an elementary fact, but so important that we restate it formally as a theorem.

Theorem 11.2: Suppose X is a random variable with d outcomes. Then $H(X) \leq \log d$, with equality if and only if X is uniformly distributed over those d outcomes.

We use this technique - finding expressions for entropic quantities in terms of the relative entropy - often in the study of both classical and quantum entropies.

Exercise 11.5: (Subadditivity of the Shannon entropy) Show that $H(p(x,y)\|p(x)p(y)) = H(p(x)) + H(p(y)) - H(p(x,y))$. Deduce that $H(X,Y) \leq H(X) + H(Y)$, with equality if and only if X and Y are independent random variables.

9.4.5 11.2.3 Conditional entropy and mutual information

Suppose X and Y are two random variables. How is the information content of X related to the information content of Y ? In this section we introduce two concepts - the conditional entropy and the mutual information - which help answer this question. The definitions we give for these concepts are rather formal, and at times you may be confused as to why a particular quantity - say, the conditional entropy - is to be interpreted in the way we indicate. Keep in mind that the ultimate justification for these definitions is that they answer resource questions, which we investigate in more detail in Chapter 12, and that the interpretations given to the quantities depend on the nature of the resource question being answered.

We already met the joint entropy of a pair of random variables implicitly in the previous section. For clarity, we now make this definition explicit. The joint entropy of X and Y is defined in the obvious way,

$$H(X,Y) \equiv -\sum_{x,y} p(x,y) \log p(x,y) \tag{11.18}$$

and may be extended in the obvious way to any vector of random variables. The joint entropy measures our total uncertainty about the pair (X, Y). Suppose we know the value of Y, so we have acquired $H(Y)$ bits of information about the pair, (X, Y). The remaining uncertainty about the pair (X, Y), is associated with our remaining lack of knowledge about X, even given that we know Y. The entropy of X conditional on knowing Y is therefore defined by

$$H(X \mid Y) \equiv H(X,Y) - H(Y) \tag{11.19}$$

The conditional entropy is a measure of how uncertain we are, on average, about the value of X, given that we know the value of Y.

A second quantity, the mutual information content of X and Y, measures how much information X and Y have in common. Suppose we add the information content of X, $H(X)$, to the information content of Y. Information which is common to X and Y will have been counted twice in this sum, while information which is not common will have been counted exactly once. Subtracting off the joint information of $(X,Y), H(X,Y)$, we therefore obtain the common or mutual information of X and Y :

$$H(X : Y) \equiv H(X) + H(Y) - H(X,Y) \tag{11.20}$$

Note the useful equality $H(X : Y) = H(X) - H(X \mid Y)$ relating the conditional entropy and mutual information.

To get some feeling for how the Shannon entropy behaves, we now give some simple relationships between the different entropies.

Theorem 11.3: (Basic properties of Shannon entropy)

(1) $H(X,Y) = H(Y,X), H(X : Y) = H(Y : X)$.
(2) $H(Y \mid X) \geq 0$ and thus $H(X : Y) \leq H(Y)$, with equality if and only if Y is a function of $X, Y = f(X)$.

(3) $H(X) \leq H(X,Y)$, with equality if and only if Y is a function of X.
(4) Subadditivity: $H(X,Y) \leq H(X) + H(Y)$ with equality if and only if X and Y are independent random variables.
(5) $H(Y \mid X) \leq H(Y)$ and thus $H(X:Y) \geq 0$, with equality in each if and only if X and Y are independent random variables.
(6) Strong subadditivity: $H(X,Y,Z) + H(Y) \leq H(X,Y) + H(Y,Z)$, with equality if and only if $Z \to Y \to X$ forms a Markov chain.
(7) Conditioning reduces entropy: $H(X \mid Y,Z) \leq H(X \mid Y)$.

Most of the proofs are either obvious or easy exercises. We give a few hints below.

Proof

(1) Obvious from the relevant definitions.
(2) Since $p(x,y) = p(x)p(y \mid x)$ we have

$$H(X,Y) = -\sum_{xy} p(x,y) \log p(x)p(y \mid x) \tag{11.21}$$

$$= -\sum_{x} p(x) \log p(x) - \sum_{xy} p(x,y) \log p(y \mid x) \tag{11.22}$$

$$= H(X) - \sum_{xy} p(x,y) \log p(y \mid x). \tag{11.23}$$

Thus $H(Y \mid X) = -\sum_{xy} p(x,y) \log p(y \mid x)$. But $-\log p(y \mid x) \geq 0$, so $H(Y \mid X) \geq 0$ with equality if and only if Y is a deterministic function of X.
(3) Follows from the previous result.
(4) To prove subadditivity and, later, strong subadditivity we again use the fact that $\log x \leq (x-1)/\ln 2$ for all positive x, with equality if and only if $x = 1$. We find that

$$\sum_{x,y} p(x,y) \log \frac{p(x)p(y)}{p(x,y)} \leq \frac{1}{\ln 2} \sum_{x,y} p(x,y) \left(\frac{p(x)p(y)}{p(x,y)} - 1 \right) \tag{11.24}$$

$$= \frac{1}{\ln 2} \sum_{x,y} p(x)p(y) - p(x,y) = \frac{1-1}{\ln 2} = 0. \tag{11.25}$$

Subadditivity follows. Notice that equality is achieved if and only if $p(x,y) = p(x)p(y)$ for all x and y. That is, the subadditivity inequality is saturated if and only if X and Y are independent.
(5) Follows from subadditivity and the relevant definitions.
(6) Strong subadditivity of Shannon entropy follows from the same technique used to prove subadditivity; the difficulty level is only slightly higher than that proof. You will be asked to supply this proof as Exercise 11.6.
(7) Intuitively, we expect that the uncertainty about X, given that we know the value of Y and Z, is less than our uncertainty about X, given that we only know Y. More formally, inserting the relevant definitions, the result that conditioning reduces entropy is equivalent to

$$H(X,Y,Z) - H(Y,Z) \leq H(X,Y) - H(Y), \tag{11.26}$$

which is a rearranged version of the strong subadditivity inequality. □

Exercise 11.6: (Proof of classical strong subadditivity) Prove that $H(X,Y,Z) + H(Y) \leq H(X,Y) + H(Y,Z)$, with equality if and only if $Z \to Y \to X$ forms a Markov chain.

Exercise 11.7: In Exercise 11.5 you implicitly showed that the mutual information $H(X : Y)$ could be expressed as the relative entropy of two probability distributions, $H(X : Y) = H(p(x, y)\|p(x)p(y))$. Find an expression for the
conditional entropy $H(Y \mid X)$ as a relative entropy between two probability distributions. Use this expression to deduce that $H(Y \mid X) \geq 0$, and to find the equality conditions.

The various relationships between entropies may mostly be deduced from the 'entropy Venn diagram' shown in Figure 11.2. Such figures are not completely reliable as a guide to the properties of entropy, but they provide a useful mnemonic for remembering the various definitions and properties of entropy.

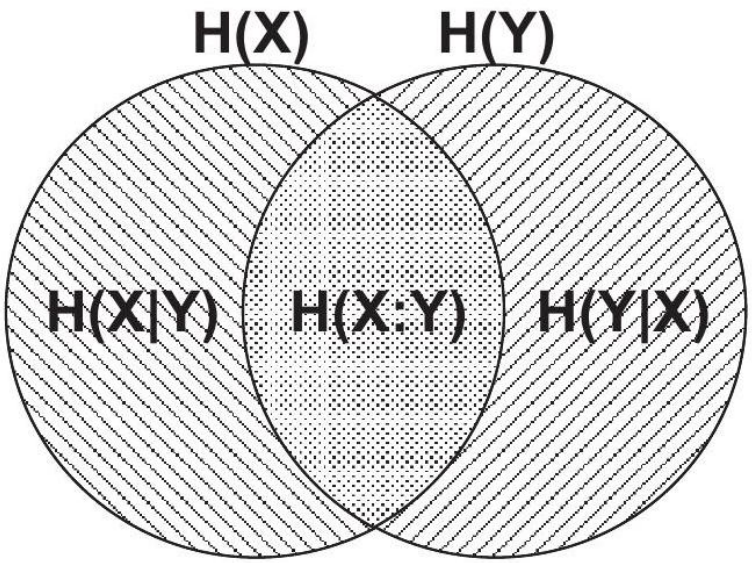


Figure 11.2. Relationships between different entropies.

We conclude our study of the elementary properties of conditional entropy and mutual information with a simple and useful chaining rule for conditional entropies.

Theorem 11.4: (Chaining rule for conditional entropies) Let $X_1, \ldots, X_n$ and Y be any set of random variables. Then

$$H(X_1, \ldots, X_n \mid Y) = \sum_{i=1}^{n} H(X_i \mid Y, X_1, \ldots, X_{i-1}) \tag{11.27}$$

Proof

We prove the result for $n = 2$, and then induct on n. Using only the definitions and some simple algebra we have

$$\begin{aligned} H(X_1, X_2 \mid Y) &= H(X_1, X_2, Y) - H(Y) && (11.28)\\ &= H(X_1, X_2, Y) - H(X_1, Y) + H(X_1, Y) - H(Y) && (11.29)\\ &= H(X_2 \mid Y, X_1) + H(X_1 \mid Y) && (11.30) \end{aligned}$$

which establishes the result for $n = 2$. Now we assume the result for general n, and show the result holds for $n + 1$. Using the already established $n = 2$ case, we have

$$H(X_1, \ldots, X_{n+1} \mid Y) = H(X_2, \ldots, X_{n+1} \mid Y, X_1) + H(X_1 \mid Y). \tag{11.31}$$

Applying the inductive hypothesis to the first term on the right hand side gives

$$H\left(X_1, \ldots, X_{n+1} \mid Y\right) = \sum_{i=2}^{n+1} H\left(X_i \mid Y, X_1, \ldots, X_{i-1}\right) + H\left(X_1 \mid Y\right) \tag{11.32}$$

$$= \sum_{i=1}^{n+1} H\left(X_i \mid Y, X_1, \ldots, X_{i-1}\right), \tag{11.33}$$

and the induction goes through. □

Exercise 11.8: (Mutual information is not always subadditive) Let X and Y be independent identically distributed random variables taking the values 0 or 1 with probability 1/2. Let $Z \equiv X \oplus Y$, where $\oplus$ denotes addition modulo 2 . Show that the mutual information in this case is not subadditive,

$$H(X, Y : Z) \not\leq H(X : Z) + H(Y : Z). \tag{11.34}$$

Exercise 11.9: (Mutual information is not always superadditive) Let X_1 be a random variable taking values 0 or 1 with respective probabilities of 1/2 and $X_2 \equiv Y_1 \equiv Y_2 \equiv X_1$. Show that the mutual information in this case is not superadditive,

$$H\left(X_1 : Y_1\right) + H\left(X_2 : Y_2\right) \not\leq H\left(X_1, X_2 : Y_1, Y_2\right) \tag{11.35}$$

9.4.6 11.2.4 The data processing inequality

In many applications of interest we perform computations on the information we have available, but that information is imperfect, as it has been subjected to noise before it becomes available to us. A basic inequality of information theory, the data processing inequality, states that information about the output of a source can only decrease with time: once information has been lost, it is gone forever. Making this statement more precise is the goal of this section.

The intuitive notion of information processing is captured in the idea of a Markov chain of random variables. A Markov chain is a sequence $X_1 \to X_2 \to \cdots$ of random variables such that X_{n+1} is independent of $X_1, \ldots, X_{n-1}$, given X_n. More formally,

$$p\left(X_{n+1} = x_{n+1} \mid X_n = x_n, \ldots, X_1 = x_1\right) = p\left(X_{n+1} = x_{n+1} \mid X_n = x_n\right). \tag{11.36}$$

Under what conditions does a Markov chain lose information about its early values, as time progresses? The following data processing inequality gives an information-theoretic way of answering this question.

Theorem 11.5: (Data processing inequality) Suppose $X \to Y \to Z$ is a Markov chain. Then

$$H(X) \geq H(X : Y) \geq H(X : Z). \tag{11.37}$$

Moreover, the first inequality is saturated if and only if, given Y, it is possible to reconstruct X.

This result is intuitively plausible: it tells us that if a random variable X is subject to noise, producing Y, then further actions on our part ('data processing') cannot be used to increase the amount of mutual information between the output of the process and the original information X.

The first inequality was proved in Theorem 11.3 on page 507. From the definitions we see that $H(X : Z) \leq H(X : Y)$ is equivalent to $H(X \mid Y) \leq H(X \mid Z)$. From the fact that $X \to Y \to Z$ is a Markov chain it is easy to prove (Exercise 11.10) that $Z \to Y \to X$ is also a Markov chain, and thus $H(X \mid Y) = H(X \mid Y, Z)$. The problem is thus reduced to proving

that $H(X,Y,Z) - H(Y,Z) = H(X \mid Y,Z) \leq H(X \mid Z) = H(X,Z) - H(Z)$. This is just the already proved strong subadditivity inequality.

Suppose $H(X:Y) < H(X)$. Then it is not possible to reconstruct X from Y, since if Z is the attempted reconstruction based only on knowledge of Y, then $X \rightarrow Y \rightarrow Z$ must be a Markov chain, and thus $H(X) > H(X:Z)$ by the data processing inequality. Thus $Z \neq X$. On the other hand, if $H(X:Y) = H(X)$, then we have $H(X \mid Y) = 0$ and thus whenever $p(X = x, Y = y) > 0$ we have $p(X = x \mid Y = y) = 1$. That is, if $Y = y$ then we can infer with certainty that X was equal to x, allowing us to reconstruct X.

As noted above, if $X \rightarrow Y \rightarrow Z$ is a Markov chain, then so is $Z \rightarrow Y \rightarrow X$. Thus, as a corollary to the data processing inequality we see that if $X \rightarrow Y \rightarrow Z$ is a Markov chain then

$$H(Z:Y) \geq H(Z:X) \tag{11.38}$$

We refer to this result as the data pipelining inequality. Intuitively, it says that any information Z shares with X must be information which Z also shares with Y; the information is 'pipelined' from X through Y to Z.

Exercise 11.10: Show that if $X \rightarrow Y \rightarrow Z$ is a Markov chain then so is

$$Z \rightarrow Y \rightarrow X$$

9.4.7 11.3 Von Neumann entropy

The Shannon entropy measures the uncertainty associated with a classical probability distribution. Quantum states are described in a similar fashion, with density operators replacing probability distributions. In this section we generalize the definition of the Shannon entropy to quantum states.

Von Neumann defined the entropy of a quantum state ρ by the formula

$$S(\rho) \equiv -\operatorname{tr}(\rho \log \rho) \tag{11.39}$$

In this formula logarithms are taken to base two, as usual. If λ_x are the eigenvalues of ρ then von Neumann's definition can be re-expressed

$$S(\rho) = -\sum_x \lambda_x \log \lambda_x \tag{11.40}$$

where we define $0 \log 0 \equiv 0$, as for the Shannon entropy. For calculations it is usually this last formula which is most useful. For instance, the completely mixed density operator in a d-dimensional space, I/d, has entropy $\log d$.

From now on, when we refer to entropy, it will usually be clear from context whether we mean the Shannon or von Neumann entropy.

Exercise 11.11: (Example calculations of entropy) Calculate $S(\rho)$ for

$$\rho = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \tag{11.41}$$

$$\rho = \frac{1}{2} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \tag{11.42}$$

$$\rho = \frac{1}{3} \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}. \tag{11.43}$$

Exercise 11.12: (Comparison of quantum and classical entropies) Suppose $\rho = p|0\rangle\langle 0| + (1-p)\frac{(|0\rangle+|1\rangle)(\langle 0|+\langle 1|)}{2}$. Evaluate $S(\rho)$. Compare the value of $S(\rho)$ to $H(p, 1-p)$.

9.4.8 11.3.1 Quantum relative entropy

As for the Shannon entropy, it is extremely useful to define a quantum version of the relative entropy. Suppose ρ and σ are density operators. The relative entropy of ρ to σ is defined by

$$S(\rho\|\sigma) \equiv \mathrm{tr}(\rho \log \rho) - \mathrm{tr}(\rho \log \sigma). \tag{11.50}$$

As with the classical relative entropy, the quantum relative entropy can sometimes be infinite. In particular, the relative entropy is defined to be $+\infty$ if the kernel of σ (the vector space spanned by the eigenvectors of σ with eigenvalue 0) has non-trivial intersection with the support of ρ (the vector space spanned by the eigenvectors of ρ with non-zero eigenvalue), and is finite otherwise. The quantum relative entropy is non-negative, a result sometimes known as Klein's inequality:

Theorem 11.7: (Klein's inequality) The quantum relative entropy is non-negative,

$$S(\rho\|\sigma) \geq 0, \tag{11.51}$$

with equality if and only if $\rho = \sigma$.

Proof

Let $\rho = \sum_i p_i |i\rangle\langle i|$ and $\sigma = \sum_j q_j |j\rangle\langle j|$ be orthonormal decompositions for ρ and σ. From the definition of the relative entropy we have

$$S(\rho\|\sigma) = \sum_i p_i \log p_i - \sum_i \langle i|\rho \log \sigma|i\rangle. \tag{11.52}$$

We substitute into this equation the equations $\langle i|\rho = p_i\langle i|$ and

$$\langle i| \log \sigma |i\rangle = \langle i| \left(\sum_j \log\left(q_j\right) |j\rangle\langle j| \right) |i\rangle = \sum_j \log\left(q_j\right) P_{ij}, \tag{11.53}$$

where $P_{ij} \equiv \langle i \mid j\rangle\langle j \mid i\rangle \geq 0$, to give

$$S(\rho\|\sigma) = \sum_i p_i \left(\log p_i - \sum_j P_{ij} \log\left(q_j\right) \right). \tag{11.54}$$

Note that P_{ij} satisfies the equations $P_{ij} \geq 0, \sum_i P_{ij} = 1$ and $\sum_j P_{ij} = 1$. (Regarding P_{ij}

Box 11.2: Continuity of the entropy

Suppose we vary ρ by a small amount. How much does $S(\rho)$ change? Fannes' inequality tells us that the answer is 'not much', and even provides a bound on how small the change is.

Theorem 11.6: (Fannes' inequality) Suppose ρ and σ are density matrices such that the trace distance between them satisfies $T(\rho, \sigma) \leq 1/e$. Then

$$|S(\rho) - S(\sigma)| \leq T(\rho, \sigma) \log d + \eta(T(\rho, \sigma)) \tag{11.44}$$

where d is the dimension of the Hilbert space, and $\eta(x) \equiv -x \log x$.
Removing the restriction that $T(\rho, \sigma) \leq 1/e$ we can prove the weaker inequality

$$|S(\rho) - S(\sigma)| \leq T(\rho, \sigma) \log d + \frac{1}{e} \tag{11.45}$$

Proof

To prove Fannes' inequality we need a simple result relating the trace distance between two operators to their eigenvalues. Let $r_1 \geq r_2 \geq \cdots \geq r_d$ be the eigenvalues of ρ, in descending order, and $s_1 \geq s_2 \geq \cdots \geq s_d$ be the eigenvalues of σ, again in descending order. By the spectral decomposition we may decompose $\rho - \sigma = Q - R$, where Q and R are positive operators with orthogonal support, so $T(\rho, \sigma) = \mathrm{tr}(R) + \mathrm{tr}(Q)$. Defining $V \equiv R + \rho = Q + \sigma$, we have $T(\rho, \sigma) = \mathrm{tr}(R) + \mathrm{tr}(Q) = \mathrm{tr}(2V) - \mathrm{tr}(\rho) - \mathrm{tr}(\sigma)$. Let $t_1 \geq t_2 \geq \cdots \geq t_d$ be the eigenvalues of T. Note that $t_i \geq \max(r_i, s_i)$, so $2t_i \geq r_i + s_i + |r_i - s_i|$, and it follows that

$$T(\rho, \sigma) \geq \sum_i |r_i - s_i| \tag{11.46}$$

By calculus whenever $|r - s| \leq 1/2$ it follows that $|\eta(r) - \eta(s)| \leq \eta(|r - s|)$. A moment's thought shows that $|r_i - s_i| \leq 1/2$ for all i, so

$$|S(\rho) - S(\sigma)| = \left| \sum_i \left(\eta(r_i) - \eta(s_i) \right) \right| \leq \sum_i \eta\left(|r_i - s_i| \right). \tag{11.47}$$

Setting $\Delta \equiv \sum_i |r_i - s_i|$ and observing that $\eta(|r_i - s_i|) = \Delta \eta(|r_i - s_i|/\Delta) - \mid r_i - s_i \mid \log(\Delta)$, we see that

$$|S(\rho) - S(\sigma)| \leq \Delta \sum \eta\left(|r_i - s_i| / \Delta \right) + \eta(\Delta) \leq \Delta \log d + \eta(\Delta) \tag{11.48}$$

where we applied Theorem 11.2 to obtain the second inequality. But $\Delta \leq T(\rho, \sigma)$ by (11.46), so by the monotonicity of $\eta(\cdot)$ on the interval $[0, 1/e]$,

$$|S(\rho) - S(\sigma)| \leq T(\rho, \sigma) \log d + \eta(T(\rho, \sigma)) \tag{11.49}$$

whenever $T(\rho, \sigma) \leq 1/e$, which is Fannes' inequality. The weaker form of Fannes' inequality for general $T(\rho, \sigma)$ follows with minor modifications.
as a matrix, this property is known as double stochasticity.) Because $\log(\cdot)$ is a strictly concave function it follows that $\sum_j P_{ij} \log q_j \leq \log r_i$, where $r_i \equiv \sum_j P_{ij} q_j$, with equality if and only if there exists a value of j for which $P_{ij} = 1$. Thus

$$S(\rho \| \sigma) \geq \sum_i p_i \log \frac{p_i}{r_i} \tag{11.55}$$

with equality if and only if for each i there exists a value of j such that $P_{ij} = 1$, that is, if and only if P_{ij} is a permutation matrix. This has the form of the classical relative entropy. From the non-negativity of the classical relative entropy, Theorem 11.1, we deduce that

$$S(\rho \| \sigma) \geq 0 \tag{11.56}$$

with equality if and only if $p_i = r_i$ for all i, and P_{ij} is a permutation matrix. To simplify the equality conditions further, note that by relabeling the eigenstates of σ if necessary, we can assume that P_{ij} is the identity matrix, and thus that ρ and σ are diagonal in the same basis. The condition $p_i = r_i$ tells us that the corresponding eigenvalues of ρ and σ are identical, and thus $\rho = \sigma$ are the equality conditions.

9.4.9 11.3.2 Basic properties of entropy

The von Neumann entropy has many interesting and useful properties:

Theorem 11.8: (Basic properties of von Neumann entropy)

(1) The entropy is non-negative. The entropy is zero if and only if the state is pure.
(2) In a d-dimensional Hilbert space the entropy is at most $\log d$. The entropy is equal to $\log d$ if and only if the system is in the completely mixed state I/d.
(3) Suppose a composite system AB is in a pure state. Then $S(A) = S(B)$.
(4) Suppose p_i are probabilities, and the states ρ_i have support on orthogonal subspaces. Then

$$S\left(\sum_i p_i \rho_i\right) = H\left(p_i\right) + \sum_i p_i S\left(\rho_i\right). \tag{11.57}$$

(5) Joint entropy theorem: Suppose p_i are probabilities, $|i\rangle$ are orthogonal states for a system A, and ρ_i is any set of density operators for another system, B. Then

$$S\left(\sum_i p_i |i\rangle\langle i| \otimes \rho_i\right) = H\left(p_i\right) + \sum_i p_i S\left(\rho_i\right). \tag{11.58}$$

Proof

(1) Clear from the definition.
(2) The result follows from the non-negativity of the relative entropy, $0 \leq S(\rho \| I/d) = -S(\rho) + \log d$.
(3) From the Schmidt decomposition we know that the eigenvalues of the density operators of systems A and B are the same. (Recall the discussion following Theorem 2.7 on page 109.) The entropy is determined completely by the eigenvalues, so $S(A) = S(B)$.
(4) Let λ_i^j and $\left|e_i^j\right\rangle$ be the eigenvalues and corresponding eigenvectors of ρ_i. Observe that $p_i \lambda_i^j$ and $\left|e_i^j\right\rangle$ are the eigenvalues and eigenvectors of $\sum_i p_i \rho_i$, and thus

$$\begin{aligned} S\left(\sum_i p_i \rho_i\right) &= -\sum_{ij} p_i \lambda_i^j \log p_i \lambda_i^j & (11.59)\\ &= -\sum_i p_i \log p_i - \sum_i p_i \sum_j \lambda_i^j \log \lambda_i^j & (11.60)\\ &= H\left(p_i\right) + \sum_i p_i S\left(\rho_i\right) & (11.61) \end{aligned}$$

as required.
(5) Immediate from the preceding result.

Exercise 11.13: (Entropy of a tensor product) Use the joint entropy theorem to show that $S(\rho \otimes \sigma) = S(\rho) + S(\sigma)$. Prove this result directly from the definition of the entropy.

By analogy with the Shannon entropies it is possible to define quantum joint and conditional entropies and quantum mutual information, for composite quantum systems. The joint entropy $S(A, B)$ for a composite system with two components A and B is defined in the obvious way, $S(A, B) \equiv -\operatorname{tr}\left(\rho^{AB} \log\left(\rho^{AB}\right)\right)$, where ρ^{AB} is the density matrix of the system AB. We define the conditional entropy and mutual information by:

$$\begin{aligned} S(A \mid B) &\equiv S(A, B) - S(B) & (11.62)\\ S(A : B) &\equiv S(A) + S(B) - S(A, B) & (11.63)\\ &= S(A) - S(A \mid B) = S(B) - S(B \mid A) & (11.64) \end{aligned}$$

Some properties of the Shannon entropy fail to hold for the von Neumann entropy, and this has many interesting consequences for quantum information theory. For instance, for random variables X and Y, the inequality $H(X) \leq H(X,Y)$ holds. This makes intuitive sense: surely we cannot be more uncertain about the state of X than we are about the joint state of X and Y. This intuition fails for quantum states. Consider a system AB of two qubits in the entangled state $(|00\rangle + |11\rangle)/\sqrt{2}$. This is a pure state, so $S(A,B) = 0$. On the other hand, system A has density operator $I/2$, and thus has entropy equal to one. Another way of stating this result is that, for this system, the quantity $S(B \mid A) = S(A,B) - S(A)$ is negative.

Exercise 11.14: (Entanglement and negative conditional entropy) Suppose $|AB\rangle$ is a pure state of a composite system belonging to Alice and Bob. Show that $|AB\rangle$ is entangled if and only if $S(B \mid A) < 0$.

9.4.10 11.3.3 Measurements and entropy

How does the entropy of a quantum system behave when we perform a measurement on that system? Not surprisingly, the answer to this question depends on the type of measurement which we perform. Nevertheless, there are some surprisingly general assertions we can make about how the entropy behaves.

Suppose, for example, that a projective measurement described by projectors P_i is performed on a quantum system, but we never learn the result of the measurement. If the state of the system before the measurement was ρ then the state after is given by

$$\rho' = \sum_i P_i \rho P_i \tag{11.65}$$

The following result shows that the entropy is never decreased by this procedure, and remains constant only if the state is not changed by the measurement:

Theorem 11.9: (Projective measurements increase entropy) Suppose P_i is a complete set of orthogonal projectors and ρ is a density operator. Then the entropy of the state $\rho' \equiv \sum_i P_i \rho P_i$ of the system after the measurement is at least as great as the original entropy,

$$S(\rho') \geq S(\rho) \tag{11.66}$$

with equality if and only if $\rho = \rho'$.

Proof

The proof is to apply Klein's inequality to ρ and ρ',

$$0 \leq S(\rho' \| \rho) = -S(\rho) - \operatorname{tr}(\rho \log \rho') \tag{11.67}$$

The result will follow if we can prove that $-\operatorname{tr}(\rho \log \rho') = S(\rho')$. To do this, we apply the completeness relation $\sum_i P_i = I$, the relation $P_i^2 = P_i$, and the cyclic property of the trace, to obtain

$$-\operatorname{tr}(\rho \log \rho') = -\operatorname{tr}\left(\sum_i P_i \rho \log \rho'\right) \tag{11.68}$$

$$= -\operatorname{tr}\left(\sum_i P_i \rho \log \rho' P_i\right). \tag{11.69}$$

Note that $\rho' P_i = P_i \rho P_i = P_i \rho'$. That is, P_i commutes with ρ' and thus with $\log \rho'$, so

$$-\operatorname{tr}(\rho \log \rho') = -\operatorname{tr}\left(\sum_i P_i \rho P_i \log \rho'\right) \tag{11.70}$$

$$= -\operatorname{tr}(\rho' \log \rho') = S(\rho') \tag{11.71}$$

This completes the proof.

Exercise 11.15: (Generalized measurements can decrease entropy) Suppose a qubit in the state ρ is measured using the measurement operators $M_1 = |0\rangle\langle 0|$ and $M_2 = |0\rangle\langle 1|$. If the result of the measurement is unknown to us then the state of the system afterwards is $M_1 \rho M_1^\dagger + M_2 \rho M_2^\dagger$. Show that this procedure can decrease the entropy of the qubit.

9.4.11 11.3.4 Subadditivity

Suppose distinct quantum systems A and B have a joint state ρ^{AB}. Then the joint entropy for the two systems satisfies the inequalities

$$S(A,B) \leq S(A) + S(B) \tag{11.72}$$

$$S(A,B) \geq |S(A) - S(B)| \tag{11.73}$$

The first of these inequalities is known as the subadditivity inequality for Von Neumann entropy, and holds with equality if and only if systems A and B are uncorrelated, that is, $\rho^{AB} = \rho^A \otimes \rho^B$. The second is called the triangle inequality, or sometimes the Araki-Lieb inequality; it is the quantum analogue of the inequality $H(X,Y) \geq H(X)$ for Shannon entropies.

The proof of subadditivity is a simple application of Klein's inequality, $S(\rho) \leq -\operatorname{tr}(\rho \log \sigma)$. Setting $\rho \equiv \rho^{AB}$ and $\sigma \equiv \rho^A \otimes \rho^B$, note that

$$-\operatorname{tr}(\rho \log \sigma) = -\operatorname{tr}\left(\rho^{AB}\left(\log \rho^A + \log \rho^B\right)\right) \tag{11.74}$$

$$= -\operatorname{tr}\left(\rho^A \log \rho^A\right) - \operatorname{tr}\left(\rho^B \log \rho^B\right) \tag{11.75}$$

$$= S(A) + S(B) \tag{11.76}$$

Klein's inequality therefore gives $S(A,B) \leq S(A) + S(B)$, as desired. The equality conditions $\rho = \sigma$ for Klein's inequality give equality conditions $\rho^{AB} = \rho^A \otimes \rho^B$ for subadditivity.

To prove the triangle inequality, introduce a system R which purifies systems A and B, as in Section 2.5. Applying subadditivity we have

$$S(R) + S(A) \geq S(A,R) \tag{11.77}$$

Since ABR is in a pure state, $S(A,R) = S(B)$ and $S(R) = S(A,B)$. The previous inequality may be rearranged to give

$$S(A,B) \geq S(B) - S(A) \tag{11.78}$$

The equality conditions for this inequality are not quite as easily stated as those for subadditivity. Formally, the equality conditions are that $\rho^{AR} = \rho^A \otimes \rho^R$. Intuitively, what this means is that A is already as entangled as it can possibly be with the outside world, given its existing correlations with system B. A more detailed mathematical statement of the equality conditions is given in Exercise 11.16 on this page.

By symmetry between the systems A and B we also have $S(A,B) \geq S(A) - S(B)$. Combining this with $S(A,B) \geq S(B) - S(A)$ gives the triangle inequality.

Exercise 11.16: (Equality conditions for $S(A,B) \geq S(B) - S(A)$) Let $\rho^{AB} = \sum_i \lambda_i |i\rangle\langle i|$ is a spectral decomposition for ρ^{AB}. Show that $S(A,B) = S(B) - S(A)$ if and only if the operators $\rho_i^A \equiv \mathrm{tr}_B(|i\rangle\langle i|)$ have a common eigenbasis, and the $\rho_i^B \equiv \mathrm{tr}_A(|i\rangle\langle i|)$ have orthogonal support.

Exercise 11.17: Find an explicit non-trivial example of a mixed state ρ for AB such that $S(A,B) = S(B) - S(A)$.

9.4.12 11.3.5 Concavity of the entropy

The entropy is a concave function of its inputs. That is, given probabilities p_i - nonnegative real numbers such that $\sum_i p_i = 1-$ and corresponding density operators ρ_i, the entropy satisfies the inequality:

$$S\left(\sum_i p_i \rho_i\right) \geq \sum_i p_i S\left(\rho_i\right) \tag{11.79}$$

The intuition is that the $\sum_i p_i \rho_i$ expresses the state of a quantum system which is in an unknown state ρ_i with probability p_i, and our uncertainty about this mixture of states should be higher than the average uncertainty of the states ρ_i, since the state $\sum_i p_i \rho_i$ expresses ignorance not only due to the states ρ_i, but also a contribution due to our ignorance of the index i.

Suppose the ρ_i are states of a system A. Introduce an auxiliary system B whose state space has an orthonormal basis $|i\rangle$ corresponding to the index i on the density operators ρ_i. Define a joint state of AB by:

$$\rho^{AB} \equiv \sum_i p_i \rho_i \otimes |i\rangle\langle i|. \tag{11.80}$$

To prove concavity we use the subadditivity of the entropy. Note that for the density matrix ρ^{AB} we have:

$$S(A) = S\left(\sum_i p_i \rho_i\right) \tag{11.81}$$

$$S(B) = S\left(\sum_i p_i |i\rangle\langle i|\right) = H\left(p_i\right) \tag{11.82}$$

$$S(A,B) = H\left(p_i\right) + \sum_i p_i S\left(\rho_i\right). \tag{11.83}$$

Applying the subadditivity inequality $S(A,B) \leq S(A) + S(B)$ we obtain

$$\sum_i p_i S\left(\rho_i\right) \leq S\left(\sum_i p_i \rho_i\right), \tag{11.84}$$

which is concavity! Note that equality holds if and only if all the states ρ_i for which $p_i > 0$ are identical; that is, the entropy is a strictly concave function of its inputs.

It's worth pausing to think about the strategy we've employed in the proof of concavity, and the similar strategy used to prove the triangle inequality. We introduced an auxiliary system B in order to prove a result about the system A. Introducing auxiliary systems is something done often in quantum information theory, and we'll see this trick again and again. The intuition behind the introduction of B in this particular instance is as follows: we want to find a system of which part is in the state $\sum_i p_i \rho_i$, where the value of i is not known. System B effectively

stores the 'true' value of i; if A were 'truly' in state ρ_i, the system B would be in state $|i\rangle\langle i|$, and observing system B in the $|i\rangle$ basis would reveal this fact. Using auxiliary systems to encode our intuition in a rigorous way is an art, but it is also an essential part of many proofs in quantum information theory.

Exercise 11.18: Prove that equality holds in the concavity inequality (11.79) if and only if all the ρ_i S are the same.

Exercise 11.19: Show that there exists a set of unitary matrices U_j and a probability distribution p_j such that for any matrix A,

$$\sum_i p_i U_i A U_i^\dagger = \mathrm{tr}(A)\frac{I}{d}, \tag{11.85}$$

where d is the dimension of the Hilbert space A lives in. Use this observation and the strict concavity of the entropy to give an alternate proof that the completely mixed state I/d on a space of d dimensions is the unique state of maximal entropy.

Exercise 11.20: Let P be a projector and $Q = I - P$ the complementary projector. Prove that there are unitary operators U_1 and U_2 and a probability p such that for all ρ, $P\rho P + Q\rho Q = pU_1\rho U_1^\dagger + (1-p)U_2\rho U_2^\dagger$. Use this observation to give an alternate proof of Theorem 11.9 based on concavity.

Exercise 11.21: (Concavity of the Shannon entropy) Use the concavity of the von Neumann entropy to deduce that the Shannon entropy is concave in probability distributions.

Exercise 11.22: (Alternate proof of concavity) Define $f(p) \equiv S(p\rho + (1-p)\sigma)$. Argue that to show concavity it is sufficient to prove that $f''(p) \leq 0$. Prove that $f''(p) \leq 0$, first for the case where ρ and σ are invertible, and then for the case where they are not.

9.4.13 11.3.6 The entropy of a mixture of quantum states

The flip side of concavity is the following useful theorem which provides an upper bound on the entropy of a mixture of quantum states. Taken together the two results imply that for a mixture $\sum_i p_i\rho_i$ of quantum states ρ_i the following inequality holds:

$$\sum_i p_i S(\rho_i) \leq S\left(\sum_i p_i\rho_i\right) \leq \sum_i p_i S(\rho_i) + H(p_i). \tag{11.86}$$

The intuition behind the upper bound on the right hand side is that our uncertainty about the state $\sum_i p_i\rho_i$ is never more than our average uncertainty about the state ρ_i, plus an additional contribution of $H(p_i)$ which represents the maximum possible contribution our uncertainty about the index i contributes to our total uncertainty. We now prove this upper bound.

Theorem 11.10: Suppose $\rho = \sum_i p_i\rho_i$, where p_i are some set of probabilities, and the ρ_i are density operators. Then

$$S(\rho) \leq \sum_i p_i S(\rho_i) + H(p_i), \tag{11.87}$$

with equality if and only if the states ρ_i have support on orthogonal subspaces.

Proof

We begin with the pure state case, $\rho_i = |\psi_i\rangle\langle\psi_i|$. Suppose the ρ_i are states of a system A, and introduce an auxiliary system B with an orthonormal basis $|i\rangle$ corresponding to the index i on the probabilities p_i. Define

$$|AB\rangle \equiv \sum_i \sqrt{p_i}\,|\psi_i\rangle\,|i\rangle. \tag{11.88}$$

Since $|AB\rangle$ is a pure state we have

$$S(B) = S(A) = S\left(\sum_i p_i\,|\psi_i\rangle\,\langle\psi_i|\right) = S(\rho). \tag{11.89}$$

Suppose we perform a projective measurement on the system B in the $|i\rangle$ basis. After the measurement the state of system B is

$$\rho^{B'} = \sum_i p_i |i\rangle\langle i|. \tag{11.90}$$

But by Theorem 11.9 projective measurements never decrease entropy, so $S(\rho) = S(B) \leq S\left(B'\right) = H\left(p_i\right)$. Observing that $S\left(\rho_i\right) = 0$ for the pure state case, we have proved that

$$S(\rho) \leq H\left(p_i\right) + \sum_i p_i S\left(\rho_i\right), \tag{11.91}$$

when the states ρ_i are pure states. Furthermore, equality holds if and only if $B = B'$, which is easily seen to occur if and only if the states $|\psi_i\rangle$ are orthogonal.

The mixed state case is now easy. Let $\rho_i = \sum_j p_j^i \left|e_j^i\right\rangle \left\langle e_j^i\right|$ be orthonormal decompositions for the states ρ_i, so $\rho = \sum_{ij} p_i p_j^i \left|e_j^i\right\rangle \left\langle e_j^i\right|$. Applying the pure state result and the observation that $\sum_j p_j^i = 1$ for each i, we have

$$\begin{aligned} S(\rho) &\leq -\sum_{ij} p_i p_j^i \log\left(p_i p_j^i\right) && (11.92)\\ &= -\sum_i p_i \log p_i - \sum_i p_i \sum_j p_j^i \log p_j^i && (11.93)\\ &= H\left(p_i\right) + \sum_i p_i S\left(\rho_i\right), && (11.94) \end{aligned}$$

which is the desired result. The equality conditions for the mixed state case follow immediately from the equality conditions for the pure state case. □

9.4.14 11.4 Strong subadditivity

The subadditivity and triangle inequalities for two quantum systems can be extended to three systems. The basic result is known as the strong subadditivity inequality, and it is one of the most important and useful results in quantum information theory. The inequality states that for a trio of quantum systems, A, B, C,

$$S(A, B, C) + S(B) \leq S(A, B) + S(B, C). \tag{11.95}$$

Unfortunately, unlike the classical case, all known proofs of the quantum strong subadditivity inequality are quite difficult. However, it is so useful in quantum information theory that we give a full proof of this result. The basic structure of the proof is presented in Section 11.4.1, with some of the details of the proof left to Appendix 6.

9.4.15 11.4.1 Proof of strong subadditivity

The proof of the strong subadditivity inequality which we shall give is based upon a deep mathematical result known as Lieb's theorem. We begin with a definition which allows us to state Lieb's theorem.

Suppose $f(A, B)$ is a real-valued function of two matrices, A and B. Then f is said to be jointly concave in A and B if for all $0 \leq \lambda \leq 1$,

$$f\left(\lambda A_1 + (1-\lambda)A_2, \lambda B_1 + (1-\lambda)B_2\right) \geq \lambda f\left(A_1, B_1\right) + (1-\lambda) f\left(A_2, B_2\right). \tag{11.96}$$

Exercise 11.23: (Joint concavity implies concavity in each input) Let $f(A, B)$ be a jointly concave function. Show that $f(A, B)$ is concave in A, with B held fixed. Find a function of two variables that is concave in each of its inputs, but is not jointly concave.

Theorem 11.11: (Lieb's theorem) Let X be a matrix, and $0 \leq t \leq 1$. Then the function

$$f(A, B) \equiv \operatorname{tr}\left(X^\dagger A^t X B^{1-t}\right) \tag{11.97}$$

is jointly concave in positive matrices A and B.

Proof

See Appendix 6 for the proof of Lieb's theorem.

Lieb's theorem implies a sequence of results, each interesting in its own right, culminating in the proof of strong subadditivity. We begin with the convexity of the relative entropy.

Theorem 11.12: (Convexity of the relative entropy) The relative entropy $S(\rho\|\sigma)$ is jointly convex in its arguments.

Proof

For arbitrary matrices A and X acting on the same space define

$$I_t(A, X) \equiv \operatorname{tr}\left(X^\dagger A^t X A^{1-t}\right) - \operatorname{tr}\left(X^\dagger X A\right) \tag{11.98}$$

The first term in this expression is concave in A, by Lieb's theorem, and the second term is linear in A. Thus, $I_t(A, X)$ is concave in A. Define

$$I(A, X) \equiv \left.\frac{d}{dt}\right|_{t=0} I_t(A, X) = \operatorname{tr}\left(X^\dagger (\log A) X A\right) - \operatorname{tr}\left(X^\dagger X (\log A) A\right) \tag{11.99}$$

Noting that $I_0(A, X) = 0$ and using the concavity of $I_t(A, X)$ in A we have

$$\begin{aligned} I\left(\lambda A_1 + (1-\lambda)A_2, X\right) &= \lim_{\Delta \to 0} \frac{I_\Delta\left(\lambda A_1 + (1-\lambda)A_2, X\right)}{\Delta} && (11.100)\\ &\geq \lambda \lim_{\Delta \to 0} \frac{I_\Delta\left(A_1, X\right)}{\Delta} + (1-\lambda) \lim_{\Delta \to 0} \frac{I_\Delta\left(A_2, X\right)}{\Delta} && (11.101)\\ &= \lambda I\left(A_1, X\right) + (1-\lambda) I\left(A_2, X\right) && (11.102) \end{aligned}$$

That is, $I(A, X)$ is a concave function of A. Defining the block matrices

$$A \equiv \begin{bmatrix} \rho & 0 \\ 0 & \sigma \end{bmatrix}, \quad X \equiv \begin{bmatrix} 0 & 0 \\ I & 0 \end{bmatrix} \tag{11.103}$$

we can easily verify that $I(A, X) = -S(\rho\|\sigma)$. The joint convexity of $S(\rho\|\sigma)$ follows from the concavity of $I(A, X)$ in A.

Corollary 11.13: (Concavity of the quantum conditional entropy) Let AB be a composite quantum system with components A and B. Then the conditional entropy $S(A \mid B)$ is concave in the state ρ^{AB} of AB.

Proof

Let d be the dimension of system A. Note that

$$S\left(\rho^{AB} \| \frac{I}{d} \otimes \rho^B\right) = -S(A,B) - \mathrm{tr}\left(\rho_{AB} \log\left(\frac{I}{d} \otimes \rho^B\right)\right) \tag{11.104}$$

$$= -S(A,B) - \mathrm{tr}\left(\rho^B \log \rho^B\right) + \log d \tag{11.105}$$

$$= -S(A \mid B) + \log d \tag{11.106}$$

Thus $S(A \mid B) = \log d - S\left(\rho^{AB} \| I/d \otimes \rho^B\right)$. The concavity of $S(A \mid B)$ follows from the joint convexity of the relative entropy. $\square$

Theorem 11.14: (Strong subadditivity) For any trio of quantum systems, A, B, C, the inequalities

$$S(A) + S(B) \leq S(A,C) + S(B,C) \tag{11.107}$$

$$S(A,B,C) + S(B) \leq S(A,B) + S(B,C) \tag{11.108}$$

hold.

Proof

The two inequalities are in fact equivalent. We will use concavity of the conditional entropy to prove the first, and then show that the second follows. Define a function $T\ (\ \rho^{ABC}\ )$ of density operators on the system ABC,

$$T\left(\rho^{ABC}\right) \equiv S(A) + S(B) - S(A,C) - S(B,C) = -S(C \mid A) - S(C \mid B) \tag{11.109}$$

From the concavity of the conditional entropy we see that $T\left(\rho^{ABC}\right)$ is a convex function of ρ^{ABC}. Let $\rho^{ABC} = \sum_i p_i |i\rangle\langle i|$ be a spectral decomposition of ρ^{ABC}. From the convexity of $T, T\left(\rho^{ABC}\right) \leq \sum_i p_i T(|i\rangle\langle i|)$. But $T(|i\rangle\langle i|) = 0$ as for a pure state $S(A,C) = S(B)$ and $S(B,C) = S(A)$. It follows that $T\left(\rho^{ABC}\right) \leq 0$, and thus

$$S(A) + S(B) - S(A,C) - S(B,C) \leq 0 \tag{11.110}$$

which is the first inequality we set out to prove.
To obtain the second inequality, introduce an auxiliary system R purifying the system ABC. Then using the just-proved inequality we have

$$S(R) + S(B) \leq S(R,C) + S(B,C) \tag{11.111}$$

Since $ABCR$ is a pure state, $S(R) = S(A,B,C)$ and $S(R,C) = S(A,B)$, so (11.111 becomes

$$S(A,B,C) + S(B) \leq S(A,B) + S(B,C), \tag{11.112}$$

as we set out to show. $\square$

Exercise 11.24: We obtained strong subadditivity as a consequence of the inequality $S(A) + S(B) \leq S(A,C) + S(B,C)$. Show that this inequality can be obtained as a consequence of strong subadditivity.

Exercise 11.25: We obtained strong subadditivity as a consequence of the concavity of the conditional information, $S(A \mid B)$. Show that the concavity of the conditional

entropy may be deduced from strong subadditivity. (Hint: You may need to introduce an auxiliary system into the problem.)

9.4.16 11.4.2 Strong subadditivity: elementary applications

Strong subadditivity and related results have many useful implications for quantum information theory. Let's take a look at a few of the elementary consequences of these results.

First, it is worth emphasizing how remarkable it is that the inequality $S(A) + S(B) \leq S(A,C)+S(B,C)$ holds. The corresponding inequality holds also for Shannon entropies, but for different reasons. For Shannon entropies it is true that $H(A) \leq H(A,C)$ and $H(B) \leq H(B,C)$, so the sum of the two inequalities must necessarily be true. In the quantum case, it is possible to have either $S(A) > S(A,C)$ or $S(B) > S(B,C)$, yet somehow Nature conspires in such a way that both of these possibilities are not true simultaneously, in order to ensure that the condition $S(A) + S(B) \leq S(A,C) + S(B,C)$ is always satisfied. Other ways of rephrasing this are in terms of conditional entropies and mutual informations,

$$0 \leq S(C \mid A) + S(C \mid B) \tag{11.113}$$

$$S(A:B) + S(A:C) \leq 2S(A) \tag{11.114}$$

both of which are also remarkable inequalities, for similar reasons. Note, however, that the inequality $0 \leq S(A \mid C) + S(B \mid C)$, which one might hope to be true based upon (11.114), is not, as can be seen by choosing ABC to be a product of a pure state for A with an EPR state for BC.

Exercise 11.26: Prove that $S(A:B) + S(A:C) \leq 2S(A)$. Note that the corresponding inequality for Shannon entropies holds since $H(A:B) \leq H(A)$. Find an example where $S(A:B) > S(A)$.

For practical applications strong subadditivity is often most easily applied by using a rephrasing in terms of the conditional or mutual informations. The following theorem lists three very simple reformulations of strong subadditivity that provide a powerful intuitive guide to the properties of quantum entropy.

Theorem 11.15:

(1) Conditioning reduces entropy: Suppose ABC is a composite quantum system. Then $S(A \mid B,C) \leq S(A \mid B)$.
(2) Discarding quantum systems never increases mutual information: Suppose ABC is a composite quantum system. Then $S(A:B) \leq S(A:B,C)$.
(3) Quantum operations never increase mutual information: Suppose AB is a composite quantum system and $\mathcal{E}$ is a trace-preserving quantum operation on system B. Let $S(A:B)$ denote the mutual information between systems A and B before $\mathcal{E}$ is applied to system B, and $S(A':B')$ the mutual information after $\mathcal{E}$ is applied to system B. Then $S(A':B') \leq S(A:B)$.

Proof

(1) The proof is the same as the classical proof (part of Theorem 11.3 on page 506), which we reproduce for convenience: $S(A \mid B,C) \leq S(A \mid B)$ is equivalent to $S(A,B,C) - S(B,C) \leq S(A,B) - S(B)$, which is equivalent to $S(A,B,C) + S(B) \leq S(A,B) + S(B,C)$, which is strong subadditivity.

(2) $S(A:B) \leq S(A:B,C)$ is equivalent to $S(A)+S(B)-S(A,B) \leq S(A)+S(B,C)-S(A,B,C)$, which is equivalent to $S(A,B,C)+S(B) \leq S(A,B)+S(B,C)$, which is strong subadditivity.
(3) By the constructions of Chapter 8 the action of $\mathcal{E}$ on B may be simulated by introducing a third system C, initially in a pure state $|0\rangle$, and a unitary interaction U between B and C. The action of $\mathcal{E}$ on B is equivalent to the action of U followed by discarding system C. Letting primes denote the state of the systems after U has acted we have $S(A:B) = S(A:B,C)$ because C starts out in a product state with AB, and clearly $S(A:B,C) = S(A':B',C')$. Discarding systems cannot increase mutual information, so $S(A':B') \leq S(A':B',C')$. Putting it all together gives $S(A':B') \leq S(A:B)$, as required. □

There is an interesting set of questions related to the subadditivity properties of quantum conditional entropies. We saw earlier that the Shannon mutual information is not subadditive, and thus the quantum mutual information is not subadditive either. What about the subadditivity of the conditional entropy? That is, is it true that

$$S(A_1,A_2 \mid B_1,B_2) \leq S(A_1 \mid B_1) + S(A_2 \mid B_2), \tag{11.115}$$

for any four quantum systems A_1, A_2, B_1 and B_2 ? It turns out that this inequality is correct. What's more, the conditional entropy is also subadditive in the first and second entries. Proving these facts is an instructive exercise in the application of strong subadditivity.

Theorem 11.16: (Subadditivity of the conditional entropy) Let $ABCD$ be a

composite of four quantum systems. Then the conditional entropy is jointly subadditive in the first and second entries:

$$S(A,B \mid C,D) \leq S(A \mid C) + S(B \mid D). \tag{11.116}$$

Let ABC be a composite of three quantum systems. Then the conditional entropy is subadditive in each of the first and second entries:

$$S(A,B \mid C) \leq S(A \mid C) + S(B \mid C) \tag{11.117}$$
$$S(A \mid B,C) \leq S(A \mid B) + S(A \mid C). \tag{11.118}$$

Proof

To prove joint subadditivity in both entries, note that by strong subadditivity

$$S(A,B,C,D) + S(C) \leq S(A,C) + S(B,C,D). \tag{11.119}$$

Adding $S(D)$ to each side of this inequality, we obtain

$$S(A,B,C,D) + S(C) + S(D) \leq S(A,C) + S(B,C,D) + S(D). \tag{11.120}$$

Applying strong subadditivity to the last two terms of the right hand side gives

$$S(A,B,C,D) + S(C) + S(D) \leq S(A,C) + S(B,D) + S(C,D) \tag{11.121}$$

Rearranging this inequality gives

$$S(A,B \mid C,D) \leq S(A \mid C) + S(B \mid D) \tag{11.122}$$

which is the joint subadditivity of the conditional entropy.
Subadditivity of the conditional entropy in the first entry, $S(A,B \mid C) \leq S(A \mid C) + S(B \mid C)$,

is trivially seen to be equivalent to strong subadditivity. Subadditivity in the second entry is slightly more challenging. We wish to show that $S(A \mid B,C) \leq S(A \mid B) + S(A \mid C)$. Note that this is equivalent to demonstrating the inequality

$$S(A,B,C) + S(B) + S(C) \leq S(A,B) + S(B,C) + S(A,C) \tag{11.123}$$

To prove this, note that at least one of the inequalities $S(C) \leq S(A,C)$ or $S(B) \leq S(A,B)$ must be true, as $S(A \mid B) + S(A \mid C) \geq 0$ by the first inequality in Theorem 11.14. Suppose $S(C) \leq S(A,C)$. Adding to this inequality the strong subadditivity inequality, $S(A,B,C) + S(B) \leq S(A,B) + S(B,C)$ gives the result. A similar proof holds in the case when $S(B) \leq S(A,B)$.

When we introduced the relative entropy it was described as being rather like a measure of distance between probability distributions or between density operators. Imagine that a quantum system consists of two parts, labeled A and B, and that we are given two density operators ρ^{AB} and σ^{AB}. In order to fulfil its distance-like promise, a very desirable property of $S(\cdot\|\cdot)$ is that it decrease when part of the system is ignored, that is:

$$S\left(\rho^A \| \sigma^A\right) \leq S\left(\rho^{AB} \| \sigma^{AB}\right) \tag{11.124}$$

This result is known as the monotonicity of the relative entropy. Intuitively this is a very reasonable property for a measure of distance to have; we expect that ignoring part of a physical system makes it harder to distinguish two states of that system (compare Section 9.2.1), and thus decrease any reasonable measure of distance between them.

Theorem 11.17: (Monotonicity of the relative entropy) Let ρ^{AB} and σ^{AB} be any two density matrices of a composite system AB. Then

$$S\left(\rho^A \| \sigma^A\right) \leq S\left(\rho^{AB} \| \sigma^{AB}\right) \tag{11.125}$$

Proof

Exercise 11.19 on page 517 implies that there exist unitary transformations U_j on the space B and probabilities p_j such that

$$\rho^A \otimes \frac{I}{d} = \sum_j p_j U_j \rho^{AB} U_j^\dagger \tag{11.126}$$

for all ρ^{AB}. From the convexity of the relative entropy we obtain

$$S\left(\rho^A \otimes \frac{I}{d} \| \sigma^A \otimes \frac{I}{d}\right) \leq \sum_j p_j S\left(U_j \rho^{AB} U_j^\dagger \| U_j \sigma^{AB} U_j^\dagger\right) \tag{11.127}$$

But the relative entropy is invariant under unitary conjugation, so this gives

$$S\left(\rho^A \otimes \frac{I}{d} \| \sigma^A \otimes \frac{I}{d}\right) \leq \sum_j p_j S\left(\rho^{AB} \| \sigma^{AB}\right) = S\left(\rho^{AB} \| \sigma^{AB}\right). \tag{11.128}$$

Combining this with the easily verified observation that

$$S\left(\rho^A \otimes \frac{I}{d} \| \sigma^A \otimes \frac{I}{d}\right) = S\left(\rho^A \| \sigma^A\right), \tag{11.129}$$

gives the monotonicity of the relative entropy. □

Problem 11.1: (Generalized Klein's inequality) Suppose $f(\cdot)$ is a convex function from real numbers to real numbers. Then f induces a natural function $f(\cdot)$ on Hermitian operators, as described in Section 2.1.8 on page 75. Prove that

$$\operatorname{tr}(f(A) - f(B)) \geq \operatorname{tr}\left((A - B)f'(B)\right). \tag{11.130}$$

Use this result to show that the relative entropy is non-negative.

Problem 11.2: (Generalized relative entropy) The definition of the relative entropy may be extended to apply to any two positive operators r and s,

$$S(r\|s) \equiv \operatorname{tr}(r \log r) - \operatorname{tr}(r \log s). \tag{11.131}$$

The earlier argument proving joint convexity of the relative entropy goes directly through for this generalized definition:

(1) For $\alpha, \beta > 0$ show that

$$S(\alpha r\|\beta s) = \alpha S(r\|s) + \alpha \operatorname{tr}(r) \log(\alpha/\beta). \tag{11.132}$$

(2) Prove that the joint convexity of the relative entropy implies the subadditivity of the relative entropy,

$$S\left(r_1 + r_2\|s_1 + s_2\right) \leq S\left(r_1\|s_1\right) + S\left(r_2\|s_2\right). \tag{11.133}$$

(3) Prove that subadditivity of the relative entropy implies joint convexity of the relative entropy.

(4) Let p_i and q_i be probability distributions over the same set of indices. Show that

$$S\left(\sum_i p_i r_i \| \sum_i q_i s_i\right) \leq \sum_i p_i S\left(r_i\|s_i\right) + \sum_i p_i \operatorname{tr}\left(r_i\right) \log\left(p_i/q_i\right). \tag{11.134}$$

In the case where the r_i are density operators so $\operatorname{tr}\left(r_i\right) = 1$, this reduces to the pretty formula

$$S\left(\sum_i p_i r_i \| \sum_i q_i s_i\right) \leq \sum_i p_i S\left(r_i\|s_i\right) + H\left(p_i\|q_i\right), \tag{11.135}$$

where $H(\cdot\|\cdot)$ is the Shannon relative entropy.

Problem 11.3: (Analogue of the triangle inequality for conditional entropy)

(1) Show that $H(X, Y \mid Z) \geq H(X \mid Z)$.

(2) Show that it is not always true that $S(A, B \mid C) \geq S(A \mid C)$.

(3) Prove the conditional version of the triangle inequality,

$$S(A, B \mid C) \geq S(A \mid C) - S(B \mid C) \tag{11.136}$$

Problem 11.4: (Conditional forms of strong subadditivity)

(1) Prove that $S(A, B, C \mid D) + S(B \mid D) \leq S(A, B \mid D) + S(B, C \mid D)$.

(2) Show by explicit example that it is not always true that $H(D \mid A, B, C) + H(D \mid B) \leq H(D \mid A, B) + H(D \mid B, C)$.

Problem 11.5: (Strong subadditivity - Research) Find a simple proof of the strong subadditivity inequality for quantum entropies.

9.4.17 Summary of Chapter 11: Entropy and information

- Fundamental measures of information arise as the answers to questions about the quantity of physical resources required to solve some information processing problem.
- Basic definitions:

(entropy)	$S(A) = -\operatorname{tr}\left(\rho^A \log \rho^A\right)$
(velative entropy)	$S(\rho\|\sigma) = -S(\rho) - \operatorname{tr}(\rho \log \sigma)$
(conditional entropy)	$S(A \mid B) = S(A,B) - S(B)$
(mutual information)	$S(A:B) = S(A) + S(B) - S(A,B)$

- Strong subadditivity: $S(A,B,C) + S(B) \leq S(A,B) + S(B,C)$. The other entropy inequalities we discussed are corollaries of this or the joint convexity of the relative entropy.
- The relative entropy is jointly convex in its arguments.
- The relative entropy is monotonic: $S\left(\rho^A\|\sigma^A\right) \leq S\left(\rho^{AB}\|\sigma^{AB}\right)$.

History and further reading

Historically, the concept of entropy first arose in the study of thermodynamics and statistical mechanics. But the modern information-theoretic foundation for the study of entropy came in Shannon's wonderful papers on information theory [*Sha*48]. A good general reference on properties of the Shannon entropy (and much else in information theory) are Chapters 2 and 16 of Cover and Thomas [CT91] . General references on the von Neumann entropy are the review article by Wehrl [Weh78], and the book by Ohya and Petz [OP93] .

The entropic uncertainty principle we prove is due to Deutsch [Deu83]. Many other people have worked on entropic uncertainty relations, and we just mention two other papers of interest. Kraus [Kra87] conjectured an entropic uncertainty relation strengthening Deutsch's for a particular class of measurements, and Maassen and Uffink [MU88] proved Kraus' conjecture. The relative entropy was introduced by Kullback and Leibler [KL 51], and its quantum generalization is due to Umegaki[Ume62]. Fannes' inequality appeared in [Fan73]. Klein's inequality was proved in [Kle31]. The triangle inequality is due to Araki
and Lieb [*AL*70]. Strong subadditivity has an interesting history. Robinson and Ruelle [*RR*67] first noted the importance of classical strong subadditivity for statistical physics. The quantum version was then conjectured in 1968 by Lanford and Robinson [LR68]. Obtaining a proof of the result was rather difficult however. Finally, in 1973 the theorem was proved in two papers: Lieb's eponymous theorem in [Lie73], while the surprising connection to strong subadditivity was developed in Lieb and Ruskai [LR73b]; see also [LR73a]. Lieb's theorem is a generalization of the Wigner-Yanase-Dyson conjecture made in 1963 by Wigner and Yanase [W463] and subsequently extended by Dyson (unpublished); prior to 1973 it was not known that the Wigner-Yanase-Dyson conjecture and strong subadditivity were related! See Wehr[[Weh78] for a discussion of the Wigner-Yanase-Dyson conjecture. The proof of Lieb's theorem we have given is due to Simon [Sim79], and is a variant of a proof by Uhlmann[Uhl77]. Other proofs of Lieb's theorem are also known. See for example, Epstein [Eps73], Ando [And79], and Petz [Pet86]. Subadditivity of the relative entropy in the first and second entries was proved by Lieb [Lie75]. Joint subadditivity of the quantum conditional entropy was proved by Nielsen [Nie98]. The monotonicity of the relative entropy was first noted by Lindblad [Lin75] . Problem 11.2 is due to Ruskai[Rus94].

9.5 12 Quantum information theory

Classical information theory is mostly concerned with the problem of sending classical information - letters in an alphabet, speech, strings of bits - over communications channels which operate in accordance with the laws of classical physics. How does the picture change if we can build quantum-mechanical communications channels? Can we transmit information more efficiently? Can we make use of quantum mechanics to transmit secret information without

being eavesdropped on? These are just two of the questions we may ask when communication channels are allowed to be quantum mechanical. This redefinition of what a channel is causes us to go back and re-examine the fundamental questions motivating classical information theory, in the search for new answers. This chapter surveys what is known about quantum information theory, including some surprising and intriguing possibilities made possible by quantum communication channels.

Quantum information theory is motivated by the study of communications channels, but it has a much wider domain of application, and it is a thought-provoking challenge to capture in a verbal nutshell the goals of the field. As described in Section 1.6, we can identify three fundamental goals uniting work on quantum information theory: to identify elementary classes of static resources in quantum mechanics (which we identify as types of 'information'); to identify elementary classes of dynamical processes in quantum mechanics (identified as types of 'information processing'); and to quantify resource tradeoffs incurred performing elementary dynamical processes. Quantum information theory is fundamentally richer than classical information theory, because quantum mechanics includes so many more elementary classes of static and dynamic resources - not only does it support all the familiar classical types, but there are entirely new classes such as the static resource of entanglement to make life even more interesting than it is classically.

The title of the chapter is 'Quantum information theory', and you may be forgiven for wondering how it is that we can hope to cover all aspects of quantum information theory in a single chapter. In fact, quantum information theory contains many facets other than those described here, including the study of quantum operations, the definition and study of fidelity measures, quantum error-correcting codes, and various notions of entropy all topics which we have described in detail in earlier chapters. The purpose of the present chapter is to describe quantum information theory in its 'purest' form; those other chapters are focused on developing specific tools, while we are concerned here with the grand sweep of things, with the most general statements one can make about the properties of quantum information.

We begin in Section 12.1 with a discussion of some of the unique properties of quantum states when compared to classical states, in the language of information theory. Not only are quantum states impossible to copy, generally, but also they cannot be perfectly distinguished! This is quantified by the Holevo bound. We then consider, in Section 12.2, an
elementary information-theoretic task, data compression, and show how quantum states can be compressed much as classical ones are. This is done by paralleling the theorem of typical sequences with the typical subspace theorem, to prove Schumacher's quantum noiseless channel coding theorem, the analogue of Shannon's noiseless channel coding theorem. A natural generalization of this problem is the capacity of a noisy channel for classical information, and in Section 12.3 we define and prove the analogue to Shannon's noisy channel coding theorem, known as the Holevo-Schumacher-Westmoreland theorem. The most difficult challenge is the capacity of a noisy quantum channel for quantum information. This is the subject of Section 12.4, in which the entropy exchange, the quantum Fano inequality, and the quantum data processing inequality are defined, but the open question of the capacity is left unresolved. Two applications of the noisy channel relations, the quantum Singleton bound, and the exorcism of Maxwell's demon, are presented, and the first half of this chapter is summarized. Two recurring themes throughout this exploration of quantum information are entanglement and non-orthogonality, and these subjects are the focus of the last two sections of the chapter. Section 12.5 describes how entanglement can be thought of as a physical resource, and explains how it can be transformed, distilled, and diluted. And finally, in Section 12.6, we present quantum cryptography, a provably secure means of communication whose success arises from the many properties of quantum information considered in this chapter.

9.5.1 12.1 Distinguishing quantum states and the accessible information

There is a simple game we can play to illustrate the remarkable differences between quantum and classical information. We will describe this game using two fictitious protagonists, Alice and Bob; of course the results can be rephrased in more abstract language, but the anthropocentric language makes the results easier to think (and write!) about.

Suppose Alice has a classical information source producing symbols $X = 0, \ldots, n$ according to a probability distribution $p_0, \ldots, p_n$. The aim of the game is for Bob to determine the value of X as best he can. To achieve this goal, Alice prepares a quantum state ρ_X chosen from some fixed set $\rho_0, \ldots, \rho_n$, and gives the state to Bob, who makes a quantum measurement on the state he has been given, and then tries to make the best guess he can as to the identity of X, based on his measurement result Y.

A good measure of how much information Bob has gained about X through the measurement is the mutual information $H(X : Y)$ between X and the measurement outcome Y, as defined in Chapter 11. By the data processing inequality we know that Bob can infer X from Y if and only if $H(X : Y) = H(X)$, and that in general $H(X : Y) \leq H(X)$; we will see later that the closeness of $H(X : Y)$ to $H(X)$ actually provides a quantitative measure of how well Bob can determine X. Bob's goal is to choose a measurement which maximizes $H(X : Y)$, bringing it as close as possible to $H(X)$. To this end, we define Bob's accessible information to be the maximum of the mutual information $H(X : Y)$ over all possible measurement schemes. The accessible information is a measure of how well Bob can do at inferring the state Alice prepared.

In classical information theory, the accessible information is not so interesting; while in practice it may be difficult to distinguish two classical states - consider the troubles we have reading bad handwriting - in principle it is always possible. In contrast, in quantum mechanics it is not always possible to distinguish distinct states, even in principle. For example, we saw in Box 2.3 on page 87 that there is no quantum mechanical procedure to
reliably distinguish two non-orthogonal quantum states. Stated in terms of accessible information, if Alice prepares the state $|\psi\rangle$ with probability p, and another, non-orthogonal state $|\varphi\rangle$ with probability $1 - p$, the accessible information of this preparation is strictly less than $H(p)$, as it is not possible for Bob to determine the identity of the state with full reliability. Classically, if Alice prepares one of two classical states - say a bit in the state 0 with probability p, or in the state 1 with probability $1 - p-$ then there is no fundamental reason of principle why Bob cannot distinguish between these two states, and thus the accessible information is the same as the entropy of preparation, $H(p)$.

There's an important caveat to this discussion, a context in which the concept of accessible information does make sense classically. The context is that of distinguishing probability distributions. Imagine that Alice prepares the state 0 or 1 according to one of two probability distributions, either $(p, 1 - p)$ or $(q, 1 - q)$. Given the state, Bob's goal is to identify which probability distribution Alice used to prepare the state. Clearly, it is not always possible for Bob to perform this identification with perfect reliability! Nevertheless, this example (analogous to the accessible information for a quantum system prepared in one of a set of mixed states) is of subsidiary importance. What is most important and remarkable is that the fundamental objects in quantum mechanics - the pure quantum states - enjoy distinguishability properties that are markedly different and much richer than the corresponding properties for the fundamental objects of classical information theory, such as ' 0 ' or ' 1 '.

The no-cloning theorem provides another perspective on the lack of accessibility suffered by quantum information in comparison to classical information. Classical information can, of course, be copied. This can be done exactly with digital information, like the multiply backed-up $\mathrm{AT_EX}$ file being used to generate this book, or approximately, as with the analog

images appearing on each page of this book, which have been copied by printing press prior to distribution. Surprisingly, the no-cloning theorem states that quantum mechanics does not allow unknown quantum states to be copied exactly, and places severe limitations on our ability to make approximate copies. The no-cloning theorem is proved in Box 12.1.

At first sight the no-cloning theorem appears rather peculiar. After all, isn't classical physics a special case of quantum mechanics? How is it possible that we can copy classical information if we can't copy quantum states? The answer is that the no-cloning theorem does not prevent all quantum states from being copied, it simply says that nonorthogonal quantum states cannot be copied. More precisely, suppose $|\psi\rangle$ and $|\varphi\rangle$ are two non-orthogonal quantum states. Then the no-cloning theorem implies that it is not possible to build a quantum device that, when input with $|\psi\rangle$ or $|\varphi\rangle$, will output two copies of the input state, $|\psi\rangle|\psi\rangle$ or $|\varphi\rangle|\varphi\rangle$. On the other hand, if $|\psi\rangle$ and $|\varphi\rangle$ are orthogonal, then the no-cloning theorem doesn't prohibit their cloning. Indeed, it is rather easy to design quantum circuits which copy such states! This observation resolves the apparent contradiction between the no-cloning theorem and the ability to copy classical information, for the different states of classical information can be thought of merely as orthogonal quantum states.

Exercise 12.1: Suppose $|\psi\rangle$ and $|\varphi\rangle$ are two orthogonal quantum states of a single qubit. Design a quantum circuit with two input qubits (the 'data' and the 'target' qubits), with the data qubit in either the state $|\psi\rangle$ or $|\varphi\rangle$, and the target qubit
prepared in the standard state $|0\rangle$, which produces as output $|\psi\rangle|\psi\rangle$ or $|\varphi\rangle|\varphi\rangle$, depending on whether $|\psi\rangle$ or $|\varphi\rangle$ was input to the data qubit.

What is the connection between cloning and accessible information? Suppose Alice prepares one of two non-orthogonal quantum states $|\psi\rangle$ and $|\varphi\rangle$ with respective probabilities p and $1-p$. Suppose it were the case that Bob's accessible information about these states was $H(p)$, that is, the laws of quantum mechanics allowed Bob to obtain enough information by measurement to identify which of the two states $|\psi\rangle$ and $|\varphi\rangle$ Alice had prepared. Then Bob could clone the states in a very simple manner: he would perform a measurement to determine which of $|\psi\rangle$ and $|\varphi\rangle$ had been prepared by Alice, and once he had made the identification, could prepare at will multiple copies of whichever state $|\psi\rangle$ or $|\varphi\rangle$ Alice had given him. Thus, the no-cloning theorem can be seen as a consequence of the fact that the accessible information for these states is strictly less than $H(p)$. It's also possible to turn this perspective around, and view the fact that the accessible information is less than $H(p)$ as a consequence of the no-cloning theorem! This is done as follows. Imagine that it is possible to clone non-orthogonal states. After receiving the state $|\psi\rangle$ or $|\varphi\rangle$ from Alice, Bob could repeatedly apply such a cloning device to obtain the state $|\psi\rangle^{\otimes n}$ or $|\varphi\rangle^{\otimes n}$. In the limit of large n these two states become very nearly orthogonal and it is possible to distinguish them with arbitrarily high reliability by a projective measurement. That is, if it were possible to clone then Bob could identify with arbitrarily high probability of success whether the state $|\psi\rangle$ or $|\varphi\rangle$ had been prepared, and thus the accessible information would be $H(p)$. We can therefore view the no-cloning theorem as being equivalent to the statement than in quantum mechanics the accessible information for non-orthogonal states is in general less than the entropy of preparation.

As we have emphasized throughout the book, the hidden nature of quantum information lies at the heart of the power of quantum computation and quantum information, and the accessible information captures in a quantitative way this hidden nature of quantum information. Unfortunately, no general method for calculating the accessible information is known; however, a variety of important bounds can be proved, the most important of which is the Holevo bound.

9.5.2 12.1.1 The Holevo bound

The Holevo bound is an exceedingly useful upper bound on the accessible information that plays an important role in many applications of quantum information theory.

Theorem 12.1: (The Holevo bound) Suppose Alice prepares a state ρ_X where $X = 0, \ldots, n$ with probabilities $p_0, \ldots, p_n$. Bob performs a measurement described by POVM elements $\{E_y\} = \{E_0, \ldots, E_m\}$ on that state, with measurement outcome Y. The Holevo bound states that for any such measurement Bob may do:

$$H(X:Y) \leq S(\rho) - \sum_x p_x S(\rho_x) \tag{12.6}$$

where $\rho = \sum_x p_x \rho_x$.

The Holevo bound is thus an upper bound on the accessible information. The quantity appearing on the right hand side of the Holevo bound is so useful in quantum information theory that it is given a name, the Holevo χ quantity, and is sometimes denoted χ.

Box 12.1: The no-cloning theorem

Is it possible to make a copy of an unknown quantum state? Surprisingly, it turns out that the answer to this question is no. In this box we describe an elementary proof of this fact that captures the essential reason this is not possible.

Suppose we have a quantum machine with two slots labeled A and B. Slot A, the data slot, starts out in an unknown but pure quantum state, $|\psi\rangle$. This is the state which is to be copied into slot B, the target slot. We assume that the target slot starts out in some standard pure state, $|s\rangle$. Thus the initial state of the copying machine is

$$|\psi\rangle \otimes |s\rangle. \tag{12.1}$$

Some unitary evolution U now effects the copying procedure, ideally,

$$|\psi\rangle \otimes |s\rangle \stackrel{U}{\rightarrow} U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle. \tag{12.2}$$

Suppose this copying procedure works for two particular pure states, $|\psi\rangle$ and $|\varphi\rangle$. Then we have

$$U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle \tag{12.3}$$
$$U(|\varphi\rangle \otimes |s\rangle) = |\varphi\rangle \otimes |\varphi\rangle. \tag{12.4}$$

Taking the inner product of these two equations gives

$$\langle \psi \mid \varphi \rangle = (\langle \psi \mid \varphi \rangle)^2. \tag{12.5}$$

But $x = x^2$ has only two solutions, $x = 0$ and $x = 1$, so either $|\psi\rangle = |\varphi\rangle$ or $|\psi\rangle$ and $|\varphi\rangle$ are orthogonal. Thus a cloning device can only clone states which are orthogonal to one another, and therefore a general quantum cloning device is impossible. A potential quantum cloner cannot, for example, clone the qubit states $|\psi\rangle = |0\rangle$ and $|\varphi\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, since these states are not orthogonal.

What we have shown is that it is impossible to perfectly clone an unknown quantum state using unitary evolution. Several questions naturally arise: what if we try to copy a mixed state? What if we allow cloning devices that are not unitary? What if we are willing to allow imperfect copies that nevertheless are 'good' according to some interesting measure of fidelity? These are all good questions which have been the subject of much investigation, as

can be seen from the end of chapter 'History and further reading.' The short summary of this work is that even if one allows non-unitary cloning devices, the cloning of non-orthogonal pure states remains impossible unless one is willing to tolerate a finite loss of fidelity in the copied states. Similar conclusions hold also for mixed states, although a somewhat more sophisticated approach is necessary to even define what is meant by the notion of cloning a mixed state.

Proof

The proof of the Holevo bound is via a simple and beautiful construction involving three quantum systems, which we label P, Q and M. The system Q is the quantum system Alice gives to Bob; P and M are fictitious auxiliary systems introduced to ease the proof,
just as was done in proving many of the entropic inequalities in Chapter 11. Intuitively, P may be thought of as the 'preparation' system. By definition it has an orthonormal basis $|x\rangle$ whose elements correspond to the labels $0, \ldots, n$ on the possible preparations for the quantum system, $Q.M$ can be thought of intuitively as Bob's 'measuring device', and it has a basis $|y\rangle$ whose elements correspond to the possible outcomes $1, \ldots, n$ of Bob's measurement. The initial state of the total system is assumed to be

$$\rho^{PQM} = \sum_x p_x |x\rangle\langle x| \otimes \rho_x \otimes |0\rangle\langle 0|, \tag{12.7}$$

where we write the tensor product decomposition in the order PQM. Intuitively, this state represents the situation that Alice has chosen a value of x with probability p_x, prepared a corresponding ρ_x and given it to Bob, who is about to use his measuring apparatus, initially in the standard state $|0\rangle$, to perform the measurement. To describe the measurement we introduce a quantum operation $\mathcal{E}$ acting on the systems Q and M only (not P), whose action is to perform a measurement with POVM elements $\{E_y\}$ on the system Q, and to store the result of the measurement in system M :

$$\mathcal{E}(\sigma \otimes |0\rangle\langle 0|) \equiv \sum_y \sqrt{E_y}\sigma\sqrt{E_y} \otimes |y\rangle\langle y|, \tag{12.8}$$

where σ is any state of system Q, and $|0\rangle$ is the initial state of the measuring apparatus. In the following exercise you show that $\mathcal{E}$ is a trace-preserving quantum operation.

Exercise 12.2: Define U_y to be the unitary operator acting on system M whose action on a basis is $U_y |y'\rangle \equiv |y' + y\rangle$, where the addition is done modulo $n+1$. Show that $\left\{\sqrt{E_y} \otimes U_y\right\}$ is a set of operation elements defining a trace-preserving quantum operation $\mathcal{E}$ whose action on states of the form $\sigma \otimes |0\rangle\langle 0|$ agrees with (12.8).

The proof of Holevo's bound now proceeds as follows. Using primes to denote states of PQM after application of $\mathcal{E}$, and unprimed states to indicate the time prior to application of $\mathcal{E}$ we have $S(P : Q) = S(P : Q, M)$, since M is initially uncorrelated with P and Q, and $S(P : Q, M) \geq S(P' : Q', M')$, since applying the quantum operation $\mathcal{E}$ to QM can't increase the mutual information between P and QM (Theorem 11.15 on page 522), and finally $S(P' : Q', M') \geq S(P' : M')$, since discarding systems can't increase mutual information (also Theorem 11.15). Putting these results together gives

$$S(P' : M') \leq S(P : Q) \tag{12.9}$$

This result, with a little simple algebra, is easily understood to be the Holevo bound! Let's first calculate the quantity on the right hand side. Note that

$$\rho^{PQ} = \sum_x p_x |x\rangle\langle x| \otimes \rho_x, \tag{12.10}$$

from which it follows that $S(P) = H(p_x), S(Q) = S(\rho)$, and $S(P,Q) = H(p_x) + \sum_x p_x S(\rho_x)$ (by Theorem 11.10 on page 518), whence

$$S(P:Q) = S(P) + S(Q) - S(P,Q) = S(\rho) - \sum_x p_x S(\rho_x) \tag{12.11}$$

which is exactly what we want on the right hand side of the Holevo bound! To calculate the quantity on the left hand side of (12.9), note that

$$\rho^{P'Q'M'} = \sum_{xy} p_x |x\rangle\langle x| \otimes \sqrt{E_y}\rho_x\sqrt{E_y} \otimes |y\rangle\langle y|. \tag{12.12}$$

Tracing out system Q' and using the observation that the joint distribution $p(x,y)$ for the pair (X,Y) satisfies $p(x,y) = p_x p(y \mid x) = p_x \operatorname{tr}(\rho_x E_y) = p_x \operatorname{tr}\left(\sqrt{E_y}\rho_x\sqrt{E_y}\right)$, gives

$$\rho^{P'M'} = \sum_{xy} p(x,y)|x\rangle\langle x| \otimes |y\rangle\langle y|, \tag{12.13}$$

whence $S(P':M') = H(X:Y)$, which is exactly what we want on the left hand side of the Holevo bound! This completes the proof of the Holevo bound.

9.5.3 12.1.2 Example applications of the Holevo bound

The Holevo bound is a keystone in the proof of many results in quantum information theory. For now, we'll give just a taste of how this important result may be applied. Recall Theorem 11.10, which implies that

$$S(\rho) - \sum_x p_x S(\rho_x) \leq H(X) \tag{12.14}$$

with equality if and only if the states ρ_x have orthogonal support. Suppose that the states ρ_x do not have orthogonal support, so the inequality in (12.14) is strict. Then the Holevo bound implies that $H(X:Y)$ is strictly less than $H(X)$, and thus it is impossible for Bob to determine X with perfect reliability based on his measurement result Y, which generalizes our existing understanding that if the states prepared by Alice are not orthogonal then it is not possible for Bob to determine with certainty which state Alice prepared.

A concrete example involves Alice preparing a single qubit in one of two quantum states according to the outcome of a fair coin toss. If the coin toss yields heads, then Alice prepares the state $|0\rangle$, and if the coin toss yields tails, then Alice prepares the state $\cos\theta|0\rangle + \sin\theta|1\rangle$, where θ is some real parameter. In the $|0\rangle, |1\rangle$ basis it follows that ρ may be written

$$\rho = \frac{1}{2}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \frac{1}{2}\begin{bmatrix} \cos^2\theta & \cos\theta\sin\theta \\ \cos\theta\sin\theta & \sin^2\theta \end{bmatrix}. \tag{12.15}$$

A simple calculation shows that the eigenvalues of ρ are $(1 \pm \cos\theta)/2$, and the Holevo bound is therefore given by the binary entropy $H((1+\cos\theta)/2)$, as illustrated in Figure 12.1. Notice that the Holevo bound is maximized when $\theta = \pi/2$, attaining a value of 1 bit, corresponding to the case of Alice preparing states chosen from an orthogonal set, at which point it is possible for Bob to determine with surety which state Alice prepared. For other values of θ the Holevo bound is strictly less than 1 bit, and it is impossible for Bob to determine with surety which state Alice prepared.

The Holevo bound may be given more operational meaning by making use of the Fano inequality (see Box 12.2 on page 536 for a derivation). Suppose Bob makes a guess $\tilde{X} = f(Y)$ as to which state Alice prepared, based on the outcome of his measurement Y and some rule

for making a guess, encapsulated in the function $f(\cdot)$. Then according to the Fano inequality and the Holevo bound,

$$H(p(\tilde{X} \neq X)) + p(\tilde{X} \neq X) \log(|X| - 1) \geq H(X \mid Y)$$

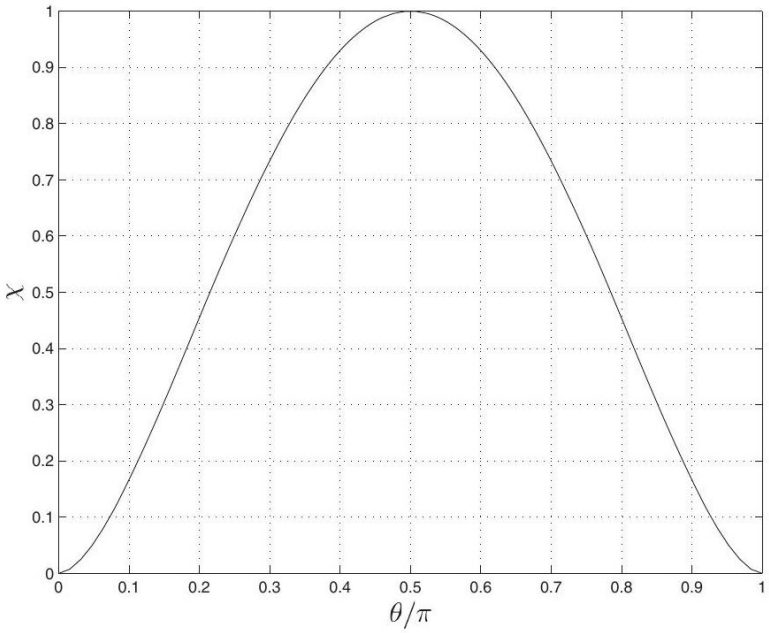


Figure 12.1. Plot of the Holevo bound χ as a function of θ when the states $|0\rangle$ and $\cos\theta|0\rangle + \sin\theta|1\rangle$ are prepared with equal probability. Notice that the Holevo bound reaches a maximum when $\theta = \pi/2$, corresponding to orthogonal states. It is only at this point that it is possible for Bob to determine with certainty which state Alice prepared.

$$\begin{aligned} &= H(X) - H(X:Y) \\ &\geq H(X) - \chi \end{aligned} \tag{12.19}$$

which allows us to place bounds on how well Bob may infer the value of X. Heuristically, the smaller χ is, the harder it is for Bob to determine which state Alice prepared. This is illustrated in Figure 12.2 for the case where Alice prepares $|0\rangle$ with probability onehalf and $\cos\theta|0\rangle + \sin\theta|1\rangle$ with probability one-half, for which the bound reduces to $H(p(\tilde{X} \neq X)) \geq 1 - \chi$ and $\chi = H((1 + \cos(\theta))/2)$ as we noted before. Notice that when $\theta \neq \pi/2$, Bob has some finite probability of making an error in his guess. This error gets larger as θ gets closer to zero. Finally, when $\theta = 0$ and the two states are indistinguishable, the lower bound tells us that Bob's probability of error is at least one-half - he can do no better than chance in guessing which state Alice prepared, as we would expect.

Exercise 12.3: Use the Holevo bound to argue that n qubits can not be used to transmit more than n bits of classical information.

Exercise 12.4: Suppose Alice sends Bob an equal mixture of the four pure states

$$|X_1\rangle = |0\rangle \tag{12.20}$$

$$|X_2\rangle = \sqrt{\frac{1}{3}}[|0\rangle + \sqrt{2}|1\rangle] \tag{12.21}$$

$$|X_3\rangle = \sqrt{\frac{1}{3}}\left[|0\rangle + \sqrt{2}e^{2\pi i/3}|1\rangle\right] \tag{12.22}$$

$$|X_4\rangle = \sqrt{\frac{1}{3}}\left[|0\rangle + \sqrt{2}e^{4\pi i/3}|1\rangle\right]. \tag{12.23}$$

Box 12.2: Fano's inequality

Suppose we wish to infer the value of a random variable X based on knowledge of another random variable Y. Intuitively, we expect that the conditional entropy $H(X \mid Y)$ limits how well we may perform this inference. The Fano inequality makes this intuition rigorous, and provides a useful bound on how well we may infer X, given Y.
Suppose $\tilde{X} \equiv f(Y)$ is some function of Y which we are using as our best guess for X. Let $p_e \equiv p(X \neq \tilde{X})$ be the probability that this guess is incorrect. Then the Fano inequality states that

$$H(p_e) + p_e \log(|X| - 1) \geq H(X \mid Y) \tag{12.16}$$

where $H(\cdot)$ is the binary entropy and $|X|$ is the number of values X may assume. Qualitatively, what the inequality tells us is that if $H(X \mid Y)$ is large (that is, comparable in size to $\log(|X| - 1)$) then the probability p_e of making an error in inference must also be large.
To prove the Fano inequality, define an 'error' random variable, $E \equiv 1$ if $X \neq \tilde{X}$, and $E \equiv 0$ if $X = \tilde{X}$. Notice that $H(E) = H(p_e)$. Using the chaining rule for conditional entropies (page 508), we have $H(E, X \mid Y) = H(E \mid X, Y) + H(X \mid Y)$. But E is completely determined once X and Y are known, so $H(E \mid X, Y) = 0$ and thus $H(E, X \mid Y) = H(X \mid Y)$. Applying the chain rule for entropies again but to different variables, we obtain $H(E, X \mid Y) = H(X \mid E, Y) + H(E \mid Y)$. Conditioning reduces entropy, so $H(E \mid Y) \leq H(E) = H(p_e)$, whence $H(X \mid Y) = H(E, X \mid Y) \leq H(X \mid E, Y) + H(p_e)$. The proof of the Fano inequality is concluded by bounding $H(X \mid E, Y)$ as follows (we have omitted a few simple algebraic details, which you can easily fill in):

$$H(X \mid E, Y) = p(E = 0)H(X \mid E = 0, Y) + p(E = 1)H(X \mid E = 1, Y)(\tag{12.17}$$

$$\leq p(E = 0) \times 0 + p_e \log(|X| - 1) = p_e \log(|X| - 1) \tag{12.18}$$

where $H(X \mid E = 1, Y) \leq \log(|X| - 1)$ follows from the fact that when $E = 1$, $X \neq Y$, and X can assume at most $|X| - 1$ values, bounding its entropy, and thus its conditional entropy by $\log(|X| - 1)$. Substituting $H(X \mid E, Y) \leq p_e \log(|X| - 1)$ into $H(X \mid Y) \leq H(X \mid E, Y) + H(p_e)$ gives the Fano inequality $H(X \mid Y) \leq H(p_e) + p_e \log(|X| - 1)$.

> Show that the maximum mutual information between Bob's measurement and Alice's transmission is less than one bit. A POVM which achieves ≈ 0.415 bits is known. Can you construct this or, better yet, one which achieves the Holevo bound?

9.5.4 12.2 Data compression

Let's switch tacks now and investigate an elementary dynamical process - data compression - which arises in both classical and quantum information theory. In its most general form the problem of data compression is to determine what are the minimal

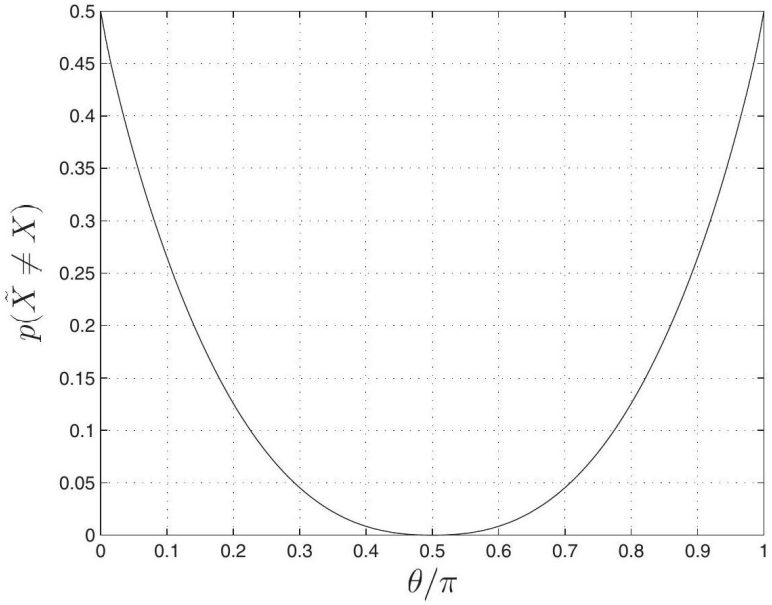


Figure 12.2. A lower bound on the probability of Bob making an error in inferring whether Alice prepared the state $|0\rangle$ or $\cos\theta|0\rangle + \sin\theta|1\rangle$. This lower bound is obtained by combining Fano's inequality with the Holevo bound. Observe that the bound decreases to zero as θ gets close to $\pi/2$, where the states may be reliably distinguished.

physical requirements needed to store an information source? It is one of the fundamental problems of information theory, with implications far beyond its immediate scope. In both classical and quantum information theory the techniques utilized in solving this problem turn out to have a far wider range of applicability than mere data compression, yet receive perhaps their simplest and most elegant expression in the solution of the data compression problem. In this section we examine in detail both quantum and classical data compression.

9.5.5 12.2.1 Shannon's noiseless channel coding theorem

Shannon's noiseless channel coding theorem quantifies the extent to which we can compress the information being produced by a classical information source. What do we mean by a classical information source? Many models of such a source are possible. A simple and very fruitful model is that a source consists of a sequence of random variables $X_1, X_2, \ldots$ whose values represent the output of the source. We will find it convenient to assume that the random variables take values from a finite alphabet of symbols, although extensions to infinite alphabets also hold. Furthermore, we assume that the different uses of the source are independent and identically distributed; that is, the source is what is known as an i.i.d information source. In the real world sources often don't behave in this way. It is easy to see, for example, that the letters in the English text in front of you don't occur in an independent fashion; strong correlations exist between the letters. To take a simple example the letter ' t ' is followed by the letter ' h ' more frequently than one would expect based upon the overall frequency of the letter 'h' in normal English text; we say
that occurrences of ' t ' and ' h ' do not occur independently, but are correlated. Nevertheless, for a wide variety of information sources (including English text) the assumption of an i.i.d. source works pretty well in practice, and the ideas introduced to deal with the special case of an i.i.d. source can be generalized to more sophisticated sources.

Before we get into the technical details of Shannon's theorem, let's use a simple example to understand the intuition behind the result. Suppose an i.i.d. information source is producing

bits $X_1, X_2, X_3, \ldots$, each being equal to zero with probability p, and equal to one with probability $1-p$. The key idea behind Shannon's theorem is to divide the possible sequences of values $x_1, \ldots, x_n$ for the random variables $X_1, \ldots, X_n$ up into two types - sequences which are highly likely to occur, known as typical sequences, and sequences which occur rarely, known as atypical sequences. How is this done? As n gets large, we expect that with high probability a fraction p of the symbols output from the source will be equal to zero, and that a fraction $1-p$ will be equal to one. The sequences $x_1, \ldots, x_n$ for which this assumption is correct are known as typical sequences. Combining this definition with the independence assumption for the source gives

$$p(x_1, \ldots, x_n) = p(x_1)\, p(x_2) \ldots p(x_n) \approx p^{np}(1-p)^{(1-p)n} \tag{12.24}$$

for typical sequences. Taking logarithms on both sides gives

$$-\log p(x_1, \ldots, x_n) \approx -np \log p - n(1-p)\log(1-p) = nH(X), \tag{12.25}$$

where X is a random variable distributed according to the source distribution and $H(X) = -p\log(p) - (1-p)\log(1-p)$ is the entropy of the source distribution, also known as the entropy rate of the source. Thus $p(x_1, \ldots, x_n) \approx 2^{-nH(X)}$, from which we see that there can be at most $2^{nH(X)}$ typical sequences, since the total probability of all typical sequences cannot be greater than one.

We now have the tools to understand a simple scheme for data compression. Suppose the output from the source is $x_1, \ldots, x_n$. To compress this output, we check to see whether $x_1, \ldots, x_n$ is a typical sequence. If it's not, we give up - declare an error. Fortunately, as n becomes large this happens very rarely, since nearly all sequences are typical in the limit of large n. If the output is a typical sequence, we record that fact. Since there are at most $2^{nH(X)}$ typical sequences, it only requires $nH(X)$ bits to uniquely identify a particular typical sequence. We choose some such scheme for identification, and compress the output from the source to the corresponding string of $nH(X)$ bits describing which typical sequence occurred, which can later be decompressed. As n becomes large this scheme succeeds with probability approaching one.

Several criticisms can be made of this scheme: (a) It has a small but finite chance of failing. Slightly more sophisticated schemes make use of similar ideas to remove the possibility of an error occurring. (b) To do the compression we have to wait until the source has emitted a large number, n, of symbols. Again, adaptations exist which allow the processing to be done as the symbols are emitted by the source. (c) No explicit scheme mapping outputs from the source to the compressed sequences has been given. Once again, slightly more sophisticated schemes can be developed which address this issue. (d) The exact procedure being used to do the data compression depends on the output distribution of the source. What if this is not known? Clever universal compression algorithms exist which can cope with this possibility. The reader who is interested in
these and other issues is referred to the book of Cover and Thomas listed in the end of chapter 'History and further reading'.

Let's generalize the notion of typical sequences beyond the binary case. Suppose $X_1, X_2, \ldots$ is an i.i.d. information source. Typically, the frequency of occurrence of any given letter x in the sequence output from the source will be close to the probability $p(x)$ of that letter occurring on any given use of the source. With this intuitive understanding in mind we make the following rigorous definition of the notion of a typical sequence. Given $\epsilon > 0$ we say that a string of source symbols $x_1 x_2 \ldots x_n$ is ϵ-typical if

$$2^{-n(H(X)+\epsilon)} \leq p(x_1, \ldots, x_n) \leq 2^{-n(H(X)-\epsilon)} \tag{12.26}$$

and denote the set of all such ϵ-typical sequences of length n by $T(n,\epsilon)$. A useful equivalent reformulation of the definition is as

$$\left|\frac{1}{n}\log\frac{1}{p\left(x_1,\ldots,x_n\right)}-H(X)\right|\leq\epsilon \tag{12.27}$$

Using the law of large numbers (stated and proved in Box 12.3 on page 541) we can prove the theorem of typical sequences, which makes rigorous the idea that in the limit of large n most sequences output by an information source are typical.

Theorem 12.2: (Theorem of typical sequences)

(1) Fix $\epsilon>0$. Then for any $\delta>0$, for sufficiently large n, the probability that a sequence is ϵ-typical is at least $1-\delta$.
(2) For any fixed $\epsilon>0$ and $\delta>0$, for sufficiently large n, the number $|T(n,\epsilon)|$ of ϵ-typical sequences satisfies

$$(1-\delta)2^{n(H(X)-\epsilon)}\leq|T(n,\epsilon)|\leq 2^{n(H(X)+\epsilon)} \tag{12.28}$$

(3) Let $S(n)$ be a collection of size at most 2^{nR}, of length n sequences from the source, where $R<H(X)$ is fixed. Then for any $\delta>0$ and for sufficiently large n,

$$\sum_{x\in S(n)}p(x)\leq\delta \tag{12.29}$$

Proof

Part 1: A direct application of the law of large numbers. Notice that $-\log p\left(X_i\right)$ are independent, identically distributed random variables. By the law of large numbers for any $\epsilon>0$ and $\delta>0$ for sufficiently large n we have

$$p\left(\left|\sum_{i=1}^{n}\frac{-\log p\left(X_i\right)}{n}-\mathbf{E}(-\log p(X))\right|\leq\epsilon\right)\geq 1-\delta \tag{12.30}$$

But $\mathbf{E}(\log p(X))=-H(X)$ and $\sum_{i=1}^{n}\log p\left(X_i\right)=\log\left(p\left(X_1,\ldots,X_n\right)\right)$. Thus

$$p\left(\left|-\log\left(p\left(X_1,\ldots,X_n\right)\right)/n-H(X)\right|\leq\epsilon\right)\geq 1-\delta \tag{12.31}$$

That is, the probability that a sequence is ϵ-typical is at least $1-\delta$.
Part 2: Follows from the definition of typicality, and the observation that the sum of the probabilities of the typical sequences must lie in the range $1-\delta$ (by part 1) to 1 (as probabilities cannot sum to more than 1). Thus

$$1\geq\sum_{x\in T(n,\epsilon)}p(x)\geq\sum_{x\in T(n,\epsilon)}2^{-n(H(X)+\epsilon)}=|T(n,\epsilon)|2^{-n(H(X)+\epsilon)} \tag{12.32}$$

from which we deduce $|T(n,\epsilon)|\leq 2^{n(H(X)+\epsilon)}$, and

$$1-\delta\leq\sum_{x\in T(n,\epsilon)}p(x)\leq\sum_{x\in T(n,\epsilon)}2^{-n(H(X)-\epsilon)}=|T(n,\epsilon)|2^{-n(H(X)-\epsilon)} \tag{12.33}$$

from which we deduce $|T(n,\epsilon)|\geq(1-\delta)2^{n(H(X)-\epsilon)}$.
Part 3: The idea is to split the sequences in $S(n)$ up into typical and atypical sequences. The atypical sequences have small probability in the large n limit. The number of typical sequences

in $S(n)$ is obviously no larger than the total number of sequences in $S(n)$, which is at most 2^{nR}, and each typical sequence has probability about $2^{-nH(X)}$ so the total probability of the typical sequences in $S(n)$ scales like $2^{n(R-H(X))}$, which goes to zero when $R < H(X)$.

More rigorously, choose ϵ so $R < H(X) - \delta$ and $0 < \epsilon < \delta/2$. Split the sequences in $S(n)$ up into the ϵ-typical sequences, and the ϵ-atypical sequences. By part 1 , for n sufficiently large the total probability of the atypical sequences can be made less than $\delta/2$. There are at most 2^{nR} typical sequences in $S(n)$, each with probability at most $2^{-n(H(X)-\epsilon)}$, so the probability of the typical sequences is at most $2^{-n(H(X)-\epsilon-R)}$, which goes to zero as n goes to infinity. Thus the total probability of the sequences in $S(n)$ is less than δ for n sufficiently large.

Shannon's noiseless channel coding theorem is an easy application of the theorem of typical sequences. We give here a very simple version of the noiseless channel coding theorem; more sophisticated versions are left to the exercises and the end of chapter 'History and further reading'. The basic setting is to suppose that $X_1, X_2, \ldots$ is an i.i.d. classical information source over some finite alphabet containing d symbols. A compression scheme of rate R maps possible sequences $x = (x_1, \ldots, x_n)$ to a bit string of length nR which we denote by $C^n(x) = C^n(x_1, \ldots, x_n)$. (Note that nR may not be an integer; our notation is simplified by agreeing that in this case $nR = \lfloor nR \rfloor$.) The matching decompression scheme takes the nR compressed bits and maps them back to a string of n letters from the alphabet, $D^n(C^n(x))$. A compression-decompression scheme (C^n, D^n) is said to be reliable if the probability that $D^n(C^n(x)) = x$ approaches one as n approaches ∞. Shannon's noiseless channel coding theorem specifies for what values of the rate R a reliable compression scheme exists, revealing a remarkable operational interpretation for the entropy rate $H(X)$: it is just the minimal physical resources necessary and sufficient to reliably store the output from the source.

Theorem 12.4: (Shannon's noiseless channel coding theorem) Suppose $\{X_i\}$ is an i.i.d. information source with entropy rate $H(X)$. Suppose $R > H(X)$. Then there exists a reliable compression scheme of rate R for the source. Conversely, if $R < H(X)$ then any compression scheme will not be reliable.

Proof

Suppose $R > H(X)$. Choose $\epsilon > 0$ such that $H(X) + \epsilon < R$. Consider the set $T(n, \epsilon)$

Box 12.3: The law of large numbers

Suppose we repeat an experiment a large number of times, each time measuring the value of some parameter, X. We label the results of the experiments $X_1, X_2, \ldots$ Assuming that the results of the experiments are independent, we intuitively expect that the value of the estimator $S_n \equiv \sum_{i=1}^n X_i/n$ of the average $\mathbf{E}(X)$, should approach $\mathbf{E}(X)$ as $n \rightarrow \infty$. The law of large numbers is a rigorous statement of this intuition.

Theorem 12.3: (Law of large numbers) Suppose $X_1, X_2, \ldots$ are independent random variables all having the same distribution as a random variable X with finite first and second moments, $|\mathbf{E}(X)| < \infty$ and $\mathbf{E}(X^2) < \infty$. Then for any $\epsilon > 0, p(|S_n - \mathbf{E}(X)| > \epsilon) \rightarrow 0$ as $n \rightarrow \infty$.

Proof

To begin we assume that $\mathbf{E}(X) = 0$ and discuss what happens when $\mathbf{E}(X) \neq 0$ upon completion of the proof. Since the random variables are independent with mean zero, it follows that $\mathbf{E}(X_i X_j) = \mathbf{E}(X_i)\mathbf{E}(X_j) = 0$ when $i \neq j$, and thus

$$\mathbf{E}\left(S_n^2\right) = \frac{\sum_{i,j=1}^n \mathbf{E}(X_i X_j)}{n^2} = \frac{\sum_{i=1}^n \mathbf{E}(X_i^2)}{n^2} = \frac{\mathbf{E}(X^2)}{n}, \tag{12.34}$$

where the final equality follows from the fact that $X_1, \ldots, X_n$ are identically distributed to X. By the same token, from the definition of the expectation we have

$$\mathbf{E}\left(S_n^2\right) = \int dP S_n^2 \tag{12.35}$$

where dP is the underlying probability measure. It is clear that either $|S_n| \leq \epsilon$ or $|S_n| > \epsilon$, so we can split this integral into two pieces, and then drop one of these pieces with the justification that it is non-negative,

$$\mathbf{E}\left(S_n^2\right) = \int_{|S_n| \leq \epsilon} dP S_n^2 + \int_{|S_n| > \epsilon} dP S_n^2 \geq \int_{|S_n| > \epsilon} dP S_n^2 \tag{12.36}$$

In the region of integration $S_n^2 > \epsilon^2$, and thus

$$\mathbf{E}\left(S_n^2\right) \geq \epsilon^2 \int_{|S_n| > \epsilon} dP = \epsilon^2 p\left(|S_n| > \epsilon\right) \tag{12.37}$$

Comparing this inequality with (12.34) we see that

$$p\left(|S_n| > \epsilon\right) \leq \frac{\mathbf{E}\left(X^2\right)}{n\epsilon^2} \tag{12.38}$$

Letting $n \to \infty$ completes the proof. In the case when $\mathbf{E}(X) \neq 0$, it is easy to obtain the result, by defining

$$Y_i \equiv X_i - \mathbf{E}(X), \quad Y \equiv X - \mathbf{E}(X) \tag{12.39}$$

Y and $Y_1, Y_2, \ldots$ are a sequence of independent, identically distributed random variables with $\mathbf{E}(Y) = 0$ and $\mathbf{E}\left(Y^2\right) < \infty$. The result follows from the earlier reasoning.
of ϵ-typical sequences. For any $\delta > 0$ and for sufficiently large n, there are at most $2^{n(H(x)+\epsilon)} < 2^{nR}$ such sequences, and the probability of the source producing such a sequence is at least $1 - \delta$. The method of compression therefore is simply to examine the output of the source to see if it is ϵ-typical. If it is not, then compress to some fixed nR bit string which indicates failure; the decompression operation simply outputs a random sequence $x_1, \ldots, x_n$ as a guess to the information produced by the source; effectively we give up on compression in this case. If the output of the source is typical then we compress the output simply by storing an index for the particular sequence using nR bits in the obvious way, allowing later recovery.

Suppose $R < H(X)$. The combined compression-decompression operation has at most 2^{nR} possible outputs, so at most 2^{nR} of the sequences output from the source can be compressed and decompressed without an error occurring. By the theorem of typical sequences, for sufficiently large n the probability of a sequence output from the source lying in a subset of 2^{nR} sequences goes to zero, for $R < H(X)$. Thus any such compression scheme cannot be reliable.

Exercise 12.5: (Variable-length zero error data compression) Consider the following heuristic for a variable length data compression scheme. Let $x_1, \ldots, x_n$ be the output from n uses of an i.i.d. source with entropy rate $H(X)$. If $x_1, \ldots, x_n$ is typical, then send a $H(X)$ bit index indicating which typical sequence it is. If $x_1, \ldots, x_n$ is atypical, send an uncompressed $\log d^n$ bit index for the sequence (recall that d is the alphabet size). Turn this heuristic into a rigorous argument that the source can be compressed to an average of R bits per source symbol, for any $R > H(X)$, with zero probability of error.

9.5.6 12.2.2 Schumacher's quantum noiseless channel coding theorem

A great conceptual breakthrough of quantum information theory is to realize that we can treat quantum states as if they were information, and ask information-theoretic questions about those quantum states. In this section we define the notion of a quantum source of information, and study the question: to what extent can the 'information' - quantum states - being produced by that source be compressed?

How might we define the notion of a quantum information source? As with the definition of a classical information source it is by no means obvious what the best means of making this definition is, and it is possible to come up with several different definitions, not all of which are equivalent. The definition we are going to use is based on the idea that entanglement is what we are trying to compress and decompress. More formally, an (i.i.d) quantum source will be described by a Hilbert space H, and a density matrix ρ on that Hilbert space. We imagine that the state ρ of the system is merely part of a larger system which is in a pure state, and the mixed nature of ρ is due to entanglement between H and the remainder of the system. A compression scheme of rate R for this source consists of two families of quantum operations $\mathcal{C}^n$ and $\mathcal{D}^n$, analogous to the compression and decompression schemes used in the classical case. $\mathcal{C}^n$ is the compression operation, taking states in $H^{\otimes n}$ to states in a 2^{nR}-dimensional state space, the compressed space. We may regard the compressed space as representing nR qubits. The operation $\mathcal{D}^n$ is a decompression operation, which takes states in the compressed space to states in the original state space. The combined compression-decompression operation is therefore $\mathcal{D}^n \circ \mathcal{C}^n$. Our criterion for reliability is that in the limit of large n the entanglement fidelity
$F\left(\rho^{\otimes n}, \mathcal{D}^n \circ \mathcal{C}^n\right)$ should tend towards one. The basic idea of quantum data compression is illustrated in Figure 12.3.

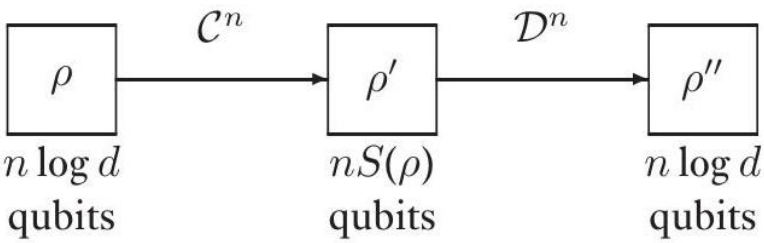


Figure 12.3. Quantum data compression. The compression operation $\mathcal{C}^n$ compresses a quantum source ρ stored in $n \log d$ qubits into $nS(\rho)$ qubits. The source is accurately recovered via the decompression operation $\mathcal{D}^n$.}

The key technical idea making the quantum noiseless channel coding theorem possible is a quantum version of the idea of typical sequences. Suppose the density operator ρ associated with a quantum source has orthonormal decomposition

$$\rho = \sum_x p(x)|x\rangle\langle x|, \tag{12.40}$$

where $|x\rangle$ is an orthonormal set, and $p(x)$ are the eigenvalues of ρ. The eigenvalues $p(x)$ of ρ obey the same rules as a probability distribution: they are non-negative and sum to one. Furthermore, $H(p(x)) = S(\rho)$. Therefore, it makes sense to talk of an ϵ-typical sequence, $x_1, \ldots, x_n$ for which

$$\left|\frac{1}{n}\log\left(\frac{1}{p\left(x_1\right)p\left(x_2\right)\ldots p\left(x_n\right)}\right)-S(\rho)\right|\leq\epsilon, \tag{12.41}$$

in exactly the same fashion as for the classical definition. An ϵ-typical state is a state $|x_1\rangle\,|x_2\rangle\ldots|x_n\rangle$ for which the sequence $x_1,x_2,\ldots,x_n$ is ϵ-typical. Define the ϵ-typical subspace to be the subspace spanned by all ϵ-typical states, $|x_1\rangle\ldots|x_n\rangle$. We'll denote the ϵ-typical subspace by $T(n,\epsilon)$, and the projector onto the ϵ-typical subspace by $P(n,\epsilon)$. Notice that

$$P(n,\epsilon)=\sum_{x\in\text{ typical}}|x_1\rangle\langle x_1|\otimes|x_2\rangle\langle x_2|\otimes\ldots|x_n\rangle\langle x_n|\,. \tag{12.42}$$

The theorem of typical sequences may now be translated into an equivalent quantum form, the typical subspace theorem.

Theorem 12.5: (Typical subspace theorem)

(1) Fix $\epsilon>0$. Then for any $\delta>0$, for sufficiently large n,

$$\text{tr}\left(P(n,\epsilon)\rho^{\otimes n}\right)\geq 1-\delta. \tag{12.43}$$

(2) For any fixed $\epsilon>0$ and $\delta>0$, for sufficiently large n, the dimension $|T(n,\epsilon)|=\text{tr}(P(n,\epsilon))$ of $T(n,\epsilon)$ satisfies:

$$(1-\delta)2^{n(S(\rho)-\epsilon)}\leq|T(n,\epsilon)|\leq 2^{n(S(\rho)+\epsilon)}. \tag{12.44}$$

(3) Let $S(n)$ be a projector onto any subspace of $H^{\otimes n}$ of dimension at most 2^{nR}, where $R<S(\rho)$ is fixed. Then for any $\delta>0$, and for sufficiently large n,

$$\text{tr}\left(S(n)\rho^{\otimes n}\right)\leq\delta. \tag{12.45}$$

In each case the result can be obtained directly using the law of large numbers, but we prefer to use the theorem of typical sequences to emphasize the close connection to the techniques used in the proof of Shannon's noiseless channel coding theorem.

Proof

Part 1: Observe that

$$\text{tr}\left(P(n,\epsilon)\rho^{\otimes n}\right)=\sum_{x\in-\text{ typical}}p\left(x_1\right)p\left(x_2\right)\ldots p\left(x_n\right) \tag{12.46}$$

The result follows immediately from part 1 of the theorem of typical sequences.
Part 2: Follows immediately from part 2 of the theorem of typical sequences.
Part 3: We split the trace up into a trace over the typical subspace and the atypical subspace,

$$\text{tr}\left(S(n)\rho^{\otimes n}\right)=\text{tr}\left(S(n)\rho^{\otimes n}P(n,\epsilon)\right)+\text{tr}\left(S(n)\rho^{\otimes n}(I-P(n,\epsilon))\right) \tag{12.47}$$

and bound each term separately. For the first term observe that

$$\rho^{\otimes n}P(n,\epsilon)=P(n,\epsilon)\rho^{\otimes n}P(n,\epsilon) \tag{12.48}$$

since $P(n,\epsilon)$ is a projector which commutes with $\rho^{\otimes n}$. But

$$\text{tr}\left(S(n)P(n,\epsilon)\rho^{\otimes n}P(n,\epsilon)\right)\leq 2^{nR}2^{-n(S(\rho)-\epsilon)}, \tag{12.49}$$

since the eigenvalues of $P(n,\epsilon)\rho^{\otimes n}P(n,\epsilon)$ are bounded above by $2^{-n(S(\rho)-\epsilon)}$. Letting $n \rightarrow \infty$ we see the first term tends to zero. For the second term note that $S(n) \leq I$. Since $S(n)$ and $\rho^{\otimes}(I - P(n,\epsilon))$ are both positive operators it follows that $0 \leq \mathrm{tr}\,(S(n)\rho^{\otimes n}(I - P(n,\epsilon)) \leq \mathrm{tr}\,(\rho^{\otimes n}(I - P(n,\epsilon)) \rightarrow 0$ as $n \rightarrow \infty$, so the second term also tends to zero as n becomes large, giving the result.

With the typical subspace theorem under our belts it is not difficult to prove a quantum analogue of Shannon's noiseless channel coding theorem. The main ideas of the proof are analogous, but the technical analysis is made a little more difficult by the appearance of non-commuting operators in the proof, which have no classical analogue.

Theorem 12.6: (Schumacher's noiseless channel coding theorem) Let $\{H, \rho\}$ be an i.i.d. quantum source. If $R > S(\rho)$ then there exists a reliable compression scheme of rate R for the source $\{H, \rho\}$. If $R < S(\rho)$ then any compression scheme of rate R is not reliable.

Proof

Suppose $R > S(\rho)$ and let $\epsilon > 0$ be such that $S(\rho)+\epsilon \leq R$. By the typical subspace theorem, for any $\delta > 0$ and for all n sufficiently large, $\mathrm{tr}\,(\rho^{\otimes n}P(n,\epsilon)) \geq 1 - \delta$, and $\dim(T(n,\epsilon)) \leq 2^{nR}$. Let H_c^n be any 2^{nR}-dimensional Hilbert space containing $T(n,\epsilon)$. The encoding is done in the following fashion. First a measurement is made, described by the complete set of orthogonal projectors $P(n,\epsilon), I - P(n,\epsilon)$, with corresponding outcomes we denote 0 and 1 . If outcome 0 occurs nothing more is done and the state is left in the typical subspace. If outcome 1 occurs then we replace the state of the system with some standard state ' $|0\rangle$ ' chosen from the typical subspace; it doesn't matter
what state is used. It follows that the encoding is a map $\mathcal{C}^n : H^{\otimes n} \rightarrow H_c^n$ into the 2^{nR}-dimensional subspace H_c^n, with operator-sum representation

$$\mathcal{C}^n(\sigma) \equiv P(n,\epsilon)\sigma P(n,\epsilon) + \sum_i A_i \sigma A_i^\dagger \tag{12.50}$$

where $A_i \equiv |0\rangle\langle i|$ and $|i\rangle$ is an orthonormal basis for the orthocomplement of the typical subspace.

The decoding operation $\mathcal{D}^n : H_c^n \rightarrow H^{\otimes n}$ is defined to be the identity on H_c^n, $\mathcal{D}^n(\sigma) = \sigma$. With these definitions for the encoding and decoding it follows that

$$F\left(\rho^{\otimes n}, \mathcal{D}^n \circ \mathcal{C}^n\right) = \left|\mathrm{tr}\left(\rho^{\otimes n}P(n,\epsilon)\right)\right|^2 + \sum_i \left|\mathrm{tr}\left(\rho^{\otimes n}A_i\right)\right|^2 \tag{12.51}$$

$$\geq \left|\mathrm{tr}\left(\rho^{\otimes n}P(n,\epsilon)\right)\right|^2 \tag{12.52}$$

$$\geq |1 - \delta|^2 \geq 1 - 2\delta \tag{12.53}$$

where the last line follows from the typical subspace theorem. But δ can be made arbitrarily small for sufficiently large n, and thus it follows that there exists a reliable compression scheme $\{\mathcal{C}^n, \mathcal{D}^n\}$ of rate R whenever $S(\rho) < R$.

To prove the converse, suppose $R < S(\rho)$. Without loss of generality we suppose that the compression operation maps from $H^{\otimes n}$ to a 2^{nR}-dimensional subspace with corresponding projector $S(n)$. Let C_j be operation elements for the compression operation $\mathcal{C}^n$, and D_k operation elements for the decompression operation $\mathcal{D}^n$. Then we have

$$F\left(\rho^{\otimes n}, \mathcal{D}^n \circ \mathcal{C}^n\right) = \sum_{jk} \left|\mathrm{tr}\left(D_k C_j \rho^{\otimes n}\right)\right|^2 \tag{12.54}$$

Each of the operators C_j maps to within the subspace with projector $S(n)$ so $C_j = S(n)C_j$. Let $S^k(n)$ be the projector onto the subspace to which the subspace $S(n)$ is mapped by D_k, so

we have $S^k(n)D_kS(n) = D_kS(n)$ and thus $D_kC_j = D_kS(n)C_j = S^k(n)D_kS(n)C_j = S^k(n)D_kC_j$, whence

$$F\left(\rho^{\otimes n}, \mathcal{D}^n \circ \mathcal{C}^n\right) = \sum_{jk} \left|\mathrm{tr}\left(D_kC_j\rho^{\otimes n}S^k(n)\right)\right|^2. \tag{12.55}$$

Applying the Cauchy-Schwarz inequality gives

$$F\left(\rho^{\otimes n}, \mathcal{D}^n \circ \mathcal{C}^n\right) \leq \sum_{jk} \mathrm{tr}\left(D_kC_j\rho^{\otimes n}C_j^\dagger D_k^\dagger\right) \mathrm{tr}\left(S^k(n)\rho^{\otimes n}\right) \tag{12.56}$$

Applying part 3 of the typical subspace theorem we see that for any $\delta > 0$ and for sufficiently large $n, \mathrm{tr}\left(S^k(n)\rho^{\otimes n}\right) \leq \delta$. Moreover, the proof of the typical subspace theorem implies that the size n needs to be for this to hold does not depend on k. Thus

$$F\left(\rho^{\otimes n}, \mathcal{D}^n \circ \mathcal{C}^n\right) \leq \delta \sum_{jk} \mathrm{tr}\left(D_kC_j\rho^{\otimes n}C_j^\dagger D_k^\dagger\right) \tag{12.57}$$

$$= \delta \tag{12.58}$$

since $\mathcal{C}^n$ and $\mathcal{D}^n$ are trace-preserving. Since δ was arbitrary it follows that $F\left(\rho^{\otimes n}, \mathcal{D}^n \circ \mathcal{C}^n\right) \to 0$ as $n \to \infty$, and thus the compression scheme is not reliable.

Schumacher's theorem not only discusses the existence of a reliable compression scheme, but it also gives clues as to how to actually construct one. The key is to be able to efficiently perform the mapping $\mathcal{C}^n : H^{\otimes n} \to H_c^n$ into the 2^{nR}-dimensional typical subspace H_c^n. Classical compression techniques such as enumerative coding, Huffman coding, and arithmetic coding can be applied but with one strong restriction: the encoding circuit must be completely reversible, and also entirely erase the original state in the process of creating the compressed one! After all, by the no-cloning theorem, it cannot copy the original state, so it cannot leave it behind as normal classical compression schemes typically do. A simple example illustrating how quantum compression works is given in Box 12.4.

Exercise 12.6: In the notation of Box 12.4, give an explicit expression for C_X in terms of X. Also, describe how to construct a quantum circuit to perform U_n for arbitrary n. How many elementary operations do you require, as a function of n ?

Exercise 12.7: (Data compression circuit) Outline the construction of a circuit to reliably compress a qubit source with $\rho = p|0\rangle\langle 0| + (1-p)|1\rangle\langle 1|$ into nR qubits for any $R > S(\rho) = H(p)$.

Exercise 12.8: (Compression of an ensemble of quantum states) Suppose that instead of adopting the definition of a quantum source based on a single density matrix ρ and the entanglement fidelity, we instead adopted the following ensemble definition, that an (i.i.d.) quantum source is specified by an ensemble $\{p_j, |\psi_j\rangle\}$ of quantum states, and that consecutive uses of the source are independent and produce a state $|\psi_j\rangle$ with probability p_j. A compression-decompression scheme ($\mathcal{C}^n, \mathcal{D}^n$) is said to be reliable in this definition if the ensemble average fidelity approaches 1 as $n \to \infty$:

$$\bar{F} \equiv \sum_J p_{j_1} \ldots p_{j_n} F\left(\rho_J, \left(\mathcal{D}^n \circ \mathcal{C}^n\right)(\rho_J)\right)^2 \tag{12.61}$$

where $J = (j_1, \ldots, j_n)$ and $\rho_J \equiv |\psi_{j_1}\rangle\langle\psi_{j_1}| \otimes \cdots \otimes |\psi_{j_n}\rangle\langle\psi_{j_n}|$. Define $\rho \equiv \sum_j p_j |\psi_j\rangle\langle\psi_j|$ and show that provided $R > S(\rho)$ there exists a reliable compression scheme of rate R with respect to this definition of fidelity.

9.5.7 12.3 Classical information over noisy quantum channels

Anything that can go wrong, will

- Attributed to Edward A. Murphy, Jr.

We all have difficulty talking on the telephone from time to time. We say we have a 'bad line' when we have exceptional difficulty understanding the person on the other end of the line. This is an example of the general phenomenon of noise which is present to some extent in all information processing systems. As described in Chapter 10 error-correcting codes can be used to combat the effects of noise, allowing reliable communication and computation to take place even in the presence of quite severe noise. Given a particular noisy communications channel $\mathcal{N}$ an interesting question is how much information can be transmitted reliably through that channel. For example, it might be possible that 1000 uses of the channel can be used to transmit 500 bits of information using an appropriate errorcorrecting code, with high probability of recovery from any errors the channel introduces.

Box 12.4: Schumacher compression

Consider an i.i.d. quantum source characterized by the single qubit density matrix

$$\rho = \frac{1}{4}\begin{bmatrix} 3 & 1 \\ 1 & 1 \end{bmatrix} \tag{12.59}$$

This could originate, for example, as a small part of a of much larger entangled system. An alternate way of viewing this source (compare Section 9.3) is that it is producing the state $|\psi_0\rangle = |0\rangle$ or $|\psi_1\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ with equal probabilities one half each (see Exercise 12.8). ρ has orthonormal decomposition $p|\overline{0}\rangle\langle\overline{0}| + (1-p)|\overline{1}\rangle\langle\overline{1}|$, where $|\overline{0}\rangle = \cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle, |\overline{1}\rangle = -\sin\frac{\pi}{8}|0\rangle + \cos\frac{\pi}{8}|1\rangle$, and $p = [3+\tan(\pi/8)]/4$. In this basis, a block of n qubits can be written as the state

$$\sum_{X=\{\overline{00}\ldots\overline{0},\overline{0}\ldots\overline{01},\ldots,\overline{11}\ldots\overline{1}\}} C_X|X\rangle. \tag{12.60}$$

By Theorem 12.6, only $|X\rangle$ for which the Hamming weight is approximately equal to np (that is, a basis for the typical subspace) need be transmitted in order to enable reconstruction of the original state with high fidelity. This is easy to appreciate, because $\left|\langle\overline{0} \mid \psi_k\rangle\right| = \cos(\pi/8)$ (for $k = \{0,1\}$) is much larger than $\left|\langle\overline{1} \mid \psi_k\rangle\right| = \sin(\pi/8)$, and for X with large Hamming weight, the coefficients C_X are very small.
How do we realize such a compression scheme? One approximate way is the following. Suppose we have quantum circuit U_n, which permutes basis states $|X\rangle$ such that states are re-ordered lexicographically according to Hamming weight. For example, for $n = 4$ it does

$$\begin{array}{llll} 0000 \to 0000 & 1000 \to 0100 & 1001 \to 1000 & 1011 \to 1100 \\ 0001 \to 0001 & 0011 \to 0101 & 1010 \to 1001 & 1101 \to 1101 \\ 0010 \to 0010 & 0101 \to 0110 & 1100 \to 1010 & 1110 \to 1110 \\ 0100 \to 0011 & 0110 \to 0111 & 0111 \to 1011 & 1111 \to 1111 \end{array}$$

Such a transform, which can be realized using just controlled-NOT and Toffoli gates, reversibly packs the typical subspace into the first $\approx nH(p)$ qubits (from left to right). To complete the scheme, we also need a quantum gate V, which rotates single qubits into the $|\overline{0}\rangle, |\overline{1}\rangle$ basis. The desired compression scheme is then $\mathcal{C}^n = \left(V^\dagger\right)^{\otimes n} U_n V^{\otimes n}$, and we need send only the first $nH(p)$ qubits output from $\mathcal{C}^n$, to enable a sequence of states from the source to be reconstructed with high fidelity, using a decoder which is the inverse of this circuit. A more

efficient coding scheme would pack just the states with Hamming weight $\approx np$ into the first $nH(p)$ qubit space; this can be done using a quantum version of arithmetic coding, for example.

We say such a code has rate $500/1000 = 1/2$. A fundamental problem of information theory is to determine the maximum rate for reliable communication through the channel $\mathcal{N}$, a number known as the capacity of the channel.

For noisy classical communications channels the capacity of the channel may be calculated using a beautiful result known as Shannon's noisy channel coding theorem. We
begin our investigation of the communication of classical information in the presence of noise in Section 12.3.1 with a discussion of some of the main ideas behind Shannon's noisy channel coding theorem. We don't get too detailed, however, because in Section 12.3.2 we move on to take a detailed look at a generalization of the problem whereby two parties attempt to communicate classical information by the use of a noisy quantum channel!

9.5.8 12.3.1 Communication over noisy classical channels

Many of the main ideas about noisy channel coding, both quantum and classical, can be understood by examining the binary symmetric channel. Recall from Section 10.1 that the binary symmetric channel is a noisy communications channel for a single bit of information, whose effect is to flip the bit being transmitted with probability $p > 0$, while with probability $1 - p$ the bit is transmitted without error, as illustrated in Figure 12.4.

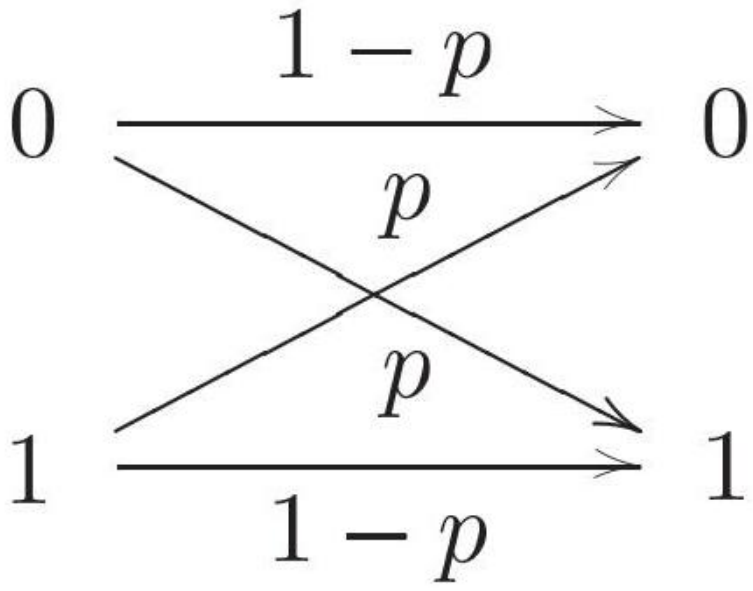


Figure 12.4. Binary symmetric channel.

How much information can we reliably transmit per use of a binary symmetric channel? Using error-correcting codes it is possible to transmit information through the channel, but at an overhead in the number of bits used to accomplish the communication. We will argue that the maximum rate at which information can be reliably transmitted is $1 - H(p)$, where $H(\cdot)$ is the Shannon entropy.

What does it mean that the transmission be reliably accomplished? This is a good question, since different answers give rise to different possible rates. We are going to use the following definition for reliability: we assume that inputs to the channel may be encoded in large blocks all at once, and require that the probability for an error in transmission using the code goes to zero as the blocksize is made large. Another possible definition of reliability is to suppose

again that the encoding may be performed in blocks, but that as the blocksize becomes large the probability of error becomes exactly zero. Unfortunately, this definition turns out to be too optimistic about what can be achieved with error-correction, and leads to zero capacity for the binary symmetric channel! Similarly, if we don't allow encoding to be performed in large blocks the capacity turns out to be zero. Indeed, it is rather amazing (and not at all obvious) that even with our less ambitious definition of reliability a non-zero rate of information transmission can be achieved. To show that this is possible several clever ideas are needed.

Random coding for the binary symmetric channel

Suppose we want to transmit nR bits of information using n uses of our binary symmetric channel; that is, we want to transmit information at a rate R through the channel. We are going to outline a proof that an error-correcting code exists that accomplishes this with low probability of error in the limit of large n, and provided $R < 1 - H(p)$. The
first idea we need is a random coding method for constructing an error-correcting code. Suppose $(q, 1-q)$ is any fixed probability distribution over the possible inputs to the channel (0 and 1). (This distribution is often called the a priori distribution of the code the introduction of this distribution is just a technical device to enable the random coding method to work, and the randomness present in the distribution should not be confused with the randomness in the channel.) Then we pick out a codeword $x = (x_1, \ldots, x_n)$ for our code simply by choosing $x_j = 0$ with probability q and $x_j = 1$ with probability $1 - q$, independently for each $j = 1, \ldots, n$. We repeat this procedure 2^{nR} times, creating a codebook C of 2^{nR} entries; we denote a generic entry in the codebook by x^j.

Obviously it's possible to construct some pretty lousy error-correcting codes using this procedure! We might get really unlucky and construct a code all of whose codewords consist of the string of n zeroes, which obviously is not much use for the transmission of information. Nevertheless, it turns out that on average this random coding procedure gives a pretty good error-correcting code. To understand why this is so, let's look at what the channel does to a single codeword in the code. Since all the codewords are constructed in the same way, we may as well look at the first, x^1.

What is the effect of the binary symmetric channel on x^1 ? On a codeword of length n we expect roughly np of the bits to be flipped, so with high probability the output from the channel will be have a Hamming distance of about np from the codeword x^1, as illustrated in Figure 12.5; we say that such an output is on the Hamming sphere of radius np around x^1. How many elements are there in this Hamming sphere? The answer to this question is roughly $2^{nH(p)}$, since the Hamming sphere consists of all the typically occurring outputs $y = x^1 \oplus e$ from the channel, where e is the error that occurs in the channel, $\oplus$ denotes bitwise addition modulo 2 , and by the theorem of typical sequences the number of such typical errors e is about $2^{nH(p)}$.

We've focused on a single codeword, but of course this same type of corruption occurs for all the codewords. We can imagine the space of all the codewords and their surrounding Hamming spheres, as depicted in Figure 12.6. If, as we've shown there, the Hamming spheres don't overlap, then there's an easy way for Bob to decode the output from the channel. He simply checks to see if the output is in one of the Hamming spheres, outputs the corresponding codeword if so, and outputs 'error' if not. Since we've assumed the spheres are non-overlapping, given any codeword as input it's highly likely that this will result in a successful decoding. Indeed, even if the spheres overlap slightly, it is still possible for Bob to perform the decoding with a good chance of success, provided the overlap is small - with high probability the output from the channel will belong to one (not zero or two or more) of the Hamming spheres, and will result in a successful decoding.

When does this small overlap condition occur? To understand this we need to better understand the structure of the possible outputs from the channel. We obtained the codewords

for our code by sampling 2^{nR} times from a set $(X_1, \ldots, X_n)$ of random variables which are independent and identically distributed with $X_j = 0$ with probability q and $X_j = 1$ with probability $1 - q$. Suppose we let Y_j be the result of sending X_j through the binary symmetric channel. The theorem of typical sequences implies that the set of typical values for $(Y_1, \ldots, Y_n)$ is of size roughly $2^{nH(Y)}$, where Y is distributed as each of the Y_j. What's more, each of these typical output values has roughly equal probability.

Now, if we sample one hundred times uniformly from a population of size one million,

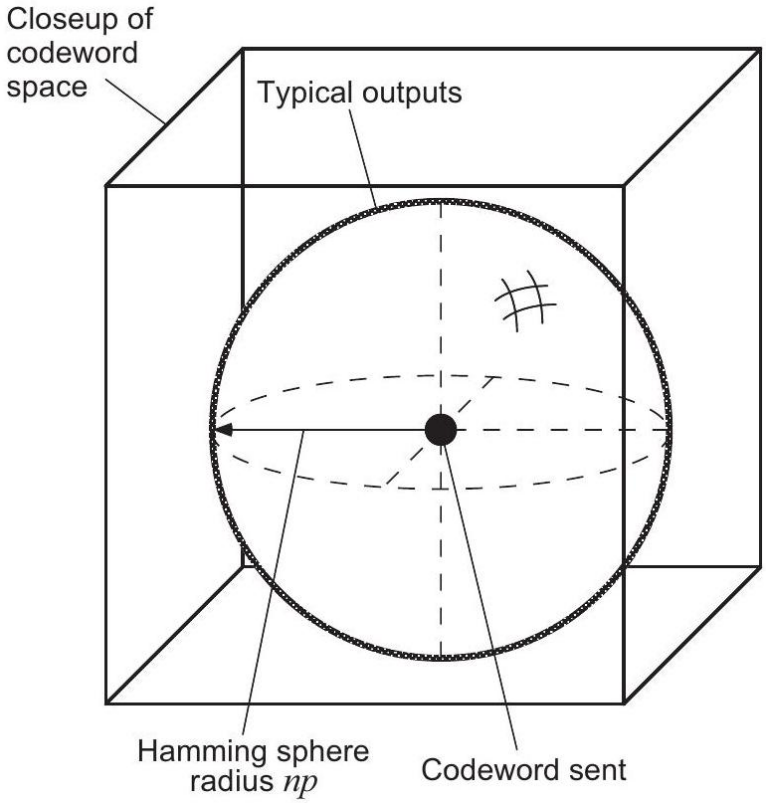


Figure 12.5. Suppose the codeword $x^{1
$ is sent through n uses of the binary symmetric channel. Then a typical output from the channel is an element of the Hamming sphere of radius np around the sequence which has been sent. (This figure is a closeup of Figure 12.6.)}

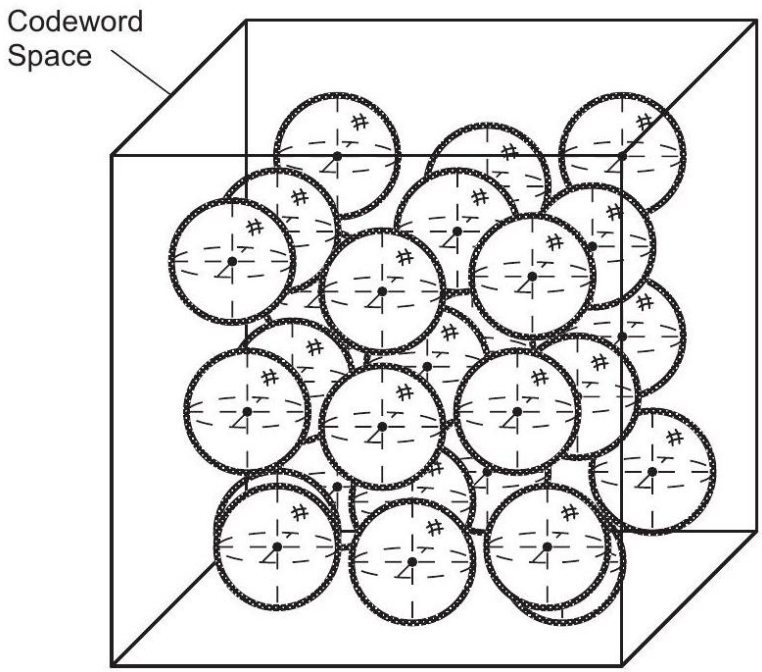


Figure 12.6. Randomly chosen codewords for the binary symmetric channel, surrounded by their Hamming spheres of 'typical' outputs. A closeup of an individual codeword may be found in Figure 12.5.

it's not too likely that we're going to get any repeats. In fact, even if we sample one hundred thousand times the number of repeats is going to be pretty small. It's not until we get out to about a million samples that the number of repeats is going to start getting large relative to the size of the sample. In a similar fashion, the amount of overlap between our 2^{nR} Hamming spheres of radius np is not going to start getting large until
the combined number of elements in all the spheres approaches the size of the space $-2^{nH(Y)}$ - that we are effectively sampling from. Since each sphere contains roughly $2^{nH(p)}$ elements, this means that we are very likely to have a good error-correcting code provided

$$2^{nR} \times 2^{nH(p)} < 2^{nH(Y)}, \tag{12.62}$$

which corresponds to the condition

$$R < H(Y) - H(p) \tag{12.63}$$

Now the entropy $H(Y)$ depends on the a priori distribution $(q, 1-q)$ chosen for the X_j. To make the rate as high as possible we try to maximize $H(Y)$. A simple calculation shows that this is achieved by using the uniform a priori distribution corresponding to $q = 1/2$, for which $H(Y) = 1$, and therefore it is possible to achieve the rate R for any R less than $1 - H(p)$.

We've just outlined a proof that it is possible to reliably transmit information through a binary symmetric channel at any rate up to $1 - H(p)$. The proof is rather sketchy, but in fact contains many of the key ideas needed for a rigorous treatment, even in the quantum case. It turns out that the rates we have shown how to achieve are also the fastest it's possible to transmit the information through the binary symmetric channel; any faster than a rate $1 - H(p)$ and the Hamming spheres start to overlap too much to determine what codeword was sent, no matter how the codewords were chosen! Thus $1 - H(p)$ is the capacity of the binary symmetric channel.

How practical is random coding as a method to achieve high rate codes for the binary symmetric channel? It is true that if we use a random code then with high probability we

can operate at a rate near the capacity. Unfortunately, there is a major difficulty with this procedure. In order to do the encoding and decoding, the sender and receiver ('Alice' and 'Bob') must first agree on a strategy for doing these tasks. In the case of random codes, this means that Alice must send Bob a list of all her random codewords. Doing this takes as much or more communication than Alice and Bob will be able to extract from the noisy channel. Clearly, this is undesirable for many applications! The random coding method is merely a method of demonstrating the existence of high rate codes, it is not a practical method for their construction. For wide practical application, what we would like is a method for achieving rates near the channel capacity which does not incur an unacceptable communication overhead for Alice and Bob. It is quite remarkable that methods for constructing such codes have only recently been discovered even for noisy classical channels, despite many decades of intense effort, and it remains an interesting open problem to find similar constructions for noisy quantum channels.

Shannon's noisy channel coding theorem

Shannon's noisy channel coding theorem generalizes the capacity result for the binary symmetric channel to the case of a discrete memoryless channel. Such a channel has a finite input alphabet $\mathcal{I}$, and a finite output alphabet $\mathcal{O}$. For the binary symmetric channel, $\mathcal{I} = \mathcal{O} = \{0, 1\}$. The action of the channel is described by a set of conditional probabilities, $p(y \mid x)$, where $x \in \mathcal{I}$ and $y \in \mathcal{O}$. These represent the probabilities of the different outputs y from the channel, given that the input was x, and satisfy the rules

$$p(y \mid x) \geq 0 \tag{12.64}$$

$$\sum_y p(y \mid x) = 1 \text{ for all } x. \tag{12.65}$$

The channel is memoryless in the sense that the channel acts the same way each time it is used, and different uses are independent of one another. We shall use the symbol $\mathcal{N}$ to denote a classical noisy channel.

Of course, there are many interesting communications channels which aren't discrete memoryless channels, such as the telephone line example given earlier, which has a continuous set of inputs and outputs. More general channels may be technically more difficult to understand than discrete memoryless channels, but many of the underlying ideas are the same and we refer you to the end of chapter 'History and further reading' for books containing information on this subject.

Let's look at the actual statement of Shannon's noisy channel coding theorem. We won't give the details of the proof, since we prove a more general result for quantum channels in the next section, but it is instructive to look at the statement of the classical result. First, we need to make our notion of reliable information transmission a little more precise. The basic idea is illustrated in Figure 12.7. In the first stage one of 2^{nR} possible messages M is produced by Alice and is encoded using a map $C^n : \left\{1, \ldots, 2^{nR}\right\} \rightarrow \mathcal{I}^n$ which assigns to each of Alice's possible messages an input string which is sent through n uses of the channel to Bob, who decodes the channel output using a map $D^n : \mathcal{O}^n \rightarrow \left\{1, \ldots, 2^{nR}\right\}$ which assigns a message to each string for each possible output from the channel. For a given encoding-decoding pair, the probability of error is defined to be the maximum probability over all messages M that the decoded output of the channel $D(Y)$ is not equal to the message M :

$$p\left(C^n, D^n\right) \equiv \max_M p\left(D^n(Y) \neq M \mid X = C^n(M)\right). \tag{12.66}$$

We say a rate R is achievable if there exists such a sequence of encoding-decoding pairs (C^n, D^n), and require in addition that $p\left(C^n, D^n\right) \rightarrow 0$ as $n \rightarrow \infty$. The capacity $C(\mathcal{N})$ of a given noisy channel $\mathcal{N}$ is defined to be the supremum over all achievable rates for the channel.

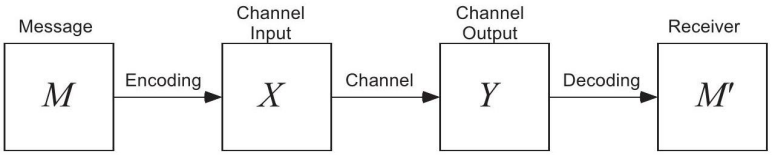


Figure 12.7. The noisy coding problem for classical messages. We require that every one of the $2^{n R} possible messages should be sent uncorrupted through the channel with high probability.}

A priori it is not at all obvious how to calculate the capacity of a channel - a barehands calculation would involve taking a supremum over a very large (infinite!) class of possible encoding and decoding methods, and does not appear to be a particularly promising approach. Shannon's noisy channel coding theorem enormously simplifies the calculation of capacity, reducing it to a simple and well-defined optimization problem that can be solved exactly in many cases, and which is computationally quite tractable even when an exact solution is not feasible.

Theorem 12.7: (Shannon's noisy channel coding theorem) For a noisy channel $\mathcal{N}$ the capacity is given by

$$C(\mathcal{N}) = \max_{p(x)} H(X:Y), \tag{12.67}$$

where the maximum is taken over all input distributions $p(x)$ for X, for one use of the channel, and Y is the corresponding induced random variable at the output of the channel.

As an example of the noisy channel coding theorem, consider the case of a binary symmetric channel flipping bits with probability p, and with input distribution $p(0) = q, p(1) = 1 - q$. We have

$$\begin{aligned} H(X:Y) &= H(Y) - H(Y \mid X) && (12.68)\\ &= H(Y) - \sum_x p(x) H(Y \mid X = x) && (12.69) \end{aligned}$$

But for each $x, H(Y \mid X = x) = H(p)$ so $H(X:Y) = H(Y) - H(p)$, which is maximized by choosing $q = 1/2$, so $H(Y) = 1$ and therefore $C(\mathcal{N}) = 1 - H(p)$ by Shannon's noisy channel coding theorem, just as our earlier intuitive calculation of the channel capacity of the binary symmetric channel suggested.

Exercise 12.9: The erasure channel has two inputs, 0 and 1 , and three outputs, 0,1 and e. With probability $1 - p$ the input is left alone. With probability p the input is 'erased', and replaced by e.
(1) Show that the capacity of the erasure channel is $1 - p$.
(2) Prove that the capacity of the erasure channel is greater than the capacity of the binary symmetric channel. Why is this result intuitively plausible?

Exercise 12.10: Suppose $\mathcal{N}_1$ and $\mathcal{N}_2$ are two discrete memoryless channels such that the input alphabet of $\mathcal{N}_2$ is equal to the output alphabet of $\mathcal{N}_1$. Show that

$$C\left(\mathcal{N}_2 \circ \mathcal{N}_1\right) \leq \min\left(C\left(\mathcal{N}_1\right), C\left(\mathcal{N}_2\right)\right) \tag{12.70}$$

Find an example where the inequality is strict.

A slight peculiarity of the noisy channel coding theorem we have presented is that nowhere does the notion of a classical information source appear! Recall that earlier we defined a classical information source as a sequence of independent and identically distributed random variables. We can combine this notion of an information source in an interesting way with the noisy channel coding theorem to obtain what is known as a source-channel coding theorem. The basic idea is illustrated in Figure 12.8. An information source with entropy rate $H(X)$ is producing information. By Shannon's noiseless channel coding theorem it is possible to compress the information from the source so that it only requires $nH(X)$ bits to describe; this step is sometimes known as source coding. The compressed output of the source is now used as the input message for the noisy channel. Transmitting at a rate R less than capacity, it requires $nH(X)/R$ uses of the channel to reliably transmit the compressed data to the receiver, who can then decompress it to recover the original output from the source.

You might wonder whether a better scheme for transmitting an information source over the noisy channel is possible. Perhaps it is possible to do something more efficient

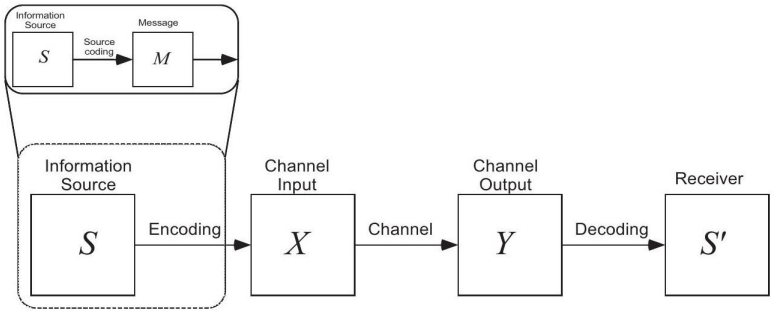


Figure 12.8. The noisy coding problem for a classical information source, sometimes known as the source-coding model.

than this two stage compress-encode and decode-decompress method? In fact, this turns out not to be the case, and the method of source-channel coding described is in fact optimal, but a proof of this fact is beyond our scope; see the end of chapter 'History and further reading' for more details.

9.5.9 12.3.2 Communication over noisy quantum channels

Suppose that instead of using a noisy classical communications channel to communicate Alice and Bob make use of a noisy quantum communications channel. More precisely, Alice has some message M that she wants to send to Bob. She encodes that message, just as she did in the classical case, but now the message is encoded as a quantum state, which is sent over the noisy quantum channel. By performing the encoding in just the right way, we hope that Bob will be able to determine what Alice's message was, with low probability of failure. Moreover, we'd like the rate at which Alice can send information to Bob to be as high as possible. What we want, in other words, is a procedure for computing the capacity for classical information of a noisy quantum channel. This problem has not yet been completely solved, but a great deal of progress has been made, and in this section we examine this progress.

What is known is how to calculate the capacity for a channel $\mathcal{E}$ assuming that Alice encodes her messages using product states of the form $\rho_1 \otimes \rho_2 \otimes \ldots$, where each of the $\rho_1, \rho_2, \ldots$ are potential inputs for one use of the channel $\mathcal{E}$. We call the capacity with this restriction the product state capacity, and denote it $C^{(1)}(\mathcal{E})$ to indicate that input states cannot be entangled across two or more uses of the channel. Note that this restricted model of communication

between Alice and Bob does allow Bob to decode using measurements entangled across multiple uses of the channel; in fact, it turns out that this is essential. The only restriction (and an unfortunate restriction it is) is that Alice can only prepare product state inputs. It is believed by many researchers, but has not been proved, that allowing entangled signals doesn't increase the capacity. The result which allows us to calculate the product state capacity is known as the Holevo-Schumacher-Westmoreland (HSW) theorem, after its discoverers. As does Shannon's noisy channel coding theorem for classical noisy channels, the HSW theorem provides an effective means for computing the product state capacity for a specified noisy channel $\mathcal{E}$, and in some instances may even allow the derivation of an exact expression.

Theorem 12.8: (Holevo-Schumacher-Westmoreland (HSW) theorem) Let $\mathcal{E}$ be a trace-preserving quantum operation. Define

$$\chi(\mathcal{E}) \equiv \max_{\{p_j,\rho_j\}} \left[S\left(\mathcal{E}\left(\sum_j p_j \rho_j\right)\right) - \sum_j p_j S\left(\mathcal{E}\left(\rho_j\right)\right) \right], \tag{12.71}$$

where the maximum is over all ensembles $\{p_j, \rho_j\}$ of possible input states ρ_j to the channel. Then $\chi(\mathcal{E})$ is the product state capacity for the channel $\mathcal{E}$, that is, $\chi(\mathcal{E}) = C^{(1)}(\mathcal{E})$.

The maximum in (12.71) is potentially over an unbounded set. In practice, we use the results of the following exercise to restrict the maximization to pure state ensembles containing at most d^2 elements, where d is the dimension of the input to the channel.

Exercise 12.11: Show that the maximum in the expression (12.71) may be achieved using an ensemble of pure states. Show further that it suffices to consider only ensembles of at most d^2 pure states, where d is the dimension of the input to the channel.

The proof of the HSW theorem involves several different ideas and it is easiest to understand the proof by breaking the discussion up into smaller pieces, and then putting the pieces together to obtain the HSW theorem.

Random coding

Suppose ρ_j is a set of possible inputs to the channel $\mathcal{E}$ and let $\sigma_j \equiv \mathcal{E}\left(\rho_j\right)$ be the corresponding outputs. We are going to develop a random coding technique similar to that described earlier for the binary symmetric channel, allowing Alice and Bob to communicate using codewords which are products of the states ρ_j. We let p_j be a probability distribution over the indices j, the a priori distribution. Alice wants to send a message M chosen from the set $\left\{1, \ldots, 2^{nR}\right\}$ to Bob. To each possible message M she associates a codeword $\rho_{M_1} \otimes \rho_{M_2} \otimes \ldots \otimes \rho_{M_n}$, where $M_1, \ldots, M_n$ are chosen from the index set $\{j\}$. (The $M_1, \ldots, M_n$ are not meant to be a decimal representation of M or anything of that sort!) For each message M Alice chooses M_1 by sampling from the distribution $\{p_j\}$. She chooses M_2 similarly and so on through to M_n, which completes the specification of the codeword. Abusing notation slightly we write $\rho_M \equiv \rho_{M_1} \otimes \cdots \otimes \rho_{M_n}$. The corresponding output states are simply denoted with a σ instead of a ρ, so for example we have $\sigma_{M_1} = \mathcal{E}\left(\rho_{M_1}\right)$ and $\sigma_M = \mathcal{E}^{\otimes n}\left(\rho_M\right)$.

When Bob receives a particular state σ_M (corresponding to Alice trying to communicate the message M) he performs a measurement in an attempt to determine what the message was. Because we are only interested in the measurement statistics and not in the post-measurement state of Bob's system, it is sufficient to describe this measurement using the POVM formalism. We suppose that for each possible message M Bob has a corresponding POVM element E_M. It is possible that Bob might have one (or more) POVM elements that don't correspond to any specific message sent by Alice; obviously these can all be summed together into a single POVM element E_0 satisfying $E_0 = I - \sum_{M \neq 0} E_M$. The probability of Bob successfully identifying M is $\mathrm{tr}\left(\sigma_M E_M\right)$, and therefore the probability of an error being made for the message M is $p_M^{\mathrm{e}} \equiv 1 - \mathrm{tr}\left(\sigma_M E_M\right)$.

What we want to do is prove the existence of high rate codes such that the probability of error $p_M^{\rm e}$ is small for all messages M. To do this we use a counter-intuitive and rather clever trick introduced by Shannon for the classical problem. We imagine that Alice is producing the messages M by choosing uniformly from the set $\left\{1, \ldots, 2^{nR}\right\}$, and analyze the average probability of error

$$p_{\rm av} \equiv \frac{\sum_M p_M^{\rm e}}{2^{nR}} = \frac{\sum_M \left(1 - {\rm tr}\left(\sigma_M E_M\right)\right)}{2^{nR}} \tag{12.72}$$

The first step of the proof is to show that high rate codes exist with $p_{\rm av}$ tending to zero as n becomes large. After this has been done we will use Shannon's trick to show that this implies the existence of codes with essentially the same rate for which $p_M^{\rm e}$ is close to zero for all M. We begin by constructing a POVM $\{E_M\}$ which represents a pretty good (though perhaps not optimal) method for Bob to decode the outputs σ_M from the channel. The key idea in the construction, as for the classical binary symmetric channel, is the idea of typicality.

Let $\epsilon > 0$. Suppose we define $\bar{\sigma} \equiv \sum_j p_j \sigma_j$, and let P be the projector onto the ϵ-typical subspace of $\bar{\sigma}^{\otimes n}$. By the theorem of typical sequences it follows that for any $\delta > 0$ and for sufficiently large n,

$$ {\rm tr}\left(\bar{\sigma}^{\otimes n}(I - P)\right) \leq \delta \tag{12.73}$$

For a given message M we are also going to define a notion of an ϵ-typical subspace for σ_M, based on the idea that typically σ_M is a tensor product of about np_1 copies of ρ_1, np_2 copies of ρ_2, and so on. Define $\bar{S} \equiv \sum_j p_j S\left(\sigma_j\right)$. Suppose σ_j has spectral decomposition $\sum_k \lambda_k^j \left|e_k^j\right\rangle \left\langle e_k^j\right|$, so

$$\sigma_M = \sum_K \lambda_K^M \left|E_K^M\right\rangle \left\langle E_K^M\right|, \tag{12.74}$$

where $K = (K_1, \ldots, K_n)$, and for convenience we define $\lambda_K^M \equiv \lambda_{K_1}^{M_1} \lambda_{K_2}^{M_2} \ldots \lambda_{K_n}^{M_n}$ and $\left|E_K^M\right\rangle \equiv \left|e_{K_1}^{M_1}\right\rangle \left|e_{K_2}^{M_2}\right\rangle \ldots \left|e_{K_n}^{M_n}\right\rangle$. Define P_M to be the projector onto the space spanned by all $\left|E_K^M\right\rangle$ such that

$$\left|\frac{1}{n} \log \frac{1}{\lambda_K^M} - \bar{S}\right| \leq \epsilon \tag{12.75}$$

(It will be useful to denote by T_M the set of all K such that this condition is satisfied.) In a similar manner to the proof of the theorem of typical sequences, the law of large numbers implies that for any $\delta > 0$ and for sufficiently large n we have $\mathbf{E}\left({\rm tr}\left(\sigma_M P_M\right)\right) \geq 1 - \delta$, where the expectation is taken with respect to the distribution over codewords ρ_M (for a fixed message M) induced by random coding, and thus for each M,

$$\mathbf{E}\left[{\rm tr}\left(\sigma_M \left(I - P_M\right)\right)\right] \leq \delta \tag{12.76}$$

Also note that by the definition (12.75) the dimension of the subspace onto which P_M projects can be at most $2^{n(\bar{S}+\epsilon)}$, and thus

$$\mathbf{E}\left({\rm tr}\left(P_M\right)\right) \leq 2^{n(\bar{S}+\epsilon)} \tag{12.77}$$

We now use the typicality notions to define Bob's decoding POVM. We define

$$E_M \equiv \left(\sum_{M'} P P_{M'} P\right)^{-1/2} P P_M P \left(\sum_{M'} P P_{M'} P\right)^{-1/2} \tag{12.78}$$

where $A^{-1/2}$ denotes the generalized inverse of $A^{1/2}$, that is, the operator which is inverse to $A^{1/2}$ on the support of A and is otherwise zero. It follows that $\sum_M E_M \leq I$, and we can define one more positive operator $E_0 \equiv I - \sum_M E_M$ to complete the POVM. The intuition behind this construction is similar to the decoding method described for the binary symmetric channel. In particular, up to small corrections E_M is equal to the projector P_M, and Bob's measurement of $\{E_M\}$ corresponds essentially to checking to see if the output from the channel falls into the space on which P_M projects; the space onto which this projector projects can be thought of as analogous to the Hamming sphere of radius np around the codewords used for the binary symmetric channel.

The main technical part of the proof that random coding works is to obtain an upper bound on the average probability of error $p_{\rm av}$. The details of how this is done are given in Box 12.5. The result is

$$p_{\rm av} \leq \frac{1}{2^{nR}} \sum_M \left[3 \operatorname{tr}\left(\sigma_M (I-P)\right) + \sum_{M' \neq M} \operatorname{tr}\left(P \sigma_M P P_{M'}\right) + \operatorname{tr}\left(\sigma_M \left(I - P_M\right)\right) \right] \tag{12.79}$$

The quantity $p_{\rm av}$ is defined with respect to a specific choice of codewords. We are going to calculate the expectation of this quantity over all random codes. By construction $\mathbf{E}\left(\sigma_M\right) = \bar{\sigma}^{\otimes n}$, and σ_M and $P_{M'}$ are independent when $M' \neq M$, so we obtain

$$\mathbf{E}\left(p_{\rm av}\right) \leq 3 \operatorname{tr}\left(\bar{\sigma}^{\otimes n}(I-P)\right) + \left(2^{nR}-1\right) \operatorname{tr}\left(P \bar{\sigma}^{\otimes n} P \mathbf{E}\left(P_1\right)\right) + \mathbf{E}\left(\operatorname{tr}\left(\sigma_1 \left(I - P_1\right)\right)\right) \tag{12.80}$$

Substituting (12.73) and (12.76) we obtain

$$\mathbf{E}\left(p_{\rm av}\right) \leq 4\delta + \left(2^{nR}-1\right) \operatorname{tr}\left(P \bar{\sigma}^{\otimes n} P \mathbf{E}\left(P_1\right)\right) \tag{12.81}$$

But $P \bar{\sigma}^{\otimes n} P \leq 2^{-n(S(\bar{\sigma})-\epsilon)} I$ and by (12.77) we have $\mathbf{E}\left(\operatorname{tr}\left(P_1\right)\right) \leq 2^{n(\bar{S}+\epsilon)}$ whence

$$\mathbf{E}\left(p_{\rm av}\right) \leq 4\delta + \left(2^{nR}-1\right) 2^{-n(S(\bar{\sigma})-\bar{S}-2\epsilon)} \tag{12.82}$$

Provided $R < S(\bar{\sigma}) - \bar{S}$ it follows that $\mathbf{E}\left(p_{\rm av}\right) \to 0$ as $n \to \infty$. Indeed, by choosing the ensemble $\{p_j, \rho_j\}$ to achieve the maximum in (12.71) we see that this must be true whenever $R < \chi(\mathcal{E})$. Thus there must exist a sequence of codes of rate R such that $p_{\rm av} \to 0$ as the block-size n of the code is increased. It follows that for any fixed $\epsilon > 0$ (note that this is a new meaning of ϵ to replace the old, which is no longer needed!) for sufficiently large n

$$p_{\rm av} = \frac{\sum_M p_M^{\rm e}}{2^{nR}} < \epsilon \tag{12.83}$$

Obviously in order for this to be true at least half the messages M must satisfy $p_M^{\rm e} < 2\epsilon$. So we construct a new code by deleting half the codewords (the codewords with high $p_M^{\rm e}$) from the code with rate R and $p_{\rm av} < \epsilon$, obtaining a new code with $2^{nR}/2 = 2^{n(R-1/n)}$ codewords, and with $p_M^{\rm e} < 2\epsilon$ for all messages M. Obviously this code also has asymptotic rate R, and the probability of an error can be made arbitrarily small for all codewords, not just on average, as n becomes large.

Summing up, we have shown that for any rate R less than $\chi(\mathcal{E})$ as defined in (12.71), there exists a code using product state inputs enabling transmission through the channel $\mathcal{E}$ at rate R. Our proof suffers the same flaw as do random coding proofs of Shannon's
classical noisy channel coding theorem, namely, it does not provide a constructive procedure for performing the coding, but it does at least demonstrate the existence of codes at rates up to capacity.

Proof of the upper bound

Suppose R is greater than $\chi(\mathcal{E})$ as defined in (12.71). We will show that it is impossible for Alice to reliably send information to Bob at this rate through the channel $\mathcal{E}$. Our general strategy is to imagine that Alice is producing messages M uniformly at random from the set $\left\{1, \ldots, 2^{nR}\right\}$ and to show that her average error probability must be bounded away from zero, and therefore the maximum error probability must also be bounded away from zero.

Suppose Alice encodes message M as $\rho_M = \rho_1^M \otimes \cdots \otimes \rho_n^M$ with corresponding outputs denoted using σ instead of ρ, and Bob decodes using a POVM $\{E_M\}$ which, without loss of generality, we may suppose contains an element E_M for each message, and possibly an extra element E_0 to ensure that the completeness relation $\sum_M E_M = I$ is satisfied. This gives an average error probability:

$$p_{\text{av}} = \frac{\sum_M \left(1 - \text{tr}\left(\sigma_M E_M\right)\right)}{2^{nR}} \tag{12.96}$$

From Exercise 12.3 we know that $R \leq \log(d)$, where d is the dimension of the input to the channel, and thus the POVM $\{E_M\}$ contains at most $d^n + 1$ elements. By Fano's inequality it follows that

$$H\left(p_{\text{av}}\right) + p_{\text{av}} \log\left(d^n\right) \geq H(M \mid Y) \tag{12.97}$$

where Y is the measurement outcome from Bob's decoding, and thus

$$np_{\text{av}} \log d \geq H(M) - H(M:Y) - H\left(p_{\text{av}}\right) = nR - H(M:Y) - H\left(p_{\text{av}}\right) \tag{12.98}$$

Applying first the Holevo bound and then the subadditivity of entropy gives

$$H(M:Y) \leq S(\bar{\sigma}) - \sum_M \frac{S\left(\sigma_1^M \otimes \cdots \otimes \sigma_n^M\right)}{2^{nR}} \tag{12.99}$$

$$\leq \sum_{j=1}^{n} \left(S\left(\bar{\sigma}^j\right) - \sum_M \frac{S\left(\sigma_j^M\right)}{2^{nR}} \right) \tag{12.100}$$

where $\bar{\sigma}^j \equiv \sum_M \sigma_j^M / 2^{nR}$. Each of the n terms in the sum on the right hand side is no greater than $\chi(\mathcal{E})$ as defined in (12.71), so

$$H(M:Y) \leq n\chi(\mathcal{E}) \tag{12.101}$$

Substituting into (12.98) gives $np_{\text{av}} \log d \geq n(R - \chi(\mathcal{E})) - H\left(p_{\text{av}}\right)$, and thus in the limit as n becomes large we obtain

$$p_{\text{av}} \geq \frac{(R - \chi(\mathcal{E}))}{\log(d)} \tag{12.102}$$

which is bounded away from zero when $R > \chi(\mathcal{E})$, which completes the proof that $\chi(\mathcal{E})$ is an upper bound on the product state capacity.

Box 12.5: HSW theorem: the error estimate

The most technically complicated part of the proof of the HSW theorem is obtaining an estimate for p_{av}. We outline the details of how this is done here; missing steps should be regarded as exercises to be filled in. Suppose we define $\left|\tilde{E}_K^M\right\rangle \equiv P \left|E_K^M\right\rangle$. Then

$$E_M = \left(\sum_{M'} \sum_{K \in T_{M'}} \left| \tilde{E}_K^{M'} \right\rangle \left\langle \tilde{E}_K^{M'} \right| \right)^{-1/2} \sum_{K \in T_M} \left| \tilde{E}_K^{M} \right\rangle \left\langle \tilde{E}_K^{M} \right| \left(\sum_{M'} \sum_{K \in T_{M'}} \left| \tilde{E}_K^{M'} \right\rangle \left\langle \tilde{E}_K^{M'} \right| \right)^{-1/2} \tag{12.84}$$

Defining

$$\alpha_{(M,K),(M',K')} \equiv \left\langle \tilde{E}_K^M \right| \left(\sum_{M''} \sum_{K'' \in T_{M''}} \left| \tilde{E}_{K''}^{M''} \right\rangle \left\langle \tilde{E}_{K''}^{M''} \right| \right)^{-1/2} \left| \tilde{E}_{K'}^{M'} \right\rangle, \tag{12.85}$$

the average probability of error can be written

$$p_{\text{av}} = \frac{1}{2^{nR}} \sum_M \left[1 - \sum_K \sum_{K' \in T_M} \lambda_K^M \left| \alpha_{(M,K),(M,K')} \right|^2 \right]. \tag{12.86}$$

Using $\sum_K \lambda_K^M = 1$ and omitting non-positive terms, we see that

$$p_{\text{av}} \leq \frac{1}{2^{nR}} \sum_M \left[\sum_{K \in T_M} \lambda_K^M \left(1 - \alpha^2_{(M,K),(M,K)} \right) + \sum_{K \notin T_M} \lambda_K^M \right]. \tag{12.87}$$

Define a matrix Γ with entries $\gamma_{(M,K),(M',K')} \equiv \left\langle \tilde{E}_K^M \mid \tilde{E}_{K'}^{M'} \right\rangle$, where the indices are such that $K \in T_M$ and $K' \in T_{M'}$. It is convenient to work in the matrix space defined by these index conventions, to let E denote the unit matrix with respect to these indices, and to use sp (for *spur*) to denote the trace operations with respect to these indices. A calculation shows that $\Gamma^{1/2} = \left[\alpha_{(M,K),(M',K')} \right]$ and it follows that $\alpha^2_{(M,K),(M,K)} \leq \gamma_{(M,K),(M,K)} \leq 1$. Using the observation that $1 - x^2 = (1+x)(1-x) \leq 2(1-x)$ when $0 \leq x \leq 1$ together with (12.87) gives

$$p_{\text{av}} \leq \frac{1}{2^{nR}} \sum_M \left[2 \sum_{K \in T_M} \lambda_K^M \left(1 - \alpha_{(M,K),(M,K)} \right) + \sum_{K \notin T_M} \lambda_K^M \right]. \tag{12.88}$$

Define the diagonal matrix $\Lambda \equiv \text{diag}\left(\lambda_K^M \right)$ and observe that

$$\begin{aligned} 2\left(E - \Gamma^{1/2} \right) &= \left(E - \Gamma^{1/2} \right)^2 + (E - \Gamma) && (12.89) \\ &= (E - \Gamma)^2 \left(E + \Gamma^{1/2} \right)^{-2} + (E - \Gamma) && (12.90) \\ &\leq (E - \Gamma)^2 + (E - \Gamma) && (12.91) \end{aligned}$$

Thus,

$$\begin{aligned} 2 \sum_M \sum_{K \in T_M} \lambda_K^M \left(1 - \alpha_{(M,K),(M,K)} \right) &= 2 \,\text{sp}\left(\Lambda \left(E - \Gamma^{1/2} \right) \right) && (12.92) \\ &\leq \text{sp}\left(\Lambda (E - \Gamma)^2 \right) + \text{sp}(\Lambda (E - \Gamma)). && (12.93) \end{aligned}$$

(continued)

Box 12.5 (continued):

Calculating the spurs on the right hand side, substituting into (12.88), and doing some simple algebra gives

$$p_{\text{av}} \leq \frac{1}{2^{nR}} \sum_M \left[\sum_K \lambda_K^M \left(2 - 2\gamma_{(M,K),(M,K)} + \sum_{K' \neq K} \left|\gamma_{(M,K),(M,K')}\right|^2 + \sum_{M' \neq M, K' \in T_{M'}} \left|\gamma_{(M,K),(M',K')}\right|^2 \right) + \sum_{K \notin T_M} \lambda_K^M \right] \tag{12.94}$$

Substituting definitions and doing some simple algebra gives

$$p_{\text{av}} \leq \frac{1}{2^{nR}} \sum_M \left[2\,\text{tr}\left(\sigma_M(I-P)\right) + \text{tr}\left(\sigma_M(I-P)P_M(I-P)\right) + \sum_{M' \neq M} \text{tr}\left(P\sigma_M P P_{M'}\right) + \text{tr}\left(\sigma_M\left(I - P_M\right)\right) \right] \tag{12.95}$$

The second term is less than $\text{tr}\left(\sigma_M(I-P)\right)$, which gives the desired error estimate, (12.79).

Examples

An interesting implication of the HSW theorem is that any quantum channel $\mathcal{E}$ whatsoever can be used to transmit classical information, provided the channel is not simply a constant. For if the channel is not a constant then there exist pure states $|\psi\rangle$ and $|\varphi\rangle$ such that $\mathcal{E}(|\psi\rangle\langle\psi|) \neq \mathcal{E}(|\varphi\rangle\langle\varphi|)$. Substituting the ensemble made up of these two states with equal probabilities $1/2$ into the expression (12.71) for the product state capacity we see that

$$C^{(1)}(\mathcal{E}) \geq S\left(\frac{\mathcal{E}(|\psi\rangle\langle\psi|) + \mathcal{E}(|\varphi\rangle\langle\varphi|)}{2}\right) - \frac{1}{2}\mathcal{E}(|\psi\rangle\langle\psi|) - \frac{1}{2}\mathcal{E}(|\varphi\rangle\langle\varphi|) > 0 \tag{12.103}$$

where the second inequality follows from the strict concavity of the entropy established in Section 11.3.5.

Let's look at a simple example where the product state capacity can be calculated exactly, the case of the depolarizing channel with parameter p. Let $\{p_j, |\psi_j\rangle\}$ be an ensemble of quantum states. Then we have

$$\mathcal{E}\left(|\psi_j\rangle\langle\psi_j|\right) = p\,|\psi_j\rangle\langle\psi_j| + (1-p)\frac{I}{2} \tag{12.104}$$

a quantum state which has eigenvalues $(1+p)/2$ and $(1-p)/2$ from which it follows that

$$S\left(\mathcal{E}\left(|\psi_j\rangle\langle\psi_j|\right)\right) = H\left(\frac{1+p}{2}\right) \tag{12.105}$$

which does not depend on $|\psi_j\rangle$ at all. Thus the maximum in (12.71) is achieved by maximizing the entropy $S\left(\sum_j \mathcal{E}\left(|\psi_j\rangle\langle\psi_j|\right)\right)$, which may be done by simply choosing the $|\psi_j\rangle$ to form an orthonormal basis (say $|0\rangle$ and $|1\rangle$) for the state space of a single qubit, giving a value for the entropy of one bit, and a product state capacity of

$$C(\mathcal{E}) = 1 - H\left(\frac{1+p}{2}\right) \tag{12.106}$$

for the depolarizing channel with parameter p.

Exercise 12.12: Adapt the proof of the HSW theorem to find a proof of Shannon's noisy channel coding theorem, simplifying the proof wherever possible.

9.5.10 12.4 Quantum information over noisy quantum channels

How much quantum information can be reliably transmitted over a noisy quantum channel? This problem of determining the quantum channel capacity is less well understood than is the problem of determining the capacity for sending classical information through a noisy quantum channel. We now present some of the information-theoretic tools that have been developed to understand the capacity of a quantum channel for quantum information, most notably quantum information-theoretic analogues to the Fano inequality (Box 12.2 on page 536), data processing inequality (Section 11.2.4 on page 509) and Singleton bound (Exercise 10.21 on page 449).

As for quantum data compression, our point of view in studying these problems is to regard a quantum source as being a quantum system in a mixed state ρ which is entangled with another quantum system, and the measure of reliability for transmission of quantum information by the quantum operation $\mathcal{E}$ is the entanglement fidelity $F(\rho, \mathcal{E})$. It is useful to introduce, as in Chapter 9, labels Q for the system ρ lives in and R, the reference system, which initially purifies Q. In this picture the entanglement fidelity is a measure of how well the entanglement between Q and R was preserved by the action of $\mathcal{E}$ on system Q.

9.5.11 12.4.1 Entropy exchange and the quantum Fano inequality

How much noise does a quantum operation cause when applied to the state ρ of a quantum system Q ? One measure of this is the extent to which the state of RQ, initially pure, becomes mixed as a result of the quantum operation. We define the entropy exchange of the operation $\mathcal{E}$ upon input of ρ by

$$S(\rho, \mathcal{E}) \equiv S\left(R', Q'\right) \tag{12.107}$$

Suppose that the action of the quantum operation $\mathcal{E}$ is mocked up by introducing an environment E, initially in a pure state, and then causing a unitary interaction between Q and E, as described in Chapter 8. Then the state of RQE after the interaction is a pure state, whence $S\left(R', Q'\right) = S\left(E'\right)$, so the entropy exchange may also be identified with the amount of entropy introduced by the operation $\mathcal{E}$ into an initially pure environment E.

Note that the entropy exchange does not depend upon the way in which the initial state of Q, ρ, is purified into RQ. The reason is because any two purifications of Q into RQ are related by a unitary operation on the system R, as shown in Exercise 2.81 on page 111. This unitary operation on R obviously commutes with the action of the
quantum operation on Q, and thus the final states of $R'Q'$ induced by the two different purifications are related by a unitary transformation on R, and thus give rise to the same value for the entropy exchange. Furthermore, it follows from these results that $S\left(E'\right)$ does not depend upon the particular environmental model for $\mathcal{E}$ which is used, provided the model starts with E in a pure state.

A useful explicit formula for the entropy exchange can be given based upon the operator-sum representation for quantum operations. Suppose a trace-preserving quantum operation $\mathcal{E}$ has operation elements $\{E_i\}$. Then, as shown in Section 8.2.3, a unitary model for this quantum operation is given by defining a unitary operator U on QE such that

$$U|\psi\rangle|0\rangle = \sum_i E_i|\psi\rangle|i\rangle \tag{12.108}$$

where $|0\rangle$ is the initial state of the environment, and $|i\rangle$ is an orthonormal basis for the environment. Note that the state of E' after application of $\mathcal{E}$ is:

$$\rho^{E'} = \sum_{i,j} \mathrm{tr}\left(E_i \rho E_j^\dagger\right) |i\rangle\langle j| \tag{12.109}$$

That is, $\mathrm{tr}\left(E_i \rho E_j^\dagger\right)$ are the matrix elements of E' in the $|i\rangle$ basis. Given a quantum operation with operation elements $\{E_i\}$ it is therefore natural to define a matrix W (the w-matrix) with matrix elements $W_{ij} \equiv \mathrm{tr}\left(E_i \rho E_j^\dagger\right)$, that is, W is the matrix of E' in an appropriate basis. This representation for $\rho^{E'}$ gives rise to a formula for the entropy exchange which is useful in making explicit calculations,

$$S(\rho, \mathcal{E}) = S(W) \equiv -\mathrm{tr}(W \log W) \tag{12.110}$$

Given a quantum operation $\mathcal{E}$ and a state ρ, it is always possible to choose operation elements $\{F_j\}$ for $\mathcal{E}$ such that W is diagonal; we say W is in canonical form. To see that such a set of operation elements exists, recall from Chapter 8 that a quantum operation may have many different sets of operation elements. In particular, two sets of operators $\{E_i\}$ and $\{F_j\}$ are operation elements for the same quantum operation if and only if $F_j = \sum_j u_{ji} E_i$, where u is a unitary matrix of complex numbers, and it may be necessary to append 0 operators to the sets E_i or F_j so that the matrix u is a square matrix. Let W be the w-matrix associated to a particular choice of operation elements $\{E_i\}$ for $\mathcal{E}$.W is a matrix representation of the environmental density operator, and thus is a positive matrix which may be diagonalized by a unitary matrix $v, D = vWv^\dagger$, where D is a diagonal matrix with non-negative entries. Define operators F_j by the equation $F_j \equiv \sum_i v_{ji} E_i$, so the F_j are also a set of operation elements for $\mathcal{E}$, giving rise to a new w-matrix $\widetilde{W}$ with matrix elements

$$\widetilde{W}_{kl} = \mathrm{tr}\left(F_k \rho F_l^\dagger\right) = \sum_{mn} v_{km} v_{ln}^* W_{mn} = D_{kl} \tag{12.111}$$

Thus, the w -matrix is diagonal if calculated with respect to the operation elements $\{F_j\}$. Any such set of operation elements $\{F_j\}$ for $\mathcal{E}$ for which the corresponding w-matrix is diagonal is said to be a canonical representation for $\mathcal{E}$ with respect to the input ρ. We see later that canonical representations turn out to have a special significance for quantum error-correction.

Many properties of the entropy exchange follow easily from properties of the entropy discussed in Chapter 11. For example, working in a canonical representation for a trace-preserving quantum operation $\mathcal{E}$ on a d-dimensional space, we see immediately that $S(I/d, \mathcal{E}) = 0$ if and only if $\mathcal{E}$ is a unitary quantum operation. Therefore, $S(I/d, \mathcal{E})$ can be thought of as quantifying the extent to which incoherent quantum noise occurs on the system as a whole. A second example is that the matrix W is linear in ρ, and by the concavity of the entropy it follows that $S(\rho, \mathcal{E})$ is concave in ρ. Since the system RQ can always be chosen to be at most d^2-dimensional, where d is the dimension of Q, it follows that the entropy exchange is bounded above by $2 \log d$.

Exercise 12.13: Show that the entropy exchange is concave in the quantum operation $\mathcal{E}$.

Intuitively, if the quantum source Q is subject to noise which results in the entanglement RQ becoming mixed, then the fidelity of the final state $R'Q'$ with the initial state RQ cannot be perfect. Moreover, the greater the noise the worse the fidelity. In Section 12.1.1 an analogous situation arose in the study of classical channels, where the uncertainty $H(X \mid Y)$ about the input of a channel, X, given the output, Y, was related to the probability of being able to recover the state of X from Y by the Fano inequality. There is a very useful quantum analogue of this result, relating the entropy exchange $S(\rho, \mathcal{E})$ to the entanglement fidelity $F(\rho, \mathcal{E})$.

Theorem 12.9: (Quantum Fano inequality) Let ρ be a quantum state and $\mathcal{E}$ a trace-preserving quantum operation. Then

$$S(\rho, \mathcal{E}) \leq H(F(\rho, \mathcal{E})) + (1 - F(\rho, \mathcal{E})) \log \left(d^2 - 1\right) \tag{12.112}$$

where $H(\cdot)$ is the binary Shannon entropy.
Inspection of the quantum Fano inequality reveals an attractive intuitive meaning: if the entropy exchange for a process is large, then the entanglement fidelity for the process must necessarily be small, indicating that the entanglement between R and Q has not been well preserved. Moreover, we note that in the quantum Fano inequality the entropy exchange $S(\rho, \mathcal{E})$ plays a role analogous to the role played by the conditional entropy $H(X \mid Y)$ in classical information theory.

Proof

To prove the quantum Fano inequality, let $|i\rangle$ be an orthonormal basis for the system RQ chosen so the first state in the set $|1\rangle = |RQ\rangle$. If we form the quantities $p_i \equiv \langle i|\rho^{R'Q'}|i\rangle$, then from the results of Section 11.3.3 it follows that

$$S\left(R', Q'\right) \leq H\left(p_1, \ldots, p_{d^2}\right) \tag{12.113}$$

where $H\left(p_i\right)$ is the Shannon information of the set $\{p_i\}$. Elementary algebra shows that

$$H\left(p_1, \ldots, p_{d^2}\right) = H\left(p_1\right) + \left(1 - p_1\right) H\left(\frac{p_2}{1 - p_1}, \ldots, \frac{p_{d^2}}{1 - p_1}\right) \tag{12.114}$$

Combining this with the observation that $H\left(\frac{p_2}{1-p_1}, \ldots, \frac{p_{d^2}}{1-p_1}\right) \leq \log\left(d^2 - 1\right)$ and $p_1 = F(\rho, \mathcal{E})$ by definition gives,

$$S(\rho, \mathcal{E}) \leq H(F(\rho, \mathcal{E})) + (1 - F(\rho, \mathcal{E})) \log \left(d^2 - 1\right) \tag{12.115}$$

which is the quantum Fano inequality.

9.5.12 12.4.2 The quantum data processing inequality

In Section 11.2.4 we discussed the classical data processing inequality. Recall that the data processing inequality states that for a Markov process $X \rightarrow Y \rightarrow Z$,

$$H(X) \geq H(X : Y) \geq H(X : Z) \tag{12.116}$$

with equality in the first stage if and only if the random variable X can be recovered from Y with probability one. Thus the data processing inequality provides informationtheoretic necessary and sufficient conditions for error-correction to be possible.

There is a quantum analogue to the data processing inequality applicable to a two stage quantum process described by quantum operations $\mathcal{E}_1$ and $\mathcal{E}_2$,

$$\rho \stackrel{\mathcal{E}_1}{\rightarrow} \rho' \stackrel{\mathcal{E}_2}{\rightarrow} \rho''. \tag{12.117}$$

We define the quantum coherent information by

$$I(\rho, \mathcal{E}) \equiv S(\mathcal{E}(\rho)) - S(\rho, \mathcal{E}) \tag{12.118}$$

This quantity, coherent information, is suspected (but not known) to play a role in quantum information theory analogous to the role played by the mutual information $H(X : Y)$ in classical

information theory. One reason for this belief is that the coherent information satisfies a quantum data processing inequality analogous to the classical data processing inequality.

Theorem 12.10: (Quantum data processing inequality) Let ρ be a quantum state and $\mathcal{E}_1$ and $\mathcal{E}_2$ trace-preserving quantum operations. Then

$$S(\rho) \geq I\left(\rho, \mathcal{E}_1\right) \geq I\left(\rho, \mathcal{E}_2 \circ \mathcal{E}_1\right) \tag{12.119}$$

with equality in the first inequality if and only if it is possible to perfectly reverse the operation $\mathcal{E}_1$, in the sense that there exists a trace-preserving reversal operation $\mathcal{R}$ such that $F(\rho, \mathcal{R} \circ \mathcal{E}) = 1$.

Comparison with the classical data processing inequality shows that the coherent information plays a role in the quantum data processing inequality identical to the role played by the mutual information in the classical data processing inequality. Of course, such a heuristic argument cannot be regarded as any sort of a rigorous justification for the view that the coherent information is the correct quantum analogue of the classical mutual information. In order to obtain such a justification, the coherent information ought to be related to the quantum channel capacity in a similar way to the relation between classical mutual information and classical channel capacity, and such a relationship has not yet been established. (See the end of chapter 'History and further reading' for some partial progress.)

How is the notion of perfect reversibility defined in the quantum data processing inequality connected with more familiar notions such as that arising in the context of quantum error-correction? By definition, we say a trace-preserving quantum operation $\mathcal{E}$ is perfectly reversible upon input of ρ if there exists a trace-preserving quantum operation $\mathcal{R}$ such that

$$F(\rho, \mathcal{R} \circ \mathcal{E}) = 1 \tag{12.120}$$

But from item (4) on page 423, it follows that a quantum operation is perfectly reversible if and only if for every state $|\psi\rangle$ in the support of ρ,

$$(\mathcal{R} \circ \mathcal{E})(|\psi\rangle\langle\psi|) = |\psi\rangle\langle\psi|. \tag{12.121}$$

This observation connects the notion of perfect reversibility to quantum error-correcting codes. Recall that a quantum error-correcting code is a subspace of some larger Hilbert space spanned by logical codewords. To be resilient against the noise induced by a quantum operation $\mathcal{E}$ it is necessary that the quantum operation $\mathcal{E}$ be reversible by a trace-preserving reversal operation $\mathcal{R}$ in the sense that for all states $|\psi\rangle$ in the code, $(\mathcal{R} \circ \mathcal{E})(|\psi\rangle\langle\psi|) = |\psi\rangle\langle\psi|$. This condition is equivalent to the criterion of perfect reversibility in the statement of the data processing inequality, that $F(\rho, \mathcal{R} \circ \mathcal{E}) = 1$, for some ρ whose support is the code space.

Proof

The quantum data processing inequality is proved using a four system construction: R and Q appear in their familiar roles, while E_1 and E_2 are systems initially in pure states, chosen such that a unitary interaction between Q and E_1 generates the dynamics $\mathcal{E}_1$, and a unitary interaction between Q and E_2 generates the dynamics $\mathcal{E}_2$. The proof of the first stage of the quantum data processing inequality is to apply the subadditivity inequality $S\left(R', E_1'\right) \leq S\left(R'\right) + S\left(E_1'\right)$ to obtain

$$I(\rho, \mathcal{E}_1) = S(\mathcal{E}_1(\rho)) - S(\rho, \mathcal{E}_1) \tag{12.122}$$
$$= S(Q') - S(E_1') \tag{12.123}$$
$$= S(R', E_1') - S(E_1') \tag{12.124}$$
$$\leq S(R') + S(E_1') - S(E_1') = S(R') \tag{12.125}$$
$$= S(R) = S(Q) = S(\rho) \tag{12.126}$$

The proof of the second part of the data processing inequality is to apply the strong subadditivity inequality,

$$S(R'', E_1'', E_2'') + S(E_1'') \leq S(R'', E_1'') + S(E_1'', E_2'') \tag{12.127}$$

From the purity of the total state of $R''Q''E_1''E_2''$ it follows that

$$S(R'', E_1'', E_2'') = S(Q'') \tag{12.128}$$

Neither of the systems R or E_1 are involved in the second stage of the dynamics in which Q and E_2 interact unitarily. Thus, their state does not change during this stage: $\rho^{R''E_1''} = \rho^{R'E_1'}$. But from the purity of RQE_1 after the first stage of the dynamics,

$$S(R'', E_1'') = S(R', E_1') = S(Q') \tag{12.129}$$

The remaining two terms in the strong subadditivity inequality (12.127) are now recognized as entropy exchanges,

$$S(E_1'') = S(E_1') = S(\rho, \mathcal{E}_1); \quad S(E_1'', E_2'') = S(\rho, \mathcal{E}_2 \circ \mathcal{E}_1) \tag{12.130}$$

Making these substitutions into (12.127) yields

$$S(Q'') + S(\rho, \mathcal{E}_1) \leq S(Q') + S(\rho, \mathcal{E}_2 \circ \mathcal{E}_1) \tag{12.131}$$

which can be rewritten as the second stage of the data processing inequality, $I(\rho, \mathcal{E}_1) \geq I(\rho, \mathcal{E}_2 \circ \mathcal{E}_1)$.

To complete the proof we need to show that $\mathcal{E}$ is perfectly reversible upon input of ρ if and only if the first inequality in the quantum data processing inequality is satisfied with equality,

$$S(\rho) = I(\rho, \mathcal{E}) = S(\rho') - S(\rho, \mathcal{E}) \tag{12.132}$$

To prove the necessity of this condition for reversal, suppose that $\mathcal{E}$ is perfectly reversible upon input of ρ, with reversal operation $\mathcal{R}$. From the second stage of the quantum data processing inequality it follows that

$$S(\rho') - S(\rho, \mathcal{E}) \geq S(\rho'') - S(\rho, \mathcal{R} \circ \mathcal{E}) \tag{12.133}$$

From the reversibility requirement it follows that $\rho'' = \rho$. Furthermore, from the quantum Fano inequality (12.112) and the perfect reversibility requirement $F(\rho, \mathcal{R} \circ \mathcal{E}) = 1$ it follows that $S(\rho, \mathcal{R} \circ \mathcal{E}) = 0$. Thus the second stage of the quantum data processing inequality when applied to $\rho \to \mathcal{E}(\rho) \to (\mathcal{R} \circ \mathcal{E})(\rho)$ may be rewritten

$$S(\rho') - S(\rho, \mathcal{E}) \geq S(\rho) \tag{12.134}$$

Combining this with the first part of the quantum data processing inequality, $S(\rho) \geq S(\rho') - S(\rho, \mathcal{E})$, we deduce that

$$S(\rho') = S(\rho) - S(\rho, \mathcal{E}) \tag{12.135}$$

for any $\mathcal{E}$ which is perfectly reversible upon input of ρ.
Next, we give a constructive proof that satisfaction of the condition

$$S(\rho) = S(\rho') - S(\rho, \mathcal{E}) \tag{12.136}$$

implies that the quantum operation $\mathcal{E}$ is reversible upon input of ρ. Noting that $S(\rho) = S(Q) = S(R) = S(R'), S(\rho') = S(Q') = S(R', E')$ and $S(\rho, \mathcal{E}) = S(E')$, we see that $S(R') + S(E') = S(R', E')$, which we saw in Section 11.3.4 is equivalent to the condition that $\rho^{R'E'} = \rho^{R'} \otimes \rho^{E'}$. Suppose the initial state of Q is $\rho = \sum_i p_i |i\rangle\langle i|$, and that we purify this state into RQ as $|RQ\rangle = \sum_i \sqrt{p_i}|i\rangle|i\rangle$, where the first system is R and the second system is Q. Note that $\rho^{R'} = \rho^R = \sum_i p_i |i\rangle\langle i|$. Furthermore, suppose that $\rho^{E'} = \sum_j q_j |j\rangle\langle j|$ for some orthonormal set $|j\rangle$, so that

$$\rho^{R'E'} = \sum_{ij} p_i q_j |i\rangle\langle i| \otimes |j\rangle\langle j|. \tag{12.137}$$

This has eigenvectors $|i\rangle|j\rangle$ so by the Schmidt decomposition we may write the total state of $R'Q'E'$ after the quantum operation $\mathcal{E}$ has been applied as

$$|R'Q'E'\rangle = \sum_{ij} \sqrt{p_i q_j}|i\rangle|i,j\rangle|j\rangle \tag{12.138}$$

where $|i,j\rangle$ is some orthonormal set of states for system Q. Define projectors P_j by $P_j \equiv \sum_i |i,j\rangle\langle i,j|$. The idea of the restoration operation is to first perform a measurement described by the projectors P_j, which reveals the state $|j\rangle$ of the environment, and then do a unitary rotation U_j conditional on j which restores the state $|i,j\rangle$ to $|i\rangle : U_j|i,j\rangle \equiv |i\rangle$.

That is, j is the measurement syndrome, and U_j the corresponding recovery operation. The complete recovery operation may be written

$$\mathcal{R}(\sigma) \equiv \sum_j U_j P_j \sigma P_j U_j^\dagger \tag{12.139}$$

The projectors P_j are orthogonal, by the orthogonality of the states $|i,j\rangle$, but may not be complete. If this is the case, then to ensure that the quantum operation $\mathcal{R}$ is tracepreserving, it is necessary to add an extra projector $\tilde{P} \equiv I - \sum_j P_j$ to the set of projectors to make the operation trace-preserving.

The final state of the system RQE after the reversal operation is given by

$$\begin{aligned}
&\sum_j U_j P_j \left|R'Q'E'\right\rangle \left\langle R'Q'E'\right| P_j U_j^\dagger \\
&\qquad = \sum_j \sum_{i_1 i_2} \sqrt{p_{i_1} p_{i_2}} q_j \left|i_1\right\rangle \left\langle i_2\right| \otimes \left(U_j \left|i_1, j\right\rangle \left\langle i_2, j\right| U_j^\dagger\right) \otimes |j\rangle\langle j| \qquad (12.140) \\
&\qquad = \sum_{i_1, i_2} \sqrt{p_{i_1} p_{i_2}} \left|i_1\right\rangle \left\langle i_2\right| \otimes \left|i_1\right\rangle \left\langle i_2\right| \otimes \rho^{E'}, \qquad (12.141)
\end{aligned}$$

from which we see that $\rho^{R''Q''} = \rho^{RQ}$, and thus $F(\rho, \mathcal{R} \circ \mathcal{E}) = 1$, that is, the operation $\mathcal{E}$ is perfectly reversible upon input of the state ρ, as we desired to show.

This completes the proof of the information-theoretic reversibility conditions for tracepreserving quantum operations. Intuition about the result may be obtained by imagining that Q

is a memory element in a quantum computer, R is the remainder of the quantum computer, and E is an environment whose interaction with Q causes noise. The information-theoretic reversibility condition is most elegantly understood as the statement that the state of the environment E' after the noise has occurred should not be correlated with the state of the remainder of the quantum computer, R'. To state it in more anthropomorphic terms, error-correction is possible precisely when the environment does not learn anything about the remainder of the quantum computer through interacting with Q !

Even more concretely, suppose Q is an n qubit system and C is an $[n, k]$ quantum error-correcting code living in the system Q with orthonormal codewords $|x\rangle$ and projector P onto the codespace. Consider the density matrix $P/2^k$, which may be purified to a pure state of RQ :

$$\frac{1}{\sqrt{2^k}} \sum_x |x\rangle |x\rangle. \tag{12.142}$$

Imagine this code is able to correct arbitrary errors on some subset Q_1 of the qubits. Then, in particular, it must be able to correct that error which simply swaps those qubits out into the environment and replaces them with some standard state. The informationtheoretic reversibility condition that $\rho^{R'E'} = \rho^{R'} \otimes \rho^{E'}$ can in this case be rephrased as the condition $\rho^{RQ_1} = \rho^R \otimes \rho^{Q_1}$. Thus the reference system R and subsystem Q_1 on which errors can be corrected must initially be uncorrelated if correction is to be possible!

Exercise 12.14: Show that the condition $\rho^{RQ_1} = \rho^R \otimes \rho^{Q_1}$ is also sufficient to be able to correct errors on the subsystem Q_1.

The reasoning used in the proof of the quantum data processing inequality can be adapted to prove a wide variety of other inequalities. For example, suppose we have a quantum system Q in a state ρ that is subjected to the quantum operation $\mathcal{E}$. The first stage of the data processing inequality follows by applying the subadditivity inequality for entropy to the systems $R'E'$. What if instead we applied the subadditivity inequality to the systems $Q'E'$, obtaining

$$S(\rho) = S(R) = S\left(R'\right) = S\left(Q', E'\right) \leq S\left(Q'\right) + S\left(E'\right) = S(\mathcal{E}(\rho)) + S(\rho, \mathcal{E}) \tag{12.143}$$

That is,

$$\Delta S + S(\rho, \mathcal{E}) \geq 0 \tag{12.144}$$

where $\Delta S \equiv S(\mathcal{E}(\rho)) - S(\rho)$ is the change in entropy caused by the process $\mathcal{E}$. Loosely speaking, this inequality says that the change in entropy of the system plus the change in entropy of the environment must be non-negative, an eminently reasonable statement in accord with the second law of thermodynamics, and one which will aid us in Section 12.4.4 in our thermodynamic analysis of quantum error-correction!

Exercise 12.15: Apply all possible combinations of the subadditivity and strong subadditivity inequalities to deduce other inequalities for the two stage quantum process $\rho \to \rho' = \mathcal{E}_1(\rho) \to \rho'' = \left(\mathcal{E}_2 \circ \mathcal{E}_1\right)(\rho)$, expressing the results whenever possible in terms of entropy exchanges and the entropies $S(\rho), S\left(\rho'\right), S\left(\rho''\right)$. When it is not possible to express a quantity appearing in such an inequality in these terms, give a prescription for calculating the quantity using only a knowledge of ρ and operation elements $\{E_j\}$ for $\mathcal{E}_1$ and $\{F_k\}$ for $\mathcal{E}_2$.

9.5.13 12.4.3 Quantum Singleton bound

The information-theoretic approach to quantum error-correction can be used to prove a beautiful bound on the ability of quantum error-correcting codes to correct errors, the quantum

Singleton bound. Recall that an $[n, k, d]$ code uses n qubits to encode k qubits, and is able to correct located errors (Exercise 10.45) on up to $d-1$ of the qubits. The quantum Singleton bound states that we must have $n-k \geq 2(d-1)$. Contrast this with the classical Singleton bound, Exercise 10.21 on page 449, which states that for an $[n, k, d]$ classical code we must have $n-k \geq d-1$. Because a quantum code to correct errors on up to t qubits must have distance at least $2t+1$ it follows that $n-k \geq 4t$. Thus, for example, a code to encode $k=1$ qubits and capable of correcting errors on $t=1$ of the qubits must satisfy $n-1 \geq 4$, that is, n must be at least 5 , so the five qubit code described in Chapter 10 is the smallest possible code for this task.

The proof of the quantum Singleton bound is an extension of the information-theoretic techniques we have been using to analyze quantum error-correction. Suppose the code is a 2^k-dimensional subspace associated with the system Q, with orthonormal basis denoted by $|x\rangle$. Introduce a 2^k-dimensional reference system R also with 2^k orthonormal basis vectors denoted $|x\rangle$, and consider the entangled state of RQ,

$$|RQ\rangle = \frac{1}{\sqrt{2^k}} \sum_x |x\rangle |x\rangle \tag{12.145}$$

We divide the n qubits of Q up into three disjoint blocks, the first and second, Q_1 and Q_2, consisting of $d-1$ qubits each, and the third Q_3 consisting of the remaining $n-2(d-1)$ qubits. Because the code has distance d any set of $d-1$ located errors may be corrected, and thus it is possible to correct errors on either Q_1 or Q_2. It follows that R and Q_1 must be uncorrelated, as are R and Q_2. By this observation, the overall purity of the state of $RQ_1Q_2Q_3$, and the subadditivity of entropy we have:

$$S(R) + S(Q_1) = S(R, Q_1) = S(Q_2, Q_3) \leq S(Q_2) + S(Q_3) \tag{12.146}$$

$$S(R) + S(Q_2) = S(R, Q_2) = S(Q_1, Q_3) \leq S(Q_1) + S(Q_3). \tag{12.147}$$

Adding these two inequalities gives

$$2S(R) + S(Q_1) + S(Q_2) \leq S(Q_1) + S(Q_2) + 2S(Q_3) \tag{12.148}$$

Canceling terms and substituting $S(R) = k$ gives $k \leq S(Q_3)$. But Q_3 is $n-2(d-1)$ qubits in size, so $S(Q_3) \leq n-2(d-1)$, giving $k \leq n-2(d-1)$, whence $2(d-1) \leq n-k$, the quantum Singleton bound.

As an example of the quantum Singleton bound in action, consider the depolarizing channel $\mathcal{E}(\rho) = p\rho + (1-p)/3(X\rho X + Y\rho Y + Z\rho Z)$. Suppose the depolarizing channel acts independently on a large number n of qubits. If $p < 3/4$ then more than one quarter of those qubits will suffer errors, so any code capable of recovering from the errors must have $t > n/4$. But the quantum Singleton bound implies that $n-k \geq 4t > n$, and thus k must be negative, that is, it is not possible to encode any qubits at all in this case. Thus, when $p < 3/4$, the quantum Singleton bound implies that the capacity of the depolarizing channel for quantum information is zero!

9.5.14 12.4.4 Quantum error-correction, refrigeration and Maxwell's demon

Quantum error-correction may be thought of as a type of refrigeration process, capable of keeping a quantum system at a constant entropy, despite the influence of noise processes which tend to change the entropy of the system. Indeed, quantum error-correction may even appear rather puzzling from this point of view, as it appears to allow a reduction in entropy of the quantum system in apparent violation of the second law of thermodynamics! To understand

why there is no violation of the second law we do an analysis of quantum error-correction similar to that used to analyze Maxwell's demon in Box 3.5 on page 162. Quantum error-correction is essentially a special type of Maxwell's demon we can imagine a 'demon' performing syndrome measurements on the quantum system, and then correcting errors according to the result of the syndrome measurement. Just as in the analysis of the classical Maxwell's demon, the storage of the syndrome in the demon's memory carries with it a thermodynamic cost, in accordance with Landauer's principle. In particular, because any memory is finite, the demon must eventually begin erasing information from its memory, in order to have space for new measurement results. Landauer's principle states that erasing one bit of information from the memory increases the total entropy of the system - quantum system, demon, and environment by at least one bit.

Rather more precisely, we can consider a four-stage error-correction 'cycle' as depicted in Figure 12.9:
(1) The system, starting in a state ρ, is subjected to a noisy quantum evolution that takes it to a state ρ'. In typical scenarios for error-correction, we are interested in cases where the entropy of the system increases, $S(\rho') > S(\rho)$, although this is not necessary.
(2) A demon performs a (syndrome) measurement on the state ρ' described by measurement operators $\{M_m\}$, obtaining result m with probability $p_m = \mathrm{tr}\left(M_m \rho' M_m^\dagger\right)$, resulting in the posterior state $\rho'_m = M_m \rho' M_m^\dagger / p_m$.
(3) The demon applies a unitary operation V_m (the recovery operation) that creates a final system state

$$\rho''_m = V_m \rho'_m V_m^\dagger = \frac{V_m M_m \rho' M_m^\dagger V_m^\dagger}{p_m} \tag{12.149}$$

(4) The cycle is restarted. In order that this actually be a cycle and that it be a successful error-correction, we must have $\rho''_m = \rho$ for each measurement outcome m.

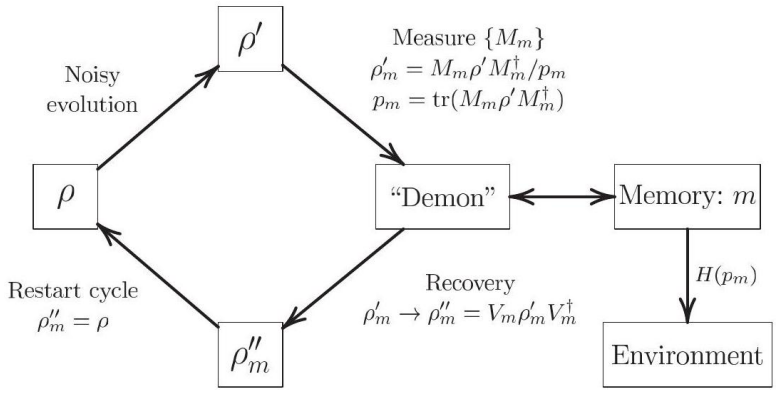


Figure 12.9. The quantum error-correction cycle.

We now show that any reduction in entropy during the second and third stages - the error-correction stages - comes at the expense of entropy production in the environment which is at least as large as the entropy reduction in the quantum system being errorcorrected. After the third stage the only record of the measurement result m is the record kept in the demon's memory. To reset its memory for the next cycle, the demon must erase its record of the measurement result, causing a net increase in the entropy of the environment by Landauer's principle. The number of bits that must be erased is determined by the representation the demon uses to store the measurement result m; by Shannon's noiseless channel coding theorem, at least $H(p_m)$ bits are required, on average, to store the measurement result, and thus a single error-correction cycle on average involves the dissipation of $H(p_m)$ bits of entropy into the environment when the measurement record is erased.

Before error-correction the state of the quantum system is ρ'. After error-correction the state of the quantum system is ρ, so the net change in entropy of the system due to the error-correction is $\Delta S \equiv S(\rho) - S(\rho')$. There is an additional entropic cost of $H(p_m)$ (on average) associated with erasing the measurement record, for a total cost of $\Delta(S) + H(p_m)$. Our goal is to bound this thermodynamic cost, and in so doing demonstrate that the second law of thermodynamics is never violated. To do so, it helps to introduce two items of notation: let $\mathcal{E}$ represent the noise process occurring during stage 1 of the error-correction cycle, $\rho \rightarrow \rho' = \mathcal{E}(\rho)$, and let $\mathcal{R}$ be the quantum operation representing
the error-correction operation,

$$\mathcal{R}(\sigma) \equiv \sum_m V_m M_m \sigma M_m^\dagger V_m^\dagger \tag{12.150}$$

With input ρ' the w-matrix for this process has elements $W_{mn} = \mathrm{tr}\left(V_m M_m \rho' M_n^\dagger V_n^\dagger\right)$, and thus has diagonal elements $W_{mm} = \mathrm{tr}\left(V_m M_m \rho' M_m^\dagger V_m^\dagger\right) = \mathrm{tr}\left(M_m \rho' M_m^\dagger\right)$, which is just the probability p_m the demon obtains measurement outcome m when measuring the error syndrome. By Theorem 11.9 on page 515 the entropy of the diagonal elements of W is at least as great as the entropy of W, so

$$H(p_m) \geq S(W) = S(\rho', \mathcal{R}), \tag{12.151}$$

with equality if and only if the operators $V_m M_m$ are a canonical decomposition of $\mathcal{R}$ with respect to ρ' so that the off-diagonal terms in W vanish. By Equation (12.144) on page 568 it follows that

$$\Delta S + S(\rho', \mathcal{R}) = S(\rho) - S(\rho') + S(\rho', \mathcal{R}) \geq 0. \tag{12.152}$$

Combining this result with (12.151) we deduce that $\Delta S + H(p_m) \geq 0$. But $\Delta S + H(p_m)$ was the total entropy change caused by the error-correction procedure. We conclude that error-correction can only ever result in a net increase in total entropy, with any decrease in system entropy due to error-correction being paid for with entropy production when the error syndrome produced during error-correction is erased.

Exercise 12.16: Show that in the case where $\mathcal{R}$ perfectly corrects $\mathcal{E}$ for the input ρ, the inequality

$$S(\rho) - S(\rho') + S(\rho', \mathcal{R}) \geq 0 \tag{12.153}$$

must actually be satisfied with equality.

9.5.15 12.5 Entanglement as a physical resource

Thus far our study of quantum information has been focused on resources that are not too far distant from the resources considered in classical information theory. For your convenience Figure 12.10 summarizes many of these results in both their quantum and classical guises. One of the delights of quantum computation and quantum information is that quantum mechanics also contains essentially new types of resource that differ vastly from the sort of resource traditionally regarded as information in classical information theory. Perhaps the best understood of these is quantum entanglement, and it is to this resource that we now turn.

We say 'best understood', but that is not saying a whole lot! We are a long way from having a general theory of quantum entanglement. Nevertheless, some encouraging progress towards such a general theory has been made, revealing an intriguing structure to the entangled states, and some quite remarkable connections between the properties of noisy quantum channels and various types of entanglement transformation. We are just going to take a quick peek at what

is known, focusing on the transformation properties of entanglement distributed between two systems ('bi-partite' entanglement), Alice and Bob. There is, of course, a great deal of interest in developing a general theory of entanglement for multi-partite systems, but how to do this is not well understood.

Information Theory

Classical

Shannon entropy

$$H(X) = -\sum_x p(x) \log p(x)$$

Quantum

von Neumann entropy

$$S(\rho) = -\operatorname{tr}(\rho \log \rho)$$

Distinguishability and accessible information

Letters always distinguishable
$N = |X|$
Holevo bound

$$H(X:Y) \leq S(\rho) - \sum_x p_x S\left(\rho_x\right)$$

$$\rho = \sum_x p_x \rho_x$$

Noiseless channel coding

Shannon's theorem

$$n_{\text{bits}} = H(X)$$

Schumacher's theorem

$$n_{\text{qubits}} = S\left(\sum_x p_x \rho_x\right)$$

Capacity of noisy channels for classical information
Shannon's noisy coding theorem

$$C(\mathcal{N}) = \max_{p(x)} H(X:Y)$$

Holevo-Schumacher-Westmoreland theorem

$$C^{(1)}(\mathcal{E}) = \max_{\{p_x, \rho_x\}} \left[S\left(\rho'\right) - \sum_x p_x S\left(\rho'_x\right)\right]$$
$$\rho'_x = \mathcal{E}\left(\rho_x\right), \quad \rho' = \sum_x p_x \rho'_x$$

Information-theoretic relations

Fano inequality

$$H(p_e) + p_e \log(|X| - 1) \geq H(X \mid Y)$$

Mutual information

$$H(X : Y) = H(Y) - H(Y \mid X)$$

Data processing inequality

$$X \to Y \to Z$$
$$H(X) \geq H(X : Y) \geq H(X : Z)$$

Quantum Fano inequality

$$H(F(\rho, \mathcal{E})) + (1 - F(\rho, \mathcal{E})) \log\left(d^2 - 1\right) \geq S(\rho, \mathcal{E})$$

Coherent information

$$I(\rho, \mathcal{E}) = S(\mathcal{E}(\rho)) - S(\rho, \mathcal{E})$$

Quantum data processing inequality

$$\rho \to \mathcal{E}_1(\rho) \to (\mathcal{E}_2 \circ \mathcal{E}_1)(\rho)$$
$$S(\rho) \geq I(\rho, \mathcal{E}_1) \geq I(\rho, \mathcal{E}_2 \circ \mathcal{E}_1)$$

Figure 12.10. Summary of some important classical information relations, and quantum analogues of those relations.

9.5.16 12.5.1 Transforming bi-partite pure state entanglement

The starting point for our investigation is the following simple question: given that Alice and Bob share an entangled pure state $|\psi\rangle$, into what other types of entanglement $|\varphi\rangle$ may they transform $|\psi\rangle$, given that they can each perform arbitrary operations on their local systems, including measurement, but can only communicate using classical communication? No quantum communication between Alice and Bob is allowed, constraining the class of transformations they may achieve.

As an example, imagine that Alice and Bob share an entangled pair of qubits in the Bell state $(|00\rangle + |11\rangle)/\sqrt{2}$. Alice performs a two outcome measurement described by measurement operators M_1 and M_2 :

$$M_1 = \begin{bmatrix} \cos\theta & 0 \\ 0 & \sin\theta \end{bmatrix}; \quad M_2 = \begin{bmatrix} \sin\theta & 0 \\ 0 & \cos\theta \end{bmatrix}. \tag{12.154}$$

After the measurement the state is either $\cos\theta|00\rangle + \sin\theta|11\rangle$ or $\cos\theta|11\rangle + \sin\theta|00\rangle$, depending on the measurement outcome, 1 or 2 . In the latter case, Alice applies a not gate after the measurement, resulting in the state $\cos\theta|01\rangle + \sin\theta|10\rangle$. She then sends the measurement result (1 or 2) to Bob, who does nothing to the state if the measurement result is 1 , and performs a NOT gate if the result is 2 . The final state of the joint system is therefore $\cos\theta|11\rangle + \sin\theta|00\rangle$, regardless of the measurement outcome obtained by Alice. That is, Alice and Bob have transformed their initial entangled resource $(|00\rangle + |11\rangle)/\sqrt{2}$ into the state $\cos\theta|00\rangle + \sin\theta|11\rangle$ using only local operations on their individual systems, and classical communication.

It is perhaps not immediately obvious what is the significance of the problem of entanglement transformation. There is a certain intrinsic interest to the class of transformations we are allowing - local operations and classical communication (LOCC) - however, it is by no means clear a priori that this is truly an interesting problem. It turns out, however, that generalizations of this entanglement transformation problem exhibit deep and unexpected connections to quantum error-correction. Furthermore, the techniques introduced in the solution to the problem are of quite considerable interest, and give unexpected insight into the properties of entanglement. In particular, we will discover a close connection between entanglement and the theory of majorization, an area of mathematics that actually predates quantum mechanics!

Before jumping into the study of entanglement transformation, let's first acquaint ourselves with a few relevant facts about majorization. Majorization is an ordering on d-dimensional real vectors intended to capture the notion that one vector is more or less disordered than another. More precisely, suppose $x = (x_1, \ldots, x_d)$ and $y = (y_1, \ldots, y_d)$ are two d-dimensional vectors. We use the notation $x^{\downarrow}$ to mean x re-ordered so the components are in decreasing order so, for example, $x_1^{\downarrow}$ is the largest component of x. We say x is majorized by y, written $x \prec y$, if $\sum_{j=1}^{k} x_j^{\downarrow} \leq \sum_{j=1}^{k} y_j^{\downarrow}$ for $k = 1, \ldots, d$, with equality instead of inequality when $k = d$. What this definition has to do with notions of disorder will become clear shortly!

The connection between majorization and entanglement transformation is easily stated yet rather surprising. Suppose $|\psi\rangle$ and $|\varphi\rangle$ are states of the joint Alice-Bob system. Define $\rho_\psi \equiv \mathrm{tr}_B(|\psi\rangle\langle\psi|), \rho_\varphi \equiv \mathrm{tr}_B(|\varphi\rangle\langle\varphi|)$ to be the corresponding reduced density matrices of Alice's system, and let λ_ψ and λ_φ be the vectors whose entries are the eigenvalues of ρ_ψ and ρ_φ. We will show that $|\psi\rangle$ may be transformed to $|\varphi\rangle$ by LOCC if and only if $\lambda_\psi \prec \lambda_\varphi$! To demonstrate this we need first a few simple facts about majorization.

Exercise 12.17: Show that $x \prec y$ if and only if for all real t, $\sum_{j=1}^{d} \max(x_j - t, 0) \leq \sum_{j=1}^{d} \max(y_j - t, 0)$, and $\sum_{j=1}^{d} x_j = \sum_{j=1}^{d} y_j$.

Exercise 12.18: Use the previous exercise to show that the set of x such that $x \prec y$ is convex.

The following proposition gives a more intuitive meaning to the notion of majorization, showing that $x \prec y$ if and only if x can be written as a convex combination of permutations of y. Intuitively, therefore, $x \prec y$ if x is more disordered than y in the sense that x can be obtained by permuting the elements of y and mixing the resulting vectors. This representation theorem is one of the most useful results in the study of majorization.

Proposition 12.11: $x \prec y$ if and only if $x = \sum_j p_j P_j y$ for some probability distribution p_j and permutation matrices P_j.

Proof

Suppose $x \prec y$. Without loss of generality we may suppose $x = x^{\downarrow}$ and $y = y^{\downarrow}$. We will prove that $x = \sum_j p_j P_j y$ by induction on the dimension d. For $d = 1$ the result is clear. Suppose x and y are $d+1$-dimensional vectors such that $x \prec y$. Then $x_1 \leq y_1$. Choose j such that $y_j \leq x_1 \leq y_{j-1}$, and define t in the range $[0, 1]$ such that $x_1 = t y_1 + (1-t) y_j$. Define a convex combination of permutations $D \equiv tI + (1-t)T$, where T is the permutation matrix which transposes the 1st and j th matrix elements. Then

$$Dy = (x_1, y_2, \ldots, y_{j-1}, (1-t)y_1 + t y_j, y_{j+1}, \ldots, y_{d+1}) \tag{12.155}$$

Define $x' \equiv (x_2, \ldots, x_{d+1})$ and $y' \equiv (y_2, \ldots, y_{j-1}, (1-t)y_1 + t y_j, y_{j+1}, \ldots, y_{d+1})$. In Exercise 12.19 on this page you show $x' \prec y'$, so by the inductive hypothesis $x' = \sum_j p'_j P'_j y'$ for probabilities p'_j and permutation matrices P'_j, whence $x = \left(\sum_j p'_j P'_j\right) Dy$, where the P'_j are extended to $d+1$ dimensions by acting trivially on the first entry. Since $D = (tI + (1-t)T)$, and a product of permutation matrices is a permutation matrix, the result follows.

Exercise 12.19: Verify that $x' \prec y'$.

Conversely, suppose $x = \sum_j p_j P_j y$. It is clear that $P_j y \prec y$ and by Exercise 12.18 it follows that $x = \sum_j p_j P_j y \prec y$.

Matrices which are convex combinations of permutation matrices have many interesting properties. Notice, for example, that the entries of such a matrix must be non-negative, and that each of the rows and columns must sum to one. A matrix with these properties is known as a doubly stochastic matrix, and there is a result known as Birkhoff's theorem which implies that the doubly stochastic matrices correspond exactly to the set of matrices which can be written as convex combinations of permutation matrices. We won't prove Birkhoff's theorem here (see the end of chapter 'History and further reading'), but merely state it:

Theorem 12.12: (Birkhoff's theorem) A d by d matrix D is doubly stochastic (that is, has non-negative entries and each row and column sums to 1) if and only if D can be written as a convex combination of permutation matrices, $D = \sum_j p_j P_j$.

From Birkhoff's theorem and Proposition 12.11 it follows that $x \prec y$ if and only if $x = Dy$ for some doubly stochastic D. This result allows us to prove a striking and useful operator generalization of Proposition 12.11. Suppose H and K are two Hermitian operators. Then we say $H \prec K$ if $\lambda(H) \prec \lambda(K)$, where we use $\lambda(H)$ to denote the vector of eigenvalues of a Hermitian operator H. Then we have:

Theorem 12.13: Let H and K be Hermitian operators. Then $H \prec K$ if and only if there is a probability distribution p_j and unitary matrices U_j such that

$$H = \sum_j p_j U_j K U_j^\dagger. \tag{12.156}$$

Proof

Suppose $H \prec K$. Then $\lambda(H) = \sum_j p_j P_j \lambda(K)$ by Proposition 12.11. Let $\Lambda(H)$ denote the diagonal matrix whose entries are the eigenvalues of H. Then the vector equation $\lambda(H) = \sum_j p_j P_j \lambda(K)$ may be re-expressed as

$$\Lambda(H) = \sum_j p_j P_j \Lambda(K) P_j^\dagger \tag{12.157}$$

But $H = V\Lambda(H)V^\dagger$ and $\Lambda(K) = WKW^\dagger$ for some unitary matrices V and W, giving $H = \sum_j p_j U_j K U_j^\dagger$ where $U_j \equiv V P_j W$ is a unitary matrix, completing the proof in the forward direction.

Conversely, suppose $H = \sum_j p_j U_j K U_j^\dagger$. Similarly to before, this is equivalent to $\Lambda(H) = \sum_j p_j V_j \Lambda(K) V_j^\dagger$ for some unitary matrices V_j. Writing the matrix components of V_j as $V_{j,kl}$, we have:

$$\lambda(H)_k = \sum_{jl} p_j V_{j,kl} \lambda(K)_l V_{j,lk}^\dagger = \sum_{jl} p_j \left|V_{j,kl}\right|^2 \lambda(K)_l. \tag{12.158}$$

Define a matrix D with entries $D_{kl} \equiv \sum_j p_j \left|V_{j,kl}\right|^2$ so we have $\lambda(H) = D\lambda(K)$. The entries of D are non-negative by definition, and the rows and columns of D all sum to one because the rows and columns of the unitary matrices V_j are unit vectors, so D is doubly stochastic and thus $\lambda(H) \prec \lambda(K)$.

We now have in hand all the facts about majorization needed in the study of LOCC transformations of bipartite pure state entanglement. The first step of the argument is to reduce the problem from the study of general protocols, which may involve two way classical communication, to protocols involving only one-way classical communication.

Proposition 12.14: Suppose $|\psi\rangle$ can be transformed to $|\varphi\rangle$ by LOCC. Then this transformation can be achieved by a protocol involving just the following steps: Alice performs a single measurement described by measurement operators M_j, sends the result j to Bob, who performs a unitary operation U_j on his system.

Proof

Without loss of generality we may suppose the protocol consists of Alice performing a measurement, sending the result to Bob, who performs a measurement (whose nature may depend on the information received from Alice), and sends the result back to Alice, who performs a measurement... and so on. The idea of the proof is simply to show that the
effect of any measurement Bob can do may be simulated by Alice (with one small caveat) so all Bob's actions can actually be replaced by actions by Alice! To see that this is the case, imagine Bob performs a measurement with measurement operators M_j on a pure state $|\psi\rangle$. Suppose this pure state has Schmidt decomposition $|\psi\rangle = \sum_l \sqrt{\lambda_l}\,|l_A\rangle\,|l_B\rangle$ and define operators N_j on Alice's system to have a matrix representation with respect to Alice's Schmidt basis which is the same as the matrix representation of Bob's operators M_j with respect to his Schmidt basis. That is, if $M_j = \sum_{kl} M_{j,kl}\,|k_B\rangle\,\langle l_B|$ then we define

$$N_j \equiv \sum_{kl} M_{j,kl}\,|k_A\rangle\,\langle l_A| \tag{12.159}$$

Suppose Bob performs the measurement defined by the measurement operators M_j. Then the post-measurement state is $|\psi_j\rangle \propto M_j|\psi\rangle = \sum_{kl} M_{j,kl}\sqrt{\lambda_l}\,|l_A\rangle\,|k_B\rangle$, with probability $\sum_{kl} \lambda_l\,|M_{j,kl}|^2$. On the other hand, if Alice had measured N_j then the post-measurement state is $|\varphi_j\rangle \propto N_j|\psi\rangle = \sum_{kl} M_{j,kl}\sqrt{\lambda_l}\,|k_A\rangle\,|l_B\rangle$, also with probability $\sum_{kl} \lambda_l\,|M_{j,kl}|^2$. Note furthermore that $|\psi_j\rangle$ and $|\varphi_j\rangle$ are the same states up to interchange of Alice and Bob's systems via the map $|k_A\rangle \leftrightarrow |k_B\rangle$, and therefore must have the same Schmidt components. It follows from Exercise 2.80 on page 111 that there exists a unitary U_j on Alice's system and V_j on Bob's system such that $|\psi_j\rangle = (U_j \otimes V_j)\,|\varphi_j\rangle$. Therefore, Bob performing a measurement described by measurement operators M_j is equivalent to Alice performing the measurement described by measurement operators $U_j N_j$ followed by Bob performing the unitary transformation V_j. Summarizing, a measurement by Bob on a known pure state can be simulated by a measurement by Alice, up to a unitary transformation by Bob.

Imagine then that Alice and Bob engage in a multi-round protocol transforming $|\psi\rangle$ to $|\varphi\rangle$. Without loss of generality, we may suppose that the first round of the protocol consists of Alice performing a measurement and sending the result to Bob. The second round consists of Bob performing a measurement (perhaps with the type of measurement determined by the result of the first) and sending the result to Alice. Instead, however, we can suppose that this measurement is simulated by a measurement performed by Alice, up to a unitary transformation by Bob. Indeed, we can replace all the measurements by Bob and communication from Bob to Alice by measurements by Alice, with a unitary to be done by Bob conditional on Alice's measurement result. Finally, all the measurements performed by Alice can be combined into one single measurement (Exercise 2.57 on page 86), whose result determines a unitary transformation to be performed by Bob; the net effect of this protocol is exactly the same as the original protocol with two-way communication.

Theorem 12.15: A bipartite pure state $|\psi\rangle$ may be transformed to another pure state $|\varphi\rangle$ by LOCC if and only if $\lambda_\psi \prec \lambda_\varphi$.

Proof

Suppose $|\psi\rangle$ may be transformed to $|\varphi\rangle$ by LOCC. By Proposition 12.14 we may assume that the transformation is effected by Alice performing a measurement with measurement operators M_j, then sending the result to Bob, who performs a unitary transformation U_j. From Alice's point of view she starts with the state ρ_ψ and ends with the state ρ_φ regardless of the measurement outcome, so we must have

$$M_j \rho_\psi M_j^\dagger = p_j \rho_\varphi \tag{12.160}$$

where p_j is the probability of outcome j. Polar decomposing $M_j \sqrt{\rho_\psi}$ implies that there exists a unitary V_j such that

$$M_j \sqrt{\rho_\psi} = \sqrt{M_j \rho_\psi M_j^\dagger} V_j = \sqrt{p_j \rho_\varphi} V_j. \tag{12.161}$$

Premultiplying this equation by its adjoint gives

$$\sqrt{\rho_\psi} M_j^\dagger M_j \sqrt{\rho_\psi} = p_j V_j^\dagger \rho_\varphi V_j. \tag{12.162}$$

Summing on j and using the completeness relation $\sum_j M_j^\dagger M_j = I$ gives

$$\rho_\psi = \sum_j p_j V_j^\dagger \rho_\varphi V_j \tag{12.163}$$

whence $\lambda_\psi \prec \lambda_\varphi$ by Theorem 12.13.

The proof of the converse is essentially to run the proof in the forwards direction backwards. Suppose $\lambda_\psi \prec \lambda_\varphi$, so $\rho_\psi \prec \rho_\varphi$ and by Theorem 12.13 there exist probabilities p_j and unitary operators U_j such that $\rho_\psi = \sum_j p_j U_j \rho_\varphi U_j^\dagger$. Assume for now that ρ_ψ is invertible (this assumption is easily removed; see Exercise 12.20) and define operators M_j for Alice's system by

$$M_j \sqrt{\rho_\psi} \equiv \sqrt{p_j \rho_\varphi} U_j^\dagger \tag{12.164}$$

To see that these operators define a measurement we need to check the completeness relation. We have $M_j = \sqrt{p_j \rho_\varphi} U_j^\dagger \rho_\psi^{-1/2}$ and thus

$$\sum_j M_j^\dagger M_j = \rho_\psi^{-1/2} \left(\sum_j p_j U_j \rho_\varphi U_j^\dagger \right) \rho_\psi^{-1/2} = \rho_\psi^{-1/2} \rho_\psi \rho_\psi^{-1/2} = I, \tag{12.165}$$

which is the completeness relation. Suppose Alice performs the measurement described by the operators M_j, obtaining the outcome j and the corresponding state $|\psi_j\rangle \propto M_j |\psi\rangle$. Let ρ_j denote Alice's reduced density matrix corresponding to the state $|\psi_j\rangle$, so

$$\rho_j \propto M_j \rho_\psi M_j^\dagger = p_j \rho_\varphi \tag{12.166}$$

by substitution of (12.164), and thus $\rho_j = \rho_\varphi$. It follows by Exercise 2.81 that Bob may convert $|\psi_j\rangle$ into $|\varphi\rangle$ by application of a suitable unitary transformation V_j.

Exercise 12.20: Show that the assumption that ρ_ψ is invertible may be removed from the proof of the converse part of Theorem 12.15.

Exercise 12.21: (Entanglement catalysis) Suppose Alice and Bob share a pair of four level systems in the state $|\psi\rangle = \sqrt{0.4}|00\rangle + \sqrt{0.4}|11\rangle + \sqrt{0.1}|22\rangle + \sqrt{0.1}|33\rangle$. Show that it is not possible for them to convert this state by LOCC to the state $|\varphi\rangle = \sqrt{0.5}|00\rangle + \sqrt{0.25}|11\rangle + \sqrt{0.25}|22\rangle$. Imagine, however, that a friendly bank is willing to offer them the loan of a catalyst, an entangled pair of qubits in the state $|c\rangle = \sqrt{0.6}|00\rangle + \sqrt{0.4}|11\rangle$. Show that it is possible for Alice and Bob to convert the state $|\psi\rangle|c\rangle$ to $|\varphi\rangle|c\rangle$ by local operations and classical communication, returning the catalyst $|c\rangle$ to the bank after the transformation is complete.

Exercise 12.22: (Entanglement conversion without communication) Suppose Alice and Bob are trying to convert a pure state $|\psi\rangle$ into a pure state $|\varphi\rangle$ using local operations only - no classical communication. Show that this is possible if
and only if $\lambda_\psi \cong \lambda_\varphi \otimes x$, where x is some real vector with non-negative entries summing to 1 , and ' $\cong$ ' means that the vectors on the left and the right have identical non-zero entries.

9.5.17 12.5.2 Entanglement distillation and dilution

Suppose that instead of being supplied with a single copy of a state $|\psi\rangle$ Alice and Bob are supplied with a large number of copies. What types of entanglement transformation can they accomplish with all these copies? We are going to focus on two particular types of entanglement transformation, known as entanglement distillation and entanglement dilution. The idea of entanglement distillation is for Alice and Bob to convert some large number of copies of a known pure state $|\psi\rangle$ into as many copies of the Bell state $(|00\rangle + |11\rangle)/\sqrt{2}$ as possible using local operations and classical communication, requiring not that they succeed exactly, but only with high fidelity. Entanglement dilution is the reverse process of using LOCC to convert a large number of copies of the Bell state $(|00\rangle + |11\rangle)/\sqrt{2}$ into copies of $|\psi\rangle$, again with high fidelity in the limit where a large number of copies of the Bell state are initially available.

What motivates the study of entanglement distillation and dilution? Suppose we take seriously the idea that entanglement is a physical resource and that as such it should be possible to quantify entanglement, much as we quantify other physical resources such as energy or entropy. Suppose we decide to pick the Bell state $(|00\rangle + |11\rangle)/\sqrt{2}$ as our standard unit of entanglement - the basic measure, rather like the standard kilogram or the standard meter. We can associate a measure of entanglement to a quantum state $|\psi\rangle$ in a similar way to the way we associate a mass to an object. Suppose, for instance, that it takes 15 chocolate biscuits of a particular brand to attain a mass equivalent to the standard kilogram; we say that the chocolate biscuits have a mass of 1/15 th of a kilogram. Now, strictly speaking, if the chocolate biscuits had a mass of 1/14.8 kilograms we'd be in a bit of trouble, because no integer number of chocolate biscuits is going to balance the standard kilogram, and it's not so obvious how to define a non-integer number of chocolate biscuits. Fortunately, what we do is notice that 148 chocolate biscuits exactly balances 10 standard kilograms, so the mass of the chocolate biscuits is 10/148 kilograms. But what if the real mass is not 1/14.8 kilograms, but is something even more esoteric, like 1/14.7982... kilograms? Well, we simply go to the limit of balancing a large number m of chocolate biscuits with another large number n of standard kilograms, and declare the mass of a chocolate biscuit to be the limiting ratio n/m as both m and n become very large.

In a similar way, a potential approach to defining the amount of entanglement present in a pure state $|\psi\rangle$ is to imagine that we are given a large number n of Bell states $(|00\rangle + |11\rangle)/\sqrt{2}$, and are asked to produce as many (high-fidelity) copies of $|\psi\rangle$ as possible using local operations and classical communication. If the number of copies of $|\psi\rangle$ that can be produced is m then we define the limiting ratio of n/m to be the entanglement of formation of the state $|\psi\rangle$. Alternately, we might imagine performing the process in reverse, going from m copies of $|\psi\rangle$ to n copies of $(|00\rangle + |11\rangle)/\sqrt{2}$ using LOCC, and defining the limiting ratio n/m to be the distillable entanglement of the state $|\psi\rangle$. It is by no means obvious that these two definitions give the same number for the quantity of entanglement; we will see that for pure states $|\psi\rangle$ the entanglement of formation and the distillable entanglement are in fact exactly the same!

Let's take a look at a simple protocol for entanglement dilution, and another for entanglement distillation. Suppose an entangled state $|\psi\rangle$ has Schmidt decomposition

$$|\psi\rangle = \sum_x \sqrt{p(x)}\, |x_A\rangle\, |x_B\rangle\,. \tag{12.167}$$

We write the squared Schmidt co-efficients $p(x)$ in the form we usually reserve for probability distributions, both because the co-efficients satisfy the usual rules of probability distributions (non-negative and sum to one), and because ideas from probability theory turn out to be useful in understanding entanglement distillation and dilution. The m-fold tensor product $|\psi\rangle^{\otimes m}$ may be written

$$|\psi\rangle^{\otimes m} = \sum_{x_1,x_2,\ldots,x_m} \sqrt{p(x_1)\,p(x_2)\ldots p(x_m)}\,|x_{1A}x_{2A}\ldots x_{mA}\rangle\,|x_{1B}x_{2B}\ldots x_{mB}\rangle\,. \tag{12.168}$$

Suppose that we defined a new quantum state $|\varphi_m\rangle$ by omitting all those terms $x_1,\ldots,x_m$ which are not ϵ-typical, in the sense defined in Section 12.2.1:

$$|\varphi_m\rangle \equiv \sum_{x\in\text{-typical}} \sqrt{p(x_1)\,p(x_2)\ldots p(x_m)}\,|x_{1A}x_{2A}\ldots x_{mA}\rangle\,|x_{1B}x_{2B}\ldots x_{mB}\rangle\,. \tag{12.169}$$

The state $|\varphi_m\rangle$ is not quite a properly normalized quantum state; to normalize it we define $|\varphi'_m\rangle \equiv |\varphi_m\rangle / \sqrt{\langle\varphi_m \mid \varphi_m\rangle}$. By part 1 of the theorem of typical sequences the fidelity $F(|\psi\rangle^{\otimes m}, |\varphi'_m\rangle) \rightarrow 1$ as $m \rightarrow \infty$. Furthermore, by part 2 of the theorem of typical sequences the number of terms in the sum (12.169) is at most $2^{m(H(p(x))+\epsilon)} = 2^{m\left(S\left(\rho_\psi\right)+\epsilon\right)}$, where ρ_ψ is the result of tracing out Bob's part of $|\psi\rangle$.

Suppose then that Alice and Bob are in joint possession of $n = m\left(S\left(\rho_\psi\right)+\epsilon\right)$ Bell states. Alice prepares 'both parts' of $|\varphi'_m\rangle$ locally, and then uses the Bell states shared with Bob to teleport what should be Bob's half of the state $|\varphi'_m\rangle$ over to Bob. In this way, Alice and Bob can dilute their n Bell states to obtain $|\varphi'_m\rangle$, a pretty good approximation to $|\psi\rangle^{\otimes m}$. This entanglement dilution procedure has $n = m\left(S\left(\rho_\psi\right)+\epsilon\right)$, so the ratio n/m tends to $S\left(\rho_\psi\right)+\epsilon$. We may choose ϵ as small as we like, so we conclude that the entanglement of formation for the state $|\psi\rangle$ is no larger than $S\left(\rho_\psi\right)$, since we have just shown that (asymptotically) $S\left(\rho_\psi\right)$ Bell states may be converted into a single copy of $|\psi\rangle$.

An entanglement distillation protocol for converting copies of $|\psi\rangle$ into Bell states also follows along similar lines. Suppose that Alice and Bob are in possession of m copies of $|\psi\rangle$. By performing a measurement onto the ϵ-typical subspace of ρ_ψ Alice may, with high fidelity, convert the state $|\psi\rangle^{\otimes m}$ into the state $|\varphi'_m\rangle$. The largest Schmidt co-efficient appearing in $|\varphi_m\rangle$ is at most $2^{-m\left(S\left(\rho_\psi\right)-\epsilon\right)}$ by the definition of typical sequences. The renormalized state $|\varphi'_m\rangle$ has Schmidt co-efficients at most a factor $1/\sqrt{(1-\delta)}$ larger, since the theorem of typical sequences tells us that $1-\delta$ is a lower bound on the probability that a sequence is ϵ-typical, and may be made arbitrarily close to 1 for sufficiently large m. Thus, the largest eigenvalue of the state $\rho_{\varphi'_m}$ is at most $2^{-m\left(S\left(\rho_\psi\right)-\epsilon\right)}/(1-\delta)$. Suppose we choose any n such that

$$\frac{2^{-m\left(S\left(\rho_\psi\right)-\epsilon\right)}}{1-\delta} \leq 2^{-n}. \tag{12.170}$$

Then the vector of eigenvalues for $\rho_{\varphi'_m}$ is majorized by the vector $(\,2^{-n}, 2^{-n}, \ldots, 2^{-n}\,)$, and thus by Theorem 12.15 the state $|\varphi'_m\rangle$ may be converted to n Bell states by local operations and classical communication. Examining (12.170) we see that this is possible provided $n \approx mS\left(\rho_\psi\right)$, and thus the entanglement of distillation is at least $S\left(\rho_\psi\right)$.

We have exhibited strategies for distilling $|\psi\rangle$ into $S\left(\rho_\psi\right)$ Bell states and for diluting $S\left(\rho_\psi\right)$ Bell states into a copy of $|\psi\rangle$. In fact, it is not very difficult to see that the procedures we have described are really the optimal methods for doing entanglement dilution and distillation! Suppose, for example, that a more efficient protocol for entanglement dilution existed, that could dilute $|\psi\rangle$ into $S > S\left(\rho_\psi\right)$ Bell states. Then starting with $S\left(\rho_\psi\right)$ Bell states Alice and Bob

could produce a copy of $|\psi\rangle$ using the protocol already described, and then use the hypothetical protocol to produce S Bell states. Thus, by local operations and classical communication, Alice and Bob have taken $S(\rho_\psi)$ Bell states and turned them into $S > S(\rho_\psi)$ Bell states! It is not very difficult to convince yourself (and see Exercise 12.24) that increasing the number of Bell states present using local operations and classical communication is not possible, so such a hypothetical dilution protocol can not exist. In a similar way we can see that the procedure for entanglement distillation is optimal. Thus, the entanglement of formation and entanglement of distillation for the state $|\psi\rangle$ are the same, and both equal $S(\rho_\psi)$!

Exercise 12.23: Prove that the procedure for entanglement distillation we have described is optimal.

Exercise 12.24: Recall that the Schmidt number of a bi-partite pure state is the number of non-zero Schmidt components. Prove that the Schmidt number of a pure quantum state cannot be increased by local operations and classical communication. Use this result to argue that the number of Bell states shared between Alice and Bob cannot be increased by local operations and classical communication.

We've learned how to transform Bell states of a bipartite quantum system into copies of another entangled state, $|\psi\rangle$, and back again, in an optimal fashion, motivating us to define the amount of entanglement present in that quantum state to be the number of Bell states into which copies of $|\psi\rangle$ may be inter-converted, that is, $S(\rho_\psi)$. What do we learn from this definition? Below we will see that it is possible to obtain some interesting insights into quantum error-correction by further generalizing the notion of distillable entanglement. Nevertheless, at the time of writing it seems fair to say that the study of entanglement is in its infancy, and it is not yet entirely clear what advances in our understanding of quantum computation and quantum information can be expected as a result of the study of quantitative measures of entanglement. We have a reasonable understanding of the properties of pure states of bi-partite quantum systems, but a very poor understanding of systems containing three or more components, or even of mixed states for bi-partite systems. Developing a better understanding of entanglement and connecting that understanding to topics such as quantum algorithms, quantum error-correction and quantum communication is a major outstanding task of quantum computation and quantum information!

9.5.18 12.5.3 Entanglement distillation and quantum error-correction

We defined entanglement distillation for pure states, but there is no reason that definition cannot be extended to mixed states. More precisely, suppose ρ is a general state of a bi-partite quantum system belonging to Alice and Bob. They are supplied with a large number m of copies of these states, and using local operations and classical communication attempt to convert these states to the largest possible number n of Bell states, with high fidelity. The distillable entanglement $D(\rho)$ of ρ is the limiting value of the ratio n/m
for the best possible distillation protocol; for pure states $|\psi\rangle$ we have already shown that $D(|\psi\rangle) = S(\rho_\psi)$, but we do not yet know how to evaluate $D(\rho)$ for a mixed state.

A considerable number of techniques for doing entanglement distillation have been developed, giving lower bounds on the value for $D(\rho)$ for specific classes of states ρ. We won't review these techniques here (see the end of chapter 'History and further reading'). What we will describe is a fascinating connection between distillable entanglement and quantum error-correction.

Imagine that Alice is attempting to send Bob quantum information through a noisy quantum channel $\mathcal{E}$. We suppose the channel is a qubit channel such as the depolarizing channel, although the same basic ideas adapt easily to non-qubit channels. One method for sending quantum

information through the channel is as follows. Alice prepares a large number m of Bell states, and sends half of each Bell pair through the channel. Suppose the result of applying $\mathcal{E}$ to half a Bell pair is to create the state ρ, so Alice and Bob end up sharing m copies of ρ. Alice and Bob now perform entanglement distillation, producing $mD(\rho)$ Bell pairs. Alice can now prepare an $mD(\rho)$ qubit state and teleport it to Bob using the $mD(\rho)$ Bell pairs which they share.

Thus, entanglement distillation protocols can be used as a type of error-correction for quantum communications channels between two parties Alice and Bob, enabling Alice to reliably send $mD(\rho)$ qubits of information to Bob, where $D(\rho)$ is the distillable entanglement of ρ, the state that results when one half of a Bell pair is sent through the noisy channel $\mathcal{E}$ connecting Alice and Bob.

What is truly remarkable is that this method of communication using entanglement distillation may sometimes work even when conventional quantum error-correction techniques fail. For example, for the depolarizing channel with $p = 3/4$ we saw in Section 12.4.3 that no quantum information may be transmitted through the channel. However, entanglement distillation protocols are known which can produce a non-zero rate of transmission $D(\rho)$ even for this channel! The reason this is possible is because the entanglement distillation protocols allow classical communication back and forth between Alice and Bob, whereas conventional quantum error-correction does not allow any such classical communication.

This example allows us to explain the claim we made way back in Chapter 1, illustrated in Figure 12.11, that there are channels with zero capacity for quantum information which, when one such channel is connecting Alice to Bob, and another connects Bob to Alice, can be used to achieve a net flow of quantum information! The way this is done is very simple and is based on entanglement distillation. Now, in order that entanglement distillation be possible, we need Alice and Bob to be able to communicate classically, so we set aside half the forward uses of the channel, and all the backward uses of the channel to be used for the transmission of classical information used by the distillation protocol; these channels have non-zero rate for classical information transmission by the HSW theorem. The remaining forward uses of the channel are used to transmit halves of Bell pairs from Alice to Bob, with entanglement distillation being used to extract good Bell pairs out of the resulting states, and then teleportation with the good Bell pairs to achieve a net transmission of quantum information, providing yet another vivid demonstration of the remarkable properties of quantum information!

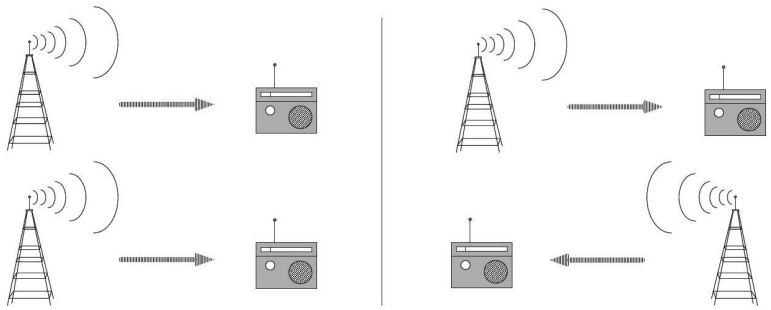


Figure 12.11. Classically, if we have two very noisy channels of zero capacity running side by side, then the combined channel has zero capacity to send information. Not surprisingly, if we reverse the direction of one of the channels, we still have zero capacity to send information. Quantum mechanically, reversing one of the zero capacity channels can actually allow us to send information!

9.5.19 12.6 Quantum cryptography

A fitting conclusion to this chapter is provided by a most remarkable application of quantum information. As we saw in Chapter 5, quantum computers can be used to break some of the best public key cryptosystems. Fortunately, however, what quantum mechanics takes away with one hand, it gives back with the other: a procedure known as quantum cryptography or quantum key distribution exploits the principles of quantum mechanics to enable provably secure distribution of private information. In this section we describe this procedure, and discuss its security. We begin by explaining the basic ideas of a classical technique, private key cryptography, in Section 12.6.1. Private key cryptography is a much older form of cryptography than the public key cryptosystems (mentioned in Chapter 5), and the principles of private key cryptography are used in quantum cryptosystems. Two other important classical techniques, privacy amplification and information reconciliation, which are also used in the quantum systems, are described in Section 12.6.2. Three different protocols for quantum key distribution are then presented in Section 12.6.3. How secure are these protocols? It turns out, as we see in Section 12.6.4, that the coherent information, a measure of quantum information we first encountered in Section 12.4.1, gives an information-theoretic lower bound on the in-principle ability to use a quantum communication channel to send private information! This suggests that ideas of quantum information may be useful in proving the security of specific quantum key distribution protocols, and indeed, they are: we conclude the chapter in Section 12.6.5 with a sketch of how the theory of quantum error-correction provides proof of the security of quantum cryptography.

9.5.20 12.6.1 Private key cryptography

Until the invention of public key cryptography in the 1970s, all cryptosystems operated on a different principle, now known as private key cryptography. In a private key cryptosystem, if Alice wishes to send messages to Bob then Alice must have an encoding key, which allows her to encrypt her message, and Bob must have a matching decoding key, which allows Bob to decrypt the encrypted message. A simple, yet highly effective private key cryptosystem is the Vernam cipher, sometimes called a one time pad. Alice
and Bob begin with n-bit secret key strings, which are identical. Alice encodes her n-bit message by adding the message and key together, and Bob decodes by subtracting to invert the encoding, as illustrated in Figure 12.12.

The great feature of this system is that as long as the key strings are truly secret, it is provably secure. That is, when the protocol used by Alice and Bob succeeds, it does so with arbitrarily high probability (an eavesdropper Eve can always jam the communication channel, but Alice and Bob can detect this jamming and declare failure). And for any eavesdropping strategy employed by Eve, Alice and Bob can guarantee that Eve's mutual information with their unencoded message can be made as small as desired. In contrast, the security of public key cryptography (Appendix 5) relies on unproven mathematical assumptions about the difficulty of solving certain problems like factoring (with classical computers!), even though it is widely used and more convenient.

Original message	Q	U	A	N	T	U
	+	+	+	+	+	+
Encryption key	G	Q	Y	R	W	□
Encrypted message	|| W	"	"	|| F	" Q	"
Received message	W	L	□ Y	□ F	□ Q	□ U
	-	-	____	-	-	-
Decryption key	G	□ Q	Y	□ R	W	A
Decrypted message	|| Q	"U	"A	" N	"T	"U

Figure 12.12. The Vernam cipher. Alice encrypts by adding the random key bits (or in this example, letters of the alphabet) to the original message. Bob decrypts by subtracting the key bits to recover the message.

The major difficulty of private key cryptosystems is secure distribution of key bits. In

particular, the Vernam cipher is secure only as long as the number of key bits is at least as large as the size of the message being encoded, and key bits cannot be reused! Thus, the large amount of key bits needed makes such schemes impractical for general use. Furthermore, key bits must be delivered in advance, guarded assiduously until used, then destroyed afterwards; otherwise, in principle, such classical information can be copied without disturbing the originals, thus compromising the security of the whole protocol. Despite these drawbacks, private key cryptosystems such as the Vernam cipher continue to be used because of their provable security, with key material delivered by clandestine meetings, trusted couriers, or private secured communication links.

Exercise 12.25: Consider a system with n users, any pair of which would like to be able to communicate privately. Using public key cryptography how many keys are required? Using private key cryptography how many keys are required?

9.5.21 12.6.2 Privacy amplification and information reconciliation

The first step in private key cryptography is distribution of the key string. What if Alice and Bob start out with imperfect keys? Specifically, suppose that Alice and Bob share correlated random classical bit strings X and Y, and they also have an upper bound on Eve's mutual information with X and Y. From these imperfect keys, how can they obtain a good enough key to conduct a secure cryptographic protocol? We now show that by performing two steps, information reconciliation, followed by privacy amplification, they can systematically increase the correlation between their key strings, while reducing eavesdropper Eve's mutual information about the result, to any desired level of security. These classical steps will be used in the next section, in the quantum key distribution protocol.

Information reconciliation is nothing more than error-correction conducted over a public channel, which reconciles errors between X and Y to obtain a shared bit string W while divulging as little as possible to Eve. After this procedure, suppose Eve has obtained a random variable Z which is partially correlated with W. Privacy amplification is then used by Alice and Bob to distill from W a smaller set of bits S whose correlation with Z is below a desired threshold. Since this last step is conceptually new, let us consider it first.

A detailed proof of why privacy amplification succeeds is beyond the scope of this book, but we will describe the basic method and present the main theorem. One way to accomplish privacy amplification uses the class of universal hash functions $\mathcal{G}$, which map the set of n-bit strings $\mathcal{A}$ to the set of m-bit strings $\mathcal{B}$, such that for any distinct $a_1, a_2 \in \mathcal{A}$, when g is chosen uniformly at random from $\mathcal{G}$, then the probability that $g(a_1) = g(a_2)$ is at most $1/|\mathcal{B}|$,

The collision entropy of the random variable X with probability distribution $p(x)$ is defined as

$$H_c(X) = -\log\left[\sum_x p(x)^2\right]. \tag{12.171}$$

(This is sometimes known as the Rènyi entropy of order 2.) Using the concavity of the log function, it is not difficult to show that the Shannon entropy provides an upper bound on this quantity: $H(X) \geq H_c(X)$.H_c is important in the following theorem about universal hash functions:

Theorem 12.16: Let X be a random variable on alphabet $\mathcal{X}$ with probability distribution $p(x)$ and collision entropy $H_c(X)$, and let G be the random variable corresponding to the random choice (with uniform distribution) of a member of the universal class of hash functions from $\mathcal{X}$ to $\{0,1\}^m$. Then

$$H(G(X) \mid G) \geq H_c(G(X) \mid G) \geq m - 2^{m-H_c(X)} \tag{12.172}$$

Theorem 12.16 can be applied to privacy amplification in the following manner. Alice and Bob publicly select $g \in \mathcal{G}$ and each apply it to W, giving a new bit string S, which they choose as their secret key. If Eve's uncertainty about W given her knowledge $Z = z$ (about a specific instance of the protocol) is known in terms of the collision entropy to be bounded below by some number, say $H_c(W \mid Z = z) > d$, then it follows from Theorem 12.16 that

$$H_c(S \mid G, Z = z) \geq m - 2^{m-d} \tag{12.173}$$

In other words, m may be chosen small enough such that $H_c(S \mid G, Z = z)$ is nearly equal to m. This maximizes Eve's uncertainty about the key S, making it a secure secret.

Information reconciliation further reduces the number of bits that Alice and Bob can obtain, but this can be bounded as follows. By computing a series of parity checks on subsets of her bits X, Alice can compose a (classical) message u consisting of subset specifications and parities, which, when transmitted to Bob, allows him to correct the errors in his string Y, after which both have the same string W. Clearly, this will require sending $k > H(W \mid Y)$ bits of information in u. However, this procedure gives Eve additional knowledge $U = u$, thus increasing her collision entropy to $H_c(W \mid Z = z, U = u)$. On average (over possible reconciliation messages u), this increase is bounded below by $H_c(W \mid Z = z, U = u) \geq H_c(W \mid Z = z) - H(U)$, where $H(U)$ is the usual Shannon entropy of U, but this bound is too weak, because it implies that the probability that the leaked information $U = u$ decreases H_c by more than $mH(U)$ is only at most $1/m$. A stronger bound is provided by this theorem:

Theorem 12.17: Let X and U be random variables with alphabets $\mathcal{X}$ and $\mathcal{U}$, respectively, where X has probability distribution $p(x)$, and U is jointly distributed with X according to $p(x, u)$. Also let $s > 0$ be an arbitrary parameter. Then, with probability at least $1 - 2^{-s}, U$ takes on a value u for which

$$H_c(X \mid U = u) \geq H_c(X) - 2 \log |\mathcal{U}| - 2s. \tag{12.174}$$

Here, s is known as a security parameter. Applying this to the reconciliation protocol gives the conclusion that Alice and Bob can choose s such that Eve's collision entropy is bounded from below by $H_c(W \mid Z = z, U = u) \geq d - 2(k + s)$, with probability better than $1 - 2^{-s}$. Following this step with privacy amplification allows them to distill m secret key bits S, for which Eve's total information is less than $2^{m-d+2(k+s)}$ bits.

CSS code privacy amplification $^{\mathcal{G}}$ information reconciliation

As we noted above, information reconciliation is nothing more than error-correction; it turns out that privacy amplification is also intimately related to error-correction, and both tasks can be implemented by using classical codes. This viewpoint provides a simple conceptual picture which will be useful in the proof of the security of quantum key distribution, in Section 12.6.5, since we have a well-developed theory of quantum errorcorrection codes. With this in mind, it is useful to observe the following.

Decoding from a randomly chosen CSS code (see Section 10.4.2) can be thought of as performing information reconciliation and privacy amplification. Although CSS codes are usually used to encode quantum information, for our present purpose we can just consider their classical properties. Consider two classical linear codes C_1 and C_2 which satisfy the conditions for a t error-correcting $[n, m]$ CSS code: $C_2 \subset C_1$ and C_1 and $C_2^{\perp}$ both correct t errors. Alice chooses a random n bit string X and transmits it to Bob, who receives Y.

Let us assume that a priori it is known that along a communication channel between Alice and Bob, the expected number of errors per code block caused by all noise sources including eavesdropping is less than t; in practice, this can be established by random testing of the

channel. Furthermore, suppose that Eve knows nothing about the codes C_1 and C_2; this can be ensured by Alice choosing the code randomly. Finally, suppose that Alice and Bob have an upper bound on the mutual information between Eve's data Z, and their own data, X and Y.

Bob receives $Y = X + \epsilon$, where ϵ is some error. Since it is known that less than t errors occurred, if Alice and Bob both correct their states to the nearest codeword in C_1, their results $X', Y' \in C_1$ are identical, $W = X' = Y'$. This step is nothing more than information reconciliation. Of course, Eve's mutual information with W may still be unacceptably large. To reduce this, Alice and Bob identify which of the 2^m cosets of C_2 in C_1 their state W belongs to; that is, that they compute the coset of $W + C_2$ in C_1. The result is their m bit key string, S. By virtue of Eve's lack of knowledge about C_2, and the error-correcting properties of C_2, this procedure can reduce Eve's mutual information with S to an acceptable level, performing privacy amplification.

9.5.22 12.6.3 Quantum key distribution

Quantum key distribution (QKD) is a protocol which is provably secure, by which private key bits can be created between two parties over a public channel. The key bits can then be used to implement a classical private key cryptosystem, to enable the parties to communicate securely. The only requirement for the QKD protocol is that qubits can be communicated over the public channel with an error rate lower than a certain threshold. The security of the resulting key is guaranteed by the properties of quantum information, and thus is conditioned only on fundamental laws of physics being correct!

The basic idea behind QKD is the following fundamental observation: Eve cannot gain any information from the qubits transmitted from Alice to Bob without disturbing their state. First of all, by the no-cloning theorem (Box 12.1), Eve cannot clone Alice's qubit. Second, we have the following proposition:

Proposition 12.18: (Information gain implies disturbance) In any attempt to distinguish between two non-orthogonal quantum states, information gain is only possible at the expense of introducing disturbance to the signal.

Proof

Let $|\psi\rangle$ and $|\varphi\rangle$ be the non-orthogonal quantum states Eve is trying to obtain information about. By the results of Section 8.2, we may assume without loss of generality that the process she uses to obtain information is to unitarily interact the state ($|\psi\rangle$ or $|\varphi\rangle$) with an ancilla prepared in a standard state $|u\rangle$. Assuming that this process does not disturb the states, in the two cases one obtains

$$|\psi\rangle|u\rangle \rightarrow |\psi\rangle|v\rangle \tag{12.175}$$
$$|\varphi\rangle|u\rangle \rightarrow |\varphi\rangle\,|v'\rangle \tag{12.176}$$

Eve would like $|v\rangle$ and $|v'\rangle$ to be different so that she can acquire information about the identity of the state. However, since inner products are preserved under unitary transformations, it must be that

$$\langle v \mid v'\rangle\,\langle\psi \mid \varphi\rangle = \langle u \mid u\rangle\langle\psi \mid \varphi\rangle \tag{12.177}$$
$$\langle v \mid v'\rangle = \langle u \mid u\rangle = 1, \tag{12.178}$$

which implies that $|v\rangle$ and $|v'\rangle$ must be identical. Thus, distinguishing between $|\psi\rangle$ and $|\varphi\rangle$ must inevitably disturb at least one of these states.

We make use of this idea by transmitting non-orthogonal qubit states between Alice and Bob. By checking for disturbance in their transmitted states, they establish an upper bound on any noise or eavesdropping occurring in their communication channel. These 'check' qubits are interspersed randomly among data qubits (from which key bits are later extracted), so that the upper bound applies to the data qubits as well. Alice and Bob then perform information reconciliation and privacy amplification to distill a shared secret key string. The threshold for the maximum tolerable error rate is thus determined by the efficacy of the best information reconciliation and privacy amplification protocols. Three different QKD protocols which work in this way are presented below.

The BB84 protocol

Alice begins with a and b, two strings each of $(4+\delta)n$ random classical bits. She then encodes these strings as a block of $(4+\delta)n$ qubits,

$$|\psi\rangle = \bigotimes_{k=1}^{(4+\delta)n} |\psi_{a_k b_k}\rangle \tag{12.179}$$

where a_k is the k^{th} bit of a (and similarly for b), and each qubit is one of the four states

$$|\psi_{00}\rangle = |0\rangle \tag{12.180}$$
$$|\psi_{10}\rangle = |1\rangle \tag{12.181}$$
$$|\psi_{01}\rangle = |+\rangle = (|0\rangle + |1\rangle)/\sqrt{2} \tag{12.182}$$
$$|\psi_{11}\rangle = |-\rangle = (|0\rangle - |1\rangle)/\sqrt{2} \tag{12.183}$$

The effect of this procedure is to encode a in the basis X or Z, as determined by b. Note that the four states are not all mutually orthogonal, and therefore no measurement can distinguish between (all of) them with certainty. Alice then sends $|\psi\rangle$ to Bob, over their public quantum communication channel.

Bob receives $\mathcal{E}(|\psi\rangle\langle\psi|)$, where $\mathcal{E}$ describes the quantum operation due to the combined effect of the channel and Eve's actions. He then publicly announces this fact. At this point, Alice, Bob, and Eve each have their own states described by separate density matrices. Note also that at this point, since Alice hasn't revealed b, Eve has no knowledge of what basis she should have measured in to eavesdrop on the communication; at best, she can only guess, and if her guess was wrong, then she would have disturbed the state received by Bob. Moreover, whereas in reality the noise $\mathcal{E}$ may be partially due to the environment (a poor channel) in addition to Eve's eavesdropping, it doesn't help Eve to have complete control over the channel, so that she is entirely responsible for $\mathcal{E}$.

Of course, Bob also finds $\mathcal{E}(|\psi\rangle\langle\psi|)$ uninformative at this point, because he does not know anything about b. Nevertheless, he goes ahead and measures each qubit in basis X or Z, as determined by a random $(4+\delta)n$ bit string b' which he creates on his own. Let

Bob's measurement result be a'. After this, Alice publicly announces b, and by discussion over a public channel, Bob and Alice discard all bits in $\{a', a\}$ except those for which corresponding bits of b' and b are equal. Their remaining bits satisfy $a' = a$, since for these bits Bob measured in the same basis Alice prepared in. Note that b reveals nothing about either a, or the bits a' resulting from Bob's measurement, but it is important that Alice not publish b until after Bob announces reception of Alice's qubits. For simplicity in the following explanation, let Alice and Bob keep just $2n$ bits of their result; δ can be chosen sufficiently large so that this can be done with exponentially high probability.

Now Alice and Bob perform some tests to determine how much noise or eavesdropping happened during their communication. Alice selects n bits (of their $2n$ bits) at random, and publicly announces the selection. Bob and Alice then publish and compare the values of these check bits. If more than t bits disagree, then they abort and re-try the protocol from the start. t is selected such that if the test passes, then they can apply information reconciliation and privacy amplification algorithms to obtain m acceptably secret shared key bits from the remaining n bits.

This protocol, known as BB84 after its inventors (see the end of chapter 'History and further reading'), is summarized in Figure 12.13, and an experimental realization is described in Box 12.7. Related versions of this protocol, such as using fewer check bits, are also known by the same name.

The BB84 QKD protocol

1: Alice chooses $(4+\delta)n$ random data bits.
2: Alice chooses a random $(4+\delta)n$-bit string b. She encodes each data bit as $\{|0\rangle, |1\rangle\}$ if the corresponding bit of b is 0 or $\{|+\rangle, |-\rangle\}$ if b is 1 .
3: Alice sends the resulting state to Bob.
4: Bob receives the $(4+\delta)n$ qubits, announces this fact, and measures each qubit in the X or Z basis at random.
5: Alice announces b.
6: Alice and Bob discard any bits where Bob measured a different basis than Alice prepared. With high probability, there are at least $2n$ bits left (if not, abort the protocol). They keep $2n$ bits.
7: Alice selects a subset of n bits that will to serve as a check on Eve's interference, and tells Bob which bits she selected.
8: Alice and Bob announce and compare the values of the n check bits. If more than an acceptable number disagree, they abort the protocol.
9: Alice and Bob perform information reconciliation and privacy amplification on the remaining n bits to obtain m shared key bits.

Figure 12.13. The four state quantum key distribution protocol known as BB84.

Exercise 12.26: Let a'_k be Bob's measurement result of qubit $|\psi_{a_k b_k}\rangle$, assuming a noiseless channel with no eavesdropping. Show that when $b'_k \neq b_k, a'_k$ is random and completely uncorrelated with a_k. But when $b'_k = b_k, a'_k = a_k$.

Exercise 12.27: (Random sampling tests) The random test of n of $2n$ check bits allows Alice and Bob to place an upper bound on the number of errors in their untested bits, with high probability. Specifically, for any $\delta > 0$, the probability of obtaining less than δn errors on the check bits, and more than $(\delta+\epsilon)n$ errors on the remaining n bits is asymptotically less than $\exp\left[-O\left(\epsilon^2 n\right)\right]$, for large n. We prove this claim here.
(1) Without loss of generality, you may assume that there are μn errors in the $2n$ bits, where $0 \leq \mu \leq 2$. Now, if there are δn errors on the check bits, and $(\delta+\epsilon)n$ errors on the rest, then $\delta = (\mu - \epsilon)/2$. The two conditional statements in the claim thus imply the following:

$$\begin{array}{lcl} < \delta n \text{ errors on check bits} & \Rightarrow & < \delta n \text{ errors on check bits} \\ > (\delta+\epsilon)n \text{ errors on rest} & \Rightarrow & > (\mu-\delta)n \text{ errors on rest} \end{array} \tag{12.185}$$

and in fact, the top claim on the right implies the bottom one on the right.
Using this, show that the probability p which we would like to bound satisfies

$$p < \binom{2n}{n}^{-1} \binom{\mu n}{\delta n} \binom{(2-\mu)n}{(1-\delta)n} \delta n. \tag{12.186}$$

(2) Show that for large n, you can bound

$$\frac{1}{an+1}2^{anH(b/a)} \leq \binom{an}{bn} \leq 2^{anH(b/a)} \tag{12.187}$$

where $H(\cdot)$ is the binary entropy function, Equation (11.8). Apply this to the above bound for p.
(3) Apply the bound $H(x) < 1-2(x-1/2)^2$ to obtain the final result, $p < \exp\left[-O\left(\epsilon^2 n\right)\right]$. You may replace μ by a constant which expresses the worst possible case.
(4) Compare the result with the Chernoff bound, Box 3.4. Can you come up with a different way to derive an upper bound on p ?

The B92 protocol

The BB84 protocol can be generalized to use other states and bases, and similar conclusions hold. In fact, a particularly simple protocol exists in which only two states are used. For simplicity, it is sufficient to consider what happens to a single bit at a time; the description easily generalizes to block tests just as is done in BB 84 .

Suppose Alice prepares one random classical bit a, and, depending on the result, sends Bob

$$|\psi\rangle = \begin{cases} |0\rangle & \text{if } a = 0 \\ \frac{|0\rangle+|1\rangle}{\sqrt{2}} & \text{if } a = 1. \end{cases} \tag{12.188}$$

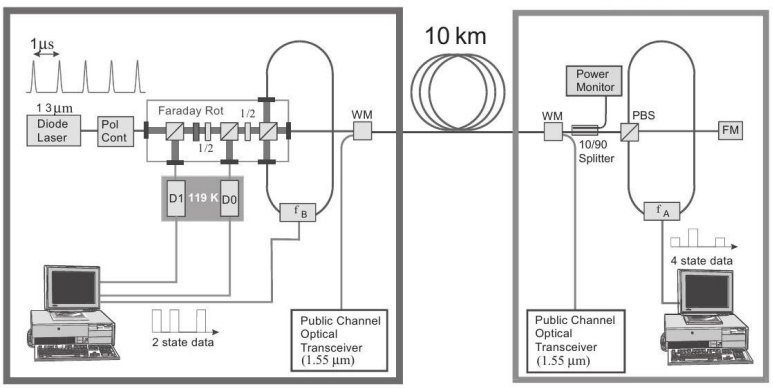
Depending on a random classical bit a' which he generates, Bob subsequently measures the qubit he receives from Alice in either the Z basis $|0\rangle, |1\rangle$ (if $a' = 0$), or in the X basis $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$ (if $a' = 1$). From his measurement, he obtains the result b, which is 0 or 1 , corresponding to the -1 and +1 eigenstates of X and Z. Bob then publicly announces b (but keeps a' secret), and Alice and Bob conduct a public discussion keeping

Box 12.7: Experimental quantum cryptography

Quantum key distribution is particularly interesting and astonishing because it is easily experimentally realized. Here is a schematic diagram of one system employing commercial fiber-optic components to deliver key bits over a ten kilometer distance, which has been built at IBM:

Alice

Bob



Bob initially generates strong coherent states $|\alpha\rangle$ using a diode laser emitting light at a wavelength of 1.3μ m, and transmits them to Alice, who attenuates them to (approximately)

generate a single photon. She also polarizes the photon in one of the four states of the BB84 protocol, using as $|0\rangle$ and $|1\rangle$ states horizontal and vertical polarization. She then returns the photon to Bob, who measures it using a polarization analyzer, in a random basis. By using this special configuration in which the photon traverses the same path twice, the apparatus can be made to autocompensate for imperfections (such as slowly fluctuating path lengths and polarization shifts) along the fiber link. Alice and Bob then select the subset of results in which they used the same basis, reconcile their information, and perform privacy amplification, communicating over a public channel with photons (over the same fiber) of 1.55 μm wavelength. Key bits can be exchanged at the rate of a few hundred per second. Ultimately, improvements in the light source and detector should allow the rate to be improved by a few orders of magnitude. Quantum key distribution over distances exceeding 40 kilometers, and also in installed telecommunication fiber (under Lake Geneva) has been demonstrated.
only those pairs $\{a, a'\}$ for which $b = 1$. Note that when $a = a'$, then $b = 0$ always. Only if $a' = 1 - a$ will Bob obtain $b = 1$, and that occurs with probability 1/2. The final key is a for Alice, and $1 - a'$ for Bob.

This protocol, known as B92 (see the end of chapter 'History and further reading'), highlights how the impossibility of perfect distinction between non-orthogonal states lies at the heart of quantum cryptography. As in BB84, because it is impossible for any eavesdropper to distinguish between Alice's states without disrupting the correlation between the bits Alice and Bob finally keep, this protocol allows Alice and Bob to created shared
key bits while also placing an upper bound on the noise and eavesdropping during their communication. They can then apply information reconciliation and privacy amplification to extract secret bits from their resulting correlated random bit strings.

Exercise 12.28: Show that when $b = 1$, then a and a' are perfectly correlated with each other.

Exercise 12.29: Give a protocol using six states, the eigenstates of X, Y, and Z, and argue why it is also secure. Discuss the sensitivity of this protocol to noise and eavesdropping, in comparison with that of BB 84 and B 92 .

The EPR protocol

The key bits generated in the BB 84 and B 92 protocols may appear to have been originated by Alice. However, it turns out that the key can be seen to arise from a fundamentally random process involving the properties of entanglement. This is illustrated by the following protocol.

Suppose Alice and Bob share a set of n entangled pairs of qubits in the state

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{12.189}$$

These states are known as EPR pairs. Obtaining these states could have come about in many different ways; for example, Alice could prepare the pairs and then send half of each to Bob, or vice versa. Alternatively, a third party could prepare the pairs and send halves to Alice and Bob. Or they could have met a long time ago and shared them, storing them until the present. Alice and Bob then select a random subset of the EPR pairs, and test to see if they violate Bell's inequality (Equation (2.225), on page 115 in Section 2.6), or some other appropriate test of fidelity. Passing the test certifies that they continue to hold sufficiently pure, entangled quantum states, placing a lower bound on the fidelity of the remaining EPR pairs (and thus any noise or eavesdropping). And when they measure these in jointly determined random bases, Alice and Bob obtain correlated classical bit strings from which they can obtain secret key bits as in the B92 and BB84 protocols. Using an argument based on Holevo's bound, the fidelity of their EPR pairs can be used to establish an upper bound on Eve's accessible information about the key bits.

Where do the key bits come from in this EPR protocol? Since it is symmetric - Alice and Bob perform identical tasks on their qubits, even possibly simultaneously - it cannot be said that either Alice or Bob generates the key. Rather, the key is truly random. In fact the same applies to the BB84 protocol, since it can be reduced to an instance of a generalized version of the EPR protocol. Suppose that Alice prepares a random classical bit b, and according to it, measures her half of the EPR pair in either the $|0\rangle, |1\rangle$ basis, or in the basis $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$, obtaining a. Let Bob do identically, measuring in (his randomly chosen) basis b' and obtaining a'. Now they communicate b and b' over a public classical channel, and keep as their key only those $\{a, a'\}$ for which $b = b'$. Note that this key is undetermined until Alice or Bob performs a measurement on their EPR pair half. Similar observations can be made about the B92 protocol. For this reason, quantum cryptography is sometimes thought of not as secret key exchange or transfer, but rather as secret key generation, since fundamentally neither Alice nor Bob can pre-determine the key they will ultimately end up with upon completion of the protocol.

9.5.23 12.6.4 Privacy and coherent information

Thus far, we have described the basic protocol for QKD and argued that it is secure, but we have not provided quantitative bounds. How secure is it? It turns out there is an interesting and fundamental connection between the basic quantitative measures of quantum information discussed in this chapter, and the in-principle obtainable security of quantum cryptography, which we describe below.

The quantum coherent information $I(\rho, \mathcal{E})$ gives a lower bound on the ability of a quantum channel to send private information. In the most general circumstance, Alice prepares states ρ_k^A, where $k = 0, 1, \ldots$ denotes the different possible states she may send, each with some probability p_k. Bob receives states $\rho_k^B = \mathcal{E}\left(\rho_k^A\right)$ which may be different from ρ_k^A because of channel noise or an eavesdropper, Eve. The mutual information between the result of any measurement Bob may do, and Alice's value k, H_{bobalice} , is bounded above by Holevo's bound, (12.6),

$$H_{\text{bob:alice}} \leq \chi^B = S\left(\rho^B\right) - \sum_k p_k S\left(\rho_k^B\right) \tag{12.190}$$

where $\rho^B = \sum_k p_k \rho_k^B$. Similarly, Eve's mutual information is bounded above,

$$H_{\text{eve:alice}} \leq \chi^E = S\left(\rho^E\right) - \sum_k p_k S\left(\rho_k^E\right) \tag{12.191}$$

Since any excess information Bob has relative to Eve (at least above a certain threshold) can in principle be exploited by Bob and Alice to distill a shared secret key using techniques such as privacy amplification, it makes sense to define the quantity

$$\mathcal{P} = \sup\left[H_{\text{bob:alice}} - H_{\text{eve:alice}}\right] \tag{12.192}$$

as the guaranteed privacy of the channel, where the supremum is taken over all strategies Alice and Bob may employ to use the channel. This is the maximum excess classical information that Bob may obtain relative to Eve about Alice's quantum signal. By the HSW theorem, Alice and Bob can employ a strategy such that $H_{\text{bob:alice}} = \chi^B$, while for any strategy Eve may employ, $H_{\text{eve:alice}} \leq \chi^E$. Thus, $\mathcal{P} \geq \chi^B - \chi^E$, for a suitable choice of strategy.

From Exercise 12.11, it follows that a lower bound on the privacy $\mathcal{P}$ can be obtained by assuming that all of Alice's signal states $\rho_k^A = \left|\psi_k^A\right\rangle\left\langle\psi_k^A\right|$ are pure states, which are initially unentangled with Eve, who starts out in some state $\left|0^E\right\rangle$ (that may also be assumed to be pure, without loss of generality). In general, the channel from Alice to Bob will include interactions

with some environment other than Eve, but to give Eve the greatest possible advantage, all such interactions may be attributed to her, such that the final joint state received by Eve and Bob after transmission is

$$\left|\psi^{EB}\right\rangle = U\left|\psi_k^A\right\rangle\left|0^E\right\rangle. \tag{12.193}$$

Since this is a pure state, the reduced density matrices ρ_k^E and ρ_k^B will have the same non-zero eigenvalues, and thus the same entropies, $S\left(\rho_k^E\right) = S\left(\rho_k^B\right)$. Thus,

$$\begin{aligned}
\mathcal{P} &\geq \chi^B - \chi^E && (12.194)\\
&= S\left(\rho^B\right) - \sum_k p_k S\left(\rho_k^B\right) - S\left(\rho^E\right) + \sum_k p_k S\left(\rho_k^E\right) && (12.195)\\
&= S\left(\rho^B\right) - S\left(\rho^E\right) && (12.196)\\
&= I(\rho, \mathcal{E}). && (12.197)
\end{aligned}$$

That is, a lower bound on the guaranteed privacy of the channel $\mathcal{E}$ is given by the quantum coherent information $I(\rho, \mathcal{E})$, as defined in Equation (12.118). Note that this result is not specific to any protocol (which may have its own security flaws). Also, the protocol must perform tests, which are not considered in this calculation, to actually determine properties of the channel $\mathcal{E}$, after which this bound can be applied. So although the information-theoretic bound we have arrived at here is quite elegant, we still have a way to go before being able to quantify the security of QKD!

9.5.24 12.6.5 The security of quantum key distribution

How secure is quantum key distribution? Because of the inevitability of disturbance of the communicated state, upon information gain by an eavesdropper, we have good reason to believe in the security of QKD. What we need, however, to conclude that the protocol truly is secure, is a quantifiable definition of security which explicitly bounds Eve's knowledge about the final key, given some measure of Alice and Bob's effort. The following criterion is acceptable:

> A QKD protocol is defined as being secure if, for any security parameters $s > 0$ and $\ell > 0$ chosen by Alice and Bob, and for any eavesdropping strategy, either the scheme aborts, or it succeeds with probability at least $1 - O\left(2^{-s}\right)$, and guarantees that Eve's mutual information with the final key is less than $2^{-\ell}$. The key string must also be essentially random.

In this final section, we give the main elements of a proof that BB 84 is secure. This proof serves as a fitting conclusion to the chapter, because of its elegant use of many concepts of quantum information in providing an argument that is sufficiently simple and transparent so as to be incontestable. The origin of this proof, intriguingly, comes from the observation that after information reconciliation and privacy amplification are performed, the ultimately obtainable key rate turns out to coincide with the achievable qubit transmission rate for CSS codes (Section 10.4.2) over noisy communication channels!

Here is the main idea, in outline. It is relatively straightforward to exhaustively establish that the BB84, B92, and EPR protocols are secure if Eve can only attack the transmission one qubit at a time. The difficulty lies in dealing with the possibility of collective attacks, in which Eve manipulates and possibly stores large blocks of the transmitted qubits. To address this, we need a more general and powerful argument. Suppose we somehow know that Eve

never introduces more than t qubit errors per block. Then Alice could encode her qubits in a t error-correcting quantum code, such that all of Eve's meddling could be removed by Bob decoding the code. Two things must be established to make this feasible: first, how can an upper bound be placed on t ? This turns out to be possible by sampling the channel in the appropriate manner, leaving us with a protocol which is secure, even against collective attacks! Unfortunately, this protocol generally requires a fault-tolerant quantum computer in order to encode and decode qubits robustly. The second challenge is thus to choose a quantum code such that the full sequence of encoding, decoding, and measurement can be performed using no quantum computation or storage - just single qubit preparation and measurement. Using CSS codes does the trick (after some simplification), and in fact gives just the BB 84 protocol. Below, we begin with a manifestly secure EPR pair based QKD protocol, and then apply solutions to the two challenges to systematically simplify the initial protocol into BB84.

Requirements for a secure QKD protocol

Suppose that Alice has n pairs of entangled qubits, each in the state

$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}. \tag{12.198}$$

Denote this state as $|\beta_{00}\rangle^{\otimes n}$. Alice then transmits half of each pair to Bob; because of noise and eavesdropping on the channel, the resulting state may be impure, and can be described as the density matrix ρ. Alice and Bob then perform local measurements to obtain a key, as described previously. The following Lemma can be used to show that the fidelity of ρ with respect to $|\beta_{00}\rangle^{\otimes n}$ places an upper bound on the mutual information Eve has with the key.

Lemma 12.19: (High fidelity implies low entropy) If $F\left(\rho, |\beta_{00}|^{\otimes n}\right)^2 > 1 - 2^{-s}$, then $S(\rho) < (2n + s + 1/\ln 2)2^{-s} + O\left(2^{-2s}\right)$.

Proof

If $F\left(\rho, |\beta_{00}\rangle^{\otimes n}\right)^2 = {}^{\otimes n}\langle\beta_{00}|\,\rho\,|\beta_{00}\rangle^{\otimes n} > 1 - 2^{-s}$, then the largest eigenvalue of ρ must be larger than $1 - 2^{-s}$. Therefore, the entropy of ρ is bounded above by the entropy of a diagonal density matrix $\rho_{\max}$ with diagonal entries $1 - 2^{-s}, 2^{-s}/\left(2^{2n} - 1\right), 2^{-s}/\left(2^{2n} - 1\right), \ldots, 2^{-s}/\left(2^{2n} - 1\right)$, that is, $\rho_{\max}$ has a large entry $1 - 2^{-s}$, and the remaining probability is distributed equally among the remaining $2^{2n} - 1$ entries. Since

$$S\left(\rho_{\max}\right) = -\left(1 - 2^{-s}\right)\log\left(1 - 2^{-s}\right) - 2^{-s}\log\frac{2^{-s}}{2^{2n} - 1} \tag{12.199}$$

the desired result follows.

By Holevo's bound (12.6), $S(\rho)$ is an upper bound on the information accessible to Eve, resulting from Alice and Bob's measurements of ρ. This implies that if a QKD protocol can provide Alice and Bob with EPR pairs of fidelity at least $1 - 2^{-s}$ (with high probability), then it is secure.

Exercise 12.30: Simplify (12.199) to obtain the expression for $S(\rho)$ given in the statement of the Lemma.

Exercise 12.31: It may be unclear why $S(\rho)$ bounds Eve's mutual information with Alice and Bob's measurement results. Show that this follows from assuming the worst about Eve, giving her all the control over the channel.

Random sampling can upper-bound eavesdropping

How can a protocol place a lower bound on the fidelity of Alice and Bob's EPR pairs? The key idea is a classical argument, based on random sampling, which we encountered in the description of the BB84 protocol (Exercise 12.27). Arguments based on classical probability, however, need not apply when considering outcomes of quantum measurements. This is vividly demonstrated by Bell's inequality (Section 2.6). On the other hand, quantum experiments do allow a classical interpretation whenever measurement observables that refer to only one basis are considered. And fortunately, it happens that measurements in only one basis are required for Alice and Bob to bound the fidelity of their EPR pairs.

According to (10.14), a qubit transmitted through a noisy quantum channel can be described as having had one of four things happen to it: nothing (I), a bit flip (X), a phase flip (Z), or a combined bit and phase flip (Y). Recall that the Bell basis is defined by the four states

$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \quad |\beta_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}, \quad |\beta_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}, \quad |\beta_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}. \tag{12.200}$$

Let the second qubit in each pair be the one that Alice sends to Bob. If a bit flip error occurs to this qubit, then $|\beta_{00}\rangle$ is transformed into $|\beta_{01}\rangle$. Similarly, a phase flip gives $|\beta_{10}\rangle$, and a combination of the two errors gives $|\beta_{11}\rangle$ (up to irrelevant overall phases). A natural measurement which detects if a bit flip has occurred is given by projectors $\Pi_{\rm bf} = |\beta_{01}\rangle\langle\beta_{01}| + |\beta_{11}\rangle\langle\beta_{11}|$ and $I - \Pi_{\rm bf}$, and likewise, the measurement described by projectors $\Pi_{\rm pf} = |\beta_{10}\rangle\langle\beta_{10}| + |\beta_{11}\rangle\langle\beta_{11}|$ and $I - \Pi_{\rm pf}$ detects phase flips. Since both these measurements commute with the Bell basis, their outcomes obey classical probability arguments. In fact, any measurement which commutes with the Bell basis will also satisfy the same classical arguments.

More precisely, Alice and Bob and can bound the fidelity of their EPR pairs by randomly sampling a subset of them. Suppose Alice sends $2n$ EPR pair halves to Bob. They subsequently randomly select n of them and check these qubits by jointly measuring either $\Pi_{\rm bf}$ or $\Pi_{\rm pf}$ (again, chosen randomly). By the same classical arguments used in the random sampling tests in BB 84 (Exercise 12.27), if δn bit or phase flip errors are detected, then the remaining n EPR pairs would be exponentially certain to have the same number of errors, were they also to be measured in the Bell basis.

Bell states are nonlocal, and generally measurements in the Bell basis require nonlocal operations, which can be difficult. Fortunately, however, they are not required in the present scheme, because $\Pi_{\rm bf} = (I \otimes I - Z \otimes Z)/2$, and $\Pi_{\rm pf} = (I \otimes I - X \otimes X)/2$. Thus, Alice and Bob can perform the desired checks with local measurements of Pauli operators, either by both measuring Z, or both measuring X.

Exercise 12.32: Note that the local measurements that Alice and Bob perform, such as $I \otimes X$ and $X \otimes I$, do not commute with the Bell basis. Show that despite this, the statistics which Alice and Bob compile from their measurements are the same as those which they would have obtained had they actually measured $\Pi_{\rm bf}$ and Π_{pf}.

The modified Lo-Chau protocol

Random sampling in the Bell basis thus provides Alice and Bob with EPR pairs ρ with known fidelity to the ideal state $|\beta_{00}\rangle^{\otimes n}$, and as previously discussed, this bounds Eve's mutual information with any measurements that might be performed on ρ. For ρ to be useful for key generation, however, Alice and Bob must reduce Eve's mutual information with their state until it is exponentially small. This task can be achieved by applying classical privacy amplification to their measurement results. Equivalently, Alice and Bob can first perform entanglement distillation, as introduced in Section 12.5.2, to obtain ρ' which is very close to $|\beta_{00}\rangle^{\otimes m}$ for some

$m < n$, then measure the final state. This sort of 'quantum privacy amplification' will be useful to us.

A rough argument is as follows. Entanglement distillation can be accomplished by performing quantum error-correction. Since ρ is nearly certain to have δn errors, encoding these qubits in a δn correcting quantum error-correction code allows up to δn errors to be perfectly corrected. As we saw in Sections 10.5.5 and 10.5.8, if an $[n, m]$ stabilizer code is used, then encoding, syndrome measurement and error recovery can be performed by measurements of Pauli operators determined by the rows of the check matrix for the code. Alice and Bob simply perform identical measurements and recovery operations on their respective n qubit halves of ρ, producing an error-corrected state which has a fidelity relative to $|\beta_{00}\rangle^{\otimes m}$ that is on the order of one minus the the probability of more than δn errors occurring. By construction, the syndrome measurements turn out to commute with the Bell basis, since Alice and Bob perform identical tasks.

Putting the random sampling and entanglement distillation pieces together gives us the modified Lo-Chau protocol, presented in Figure 12.14. A few notes about this protocol are in order. The random Hadamard transforms performed in steps 3 and 7 create a symmetry in Eve's strategy between detecting information encoded in the X and Z bases (and thus causing X and Z errors). They also enable random selection of a measurement of $\Pi_{\rm bf}$ or $\Pi_{\rm pf}$ on the check qubits. The specific procedure employed in step 9 can be justified for the case of any stabilizer code, as in Exercise 12.34. The Gilbert-Varshamov bound for CSS codes, Equation (10.74), shows that good quantum codes exist for large block lengths, so that n can be chosen sufficiently large that for a δn error-correcting $[\ n, m\ ]$ quantum code, the criteria for security can be satisfied.

QKD protocol: modified Lo-Chau

1: Alice creates $2n$ EPR pairs in the state $|\beta_{00}\rangle^{\otimes 2n}$.
2: Alice randomly selects n of the $2n$ EPR pairs to serve as checks to check for Eve's interference. She does not do anything with them yet.
3: Alice selects a random $2n$-bit string b, and performs a Hadamard transform on the second qubit of each pair for which b is 1 .
4: Alice sends the second qubit of each pair to Bob.
5: Bob receives the qubits and publicly announces this fact.
6: Alice announces b and which n qubits are to provide check bits.
7: Bob performs Hadamards on the qubits where b is 1 .
8: Alice and Bob each measure their n check qubits in the $|0\rangle, |1\rangle$ basis, and publicly share the results. If more than t of these disagree, they abort the protocol.
9: Alice and Bob measure their remaining n qubits according to the check matrix for a predetermined $[n, m]$ quantum code correcting up to t errors. They share the results, compute the syndromes for the errors, and then correct their state, obtaining m nearly perfect EPR pairs.
10: Alice and Bob measure the m EPR pairs in the $|0\rangle, |1\rangle$ basis to obtain a shared secret key.

Figure 12.14. A QKD protocol which is secure, by virtue of use of perfect quantum computers, error-correction, and random testing of EPR pairs.

Exercise 12.33: Let $\{M_1, M_2, \ldots, M_n\}$ be a set of measurement observables which produce respective results X_i when an input state ρ is measured. Argue that the random variables X_i obey classical probability arguments if $[M_i, M_j] = 0$, that is, they commute with each other.

Exercise 12.34: (Entanglement distillation by error-correction) In
Section 10.5.8, we saw that codewords of an $[n, m]$ qubit stabilizer code can be constructed by measuring its generators $g_1, \ldots, g_{n-m}$ on an arbitrary n qubit quantum state, then applying Pauli operations to change the result to be a simultaneous $+1$ eigenstate of the generators.

Using that idea, show that if we start out with n EPR pairs in the state $|\beta_{00}\rangle^{\otimes n}$, and perform identical generator measurements on the two n qubit halves of the pairs, followed by Pauli operations to correct for differences in the measurement results between the pairs, then we obtain an encoded $|\beta_{00}\rangle^{\otimes m}$ state. Also show that if the stabilizer code corrects up to δn errors, then even if δn errors are suffered by an n qubit half, we still obtain $|\beta_{00}\rangle^{\otimes m}$.

A quantum error-correction protocol

The modified Lo-Chau protocol makes use of quantum error-correction to perform entanglement distillation, and is built essentially upon the EPR protocol. Entanglement is a frail resource, and quantum error-correction generally requires robust quantum computers, which are challenging to realize. Fortunately, however, this protocol can be systematically simplified in a series of steps, each of which provably does not compromise the security of the scheme. Let us begin by removing the need to distribute EPR pairs.

Note that the measurements which Alice perform at the end of the modified Lo-Chau protocol can be performed at the very start, with no change in any of the states held by the rest of the world. Alice's measurements of her halves of the check EPR pairs in step 8 collapse the pairs into n single qubits, so instead of sending entangled states, Alice can simply send single qubits. This gives us the modified steps
$1'$: Alice creates n random check bits, and n EPR pairs in the state $|\beta_{00}\rangle^{\otimes n}$. She also encodes n qubits as $|0\rangle$ or $|1\rangle$ according to the check bits.
$2'$: Alice randomly chooses n positions (out of $2n$) and puts the check qubits in these positions and half of each EPR pair in the remaining positions.
$8'$: Bob measures the n check qubits in the $|0\rangle, |1\rangle$ basis, and publicly shares the results with Alice. If more than t of these disagree, they abort the protocol.

Similarly, Alice's measurements in steps 9 and 10 collapse EPR pairs into random qubits encoded in a random quantum code. This can be seen in the following manner. A particularly convenient choice of code, which we shall employ for the remainder of this section, is an $[n, m]$ CSS code of C_1 over C_2, $\mathrm{CSS}\,(C_1, C_2)$, which encodes m qubits in n qubits and corrects up to t errors. Recall from Section 10.4.2 that for this code, H_1 and $H_2^{\perp}$ are the parity check matrices corresponding to the classical codes C_1 and $C_2^{\perp}$, in which each of the codeword states is

$$\frac{1}{\sqrt{|C_2|}} \sum_{w \in C_2} |v_k + w\rangle\,, \tag{12.201}$$

for v_k being a representative of one of the 2^m cosets of C_2 in C_1 (the notation v_k is chosen to suggest a vector v indexed by a key string k). Also recall that there exists a family of codes equivalent to this one, $\mathrm{CSS}_{z,x}\,(C_1, C_2)$, with codeword states

$$|\xi_{v_k,z,x}\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{w \in C_2} (-1)^{z \cdot w} |v_k + w + x\rangle \tag{12.202}$$

These states form an orthonormal basis for a 2^n-dimensional Hilbert space (see Exercise 12.35), and thus we may write Alice's n EPR pair state as

$$|\beta_{00}\rangle^{\otimes n} = \sum_{j=0}^{2^n} |j\rangle|j\rangle = \sum_{v_k,z,x} |\xi_{v_k,z,x}\rangle\, |\xi_{v_k,z,x}\rangle \tag{12.203}$$

Note that in this expression, we have separated the labels into two kets, where the first denotes the qubits Alice keeps, and the second, the qubits which are sent to Bob. When Alice measures the stabilizer generators corresponding to H_1 and $H_2^{\perp}$ on her qubits in step 9, she obtains random values for x and z, and similarly, her final measurement in step 10 gives her

a random choice of v_k. The remaining n qubits are thus left in the state $|\xi_{v_k,z,x}\rangle$, which is the codeword for v_k in $\mathrm{CSS}_{z,x}(C_1, C_2)$. This is just the encoded counterpart of a 2^m qubit state $|k\rangle$. Therefore, as claimed above, Alice's measurements produce random qubits encoded in a random code.

Thus, instead of sending halves of EPR pairs, Alice can equivalently randomly choose x, z, and k, then encode $|k\rangle$ in the code $\mathrm{CSS}_{z,x}(C_1, C_2)$, and send Bob the encoded n qubits. This gives us the modified steps

$1''$: Alice creates n random check bits, a random m bit key k, and two random n bit strings x and z. She encodes $|k\rangle$ in the code $\mathrm{CSS}_{z,x}(C_1, C_2)$. She also encodes n qubits as $|0\rangle$ or $|1\rangle$ according to the check bits.

$2''$: Alice randomly chooses n positions (out of $2n$) and puts the check qubits in these positions and encoded qubits in the remaining positions.

6′ : Alice announces b, x, z, and which n qubits are to provide check bits.

9': Bob decodes the remaining n qubits from $\mathrm{CSS}_{z,x}(C_1, C_2)$.

10′ : Bob measures his qubits to obtain the shared secret key k.

The resulting scheme, known as the CSS codes protocol, is shown in Figure 12.15.

Exercise 12.35: Show that the states $|\xi_{v_k,z,x}\rangle$ defined in (12.202) form an orthonormal basis for a 2^n-dimensional Hilbert space, that is,

$$\sum_{v_k,z,x} |\xi_{v_k,z,x}\rangle \langle \xi_{v_k,z,x}| = I \tag{12.204}$$

Hint: for C_1 an $[n, k_1]$ code, C_2 an $[n, k_2]$ code, and $m = k_1 - k_2$, note that there are 2^m distinct values of v_k, 2^{n-k_1} distinct x, and 2^{k_2} distinct z.

Exercise 12.36: Verify Equation (12.203).

Exercise 12.37: This is an alternative way to understand why Alice's measurements in steps 9 and 10 collapse EPR pairs into random qubits encoded in a random quantum code. Suppose Alice has an EPR pair $(|00\rangle + |11\rangle)/\sqrt{2}$. Show that if she measures the first qubit in the X basis, then the second qubit collapses into an eigenstate of X determined by the measurement result. Similarly, show that if

she measures in the Z basis, then the second qubit is left in a Z eigenstate labeled by the measurement result. Using this observation and the results of Section 10.5.8, conclude that Alice's measurements of $H_1, H_2^{\perp}$, and $\bar{Z}$ on her EPR pair halves result in a random codeword of $\mathrm{CSS}_{z,x}(C_1, C_2)$ determined by her measurement results.

QKD protocol: CSS codes

$1''$: Alice creates n random check bits, a random m bit key k, and two random n bit strings x and z. She encodes $|k\rangle$ in the code $\mathrm{CSS}_{z,x}(C_1, C_2)$. She also encodes n qubits as $|0\rangle$ or $|1\rangle$ according to the check bits.

$2''$: Alice randomly chooses n positions (out of $2n$) and puts the check qubits in these positions and the encoded qubits in the remaining positions.

3: Alice selects a random $2n$-bit string b, and performs a Hadamard transform on each qubit for which b is 1 .

4: Alice sends the resulting qubits to Bob.

5: Bob receives the qubits and publicly announces this fact.

$6'$: Alice announces b, x, z, and which n qubits are to provide check bits.

7: Bob performs Hadamards on the qubits where b is 1 .

$8'$: Bob measures the n check qubits in the $|0\rangle, |1\rangle$ basis, and publicly shares the results with Alice. If more than t of these disagree, they abort the protocol.

9': Bob decodes the remaining n qubits from $\mathrm{CSS}_{z,x}(C_1, C_2)$.

10′ : Bob measures his qubits to obtain the shared secret key k.

Figure 12.15. A QKD protocol which is secure, by virtue of simplification of the modified Lo-Chau protocol via CSS codes.

Reduction to BB84

The CSS codes QKD protocol is secure by virtue of direct reduction from the modified Lo-Chau protocol, and is much simpler because it does not make any evident use of EPR pairs. Unfortunately, it is still unsatisfactory, because it requires perfect quantum computation to perform the encoding and decoding (instead of just single qubit preparation and measurements), and Bob needs to temporarily store qubits in a quantum memory while waiting for communication from Alice. The use of CSS codes, however, enables these two requirements to be removed, essentially because they decouple phase flip correction from bit flip correction.

First, note that Bob measures his qubits in the Z basis immediately after decoding; thus, the phase correction information Alice sends as z is unnecessary. Thus, since C_1 and C_2 are classical codes, instead of decoding then measuring, he can immediately measure to obtain $v_k + w + x + \epsilon$ (where ϵ represents some possible error, due to the channel and to Eve), then decode classically: he subtracts Alice's announced value of x, then corrects the result to a codeword in C_1, which is definitely $v_k + w$, if the distance of the code is
not exceeded. The final key k is the coset of v_k+w+C_2 in C_1 (see Appendix 2 for an explanation of cosets, and this notation). This gives us:
$\mathbf{9}''$: Bob measures the remaining qubits to get $v_k + w + x + \epsilon$, and subtracts x from the result, correcting it with code C_1 to obtain $v_k + w$.
$10''$: Bob computes the coset of $v_k + w + C_2$ in C_1 to obtain the key k.
Second, since Alice need not reveal z, the state she effectively sends is a mixed state, averaged over random values of z,

$$\rho_{v_k,x} = \frac{1}{2^n} \sum_z |\xi_{v_k,z,x}\rangle \langle \xi_{v_k,z,x}| \tag{12.205}$$

$$= \frac{1}{2^n |C_2|} \sum_z \sum_{w_1,w_2 \in C_2} (-1)^{z\cdot(w_1+w_2)} |v_k + w_1 + x\rangle \langle v_k + w_2 + x| \tag{12.206}$$

$$= \frac{1}{|C_2|} \sum_{w \in C_2} |v_k + w + x\rangle \langle v_k + w + x| \tag{12.207}$$

This state is simple to create: Alice need only classically choose $w \in C_2$ at random, and construct $|v_k + w + x\rangle$, using her randomly determined x and k. We thus have:
$1'''$: Alice creates n random check bits, a random n bit string x, a random $v_k \in C_1/C_2$, and a random $w \in C_2$. She encodes n qubits in the state $|0\rangle$ or $|1\rangle$ according to $v_k + w + x$, and similarly, n qubits according to the check bits.

Steps $\mathbf{1}'''$ and $\mathbf{9}''$ can be simplified further, by changing step $\mathbf{6}'$ slightly. Currently, Alice sends $|v_k + w + x\rangle$, Bob receives and measures to obtain $v_k + w + x + \epsilon$, then Alice sends x, which Bob subtracts to obtain $v_k + w + \epsilon$. But if Alice chooses $v_k \in C_1$ (as opposed to C_1/C_2), then w is unnecessary. Moreover, $v_k + x$ is then a completely random n bit string, and instead of the above protocol, it is equivalent if Alice chooses x at random, sends $|x\rangle$, Bob receives and measures to obtain $x + \epsilon$, then Alice sends $x - v_k$, which Bob subtracts to obtain $v_k + \epsilon$. Now, there is no difference between the random check bits and the code bits! This gives us:
$1''''$: Alice chooses a random $v_k \in C_1$, and creates $2n$ qubits in the state $|0\rangle$ or $|1\rangle$ according to $2n$ random bits.
$2'''$: Alice randomly chooses n positions (out of $2n$) and designates these as the check qubits, and the remainder as $|x\rangle$.

6″ : Alice announces $b, x - v_k$, and which n qubits are to provide check bits.
9‴ : Bob measures the remaining qubits to get $x + \epsilon$, and subtracts $x - v_k$ from the result, correcting it with code C_1 to obtain v_k.
10″ : Alice and Bob compute the coset of $v_k + C_2$ in C_1 to obtain the key k.
Next, note that Alice need not perform Hadamard operations (although in practice, single qubit operations are not so difficult to accomplish with photons). She can instead encode her qubits directly in either the $|0\rangle, |1\rangle(Z)$ basis or in the $|+\rangle, |-\rangle(X)$ basis, depending on the bits of b :
1⁗ : Alice creates $(4 + \delta)n$ random bits. For each bit, she creates a qubit in either the $|0\rangle, |1\rangle$ basis, or the $|+\rangle, |-\rangle$ basis, according to a random bit string b.

We are almost done: encoding and decoding are now performed classically. The remaining problem is to remove the need for a quantum memory. To solve this problem, suppose that Bob goes ahead and measures immediately after receiving qubits from Alice, choosing randomly to measure in either the X or Z bases. When Alice subsequently announces b, they can keep only those bits for which their bases happened to be the same. This allows Bob to do away completely with his quantum storage device. Note that with high probability they discard half their bits, so in order to obtain the same number of key bits as before, they should start with a little (say, δ) more than twice the number of original random bits. Of course, Alice now must delay her choice of which bits are to be check bits, until after the discarding step. This gives us the final protocol, shown in Figure 12.16. This protocol is exactly the same as BB84, with only minor cosmetic differences. Note how the use of the classical code C_1 performs information reconciliation, and computing the coset of $v_k + C_2$ in C_1 performs privacy amplification (see Section 12.6.2).

QKD protocol: Secure BB84

1: Alice creates $(4 + \delta)n$ random bits.
2: For each bit, she creates a qubit in either the Z basis, or the X basis, according to a random bit string b.
3: Alice sends the resulting qubits to Bob.
4: Alice chooses a random $v_k \in C_1$.
5: Bob receives the qubits, publicly announces this fact, and measures each in the Z or X bases at random.
6: Alice announces b.
7: Alice and Bob discard those bits Bob measured in a basis other than b. With high probability, there are at least $2n$ bits left; if not, abort the protocol. Alice decides randomly on a set of $2n$ bits to continue to use, randomly selects n of these to be check bits, and announces the selection.
8: Alice and Bob publicly compare their check bits. If more than t of these disagree, they abort the protocol. Alice is left with the n bit string x, and Bob with $x + \epsilon$.
9: Alice announces $x - v_k$. Bob subtracts this from his result, correcting it with code C_1 to obtain v_k.
10: Alice and Bob compute the coset of $v_k + C_2$ in C_1 to obtain the key k.

Figure 12.16. The final QKD protocol arrived at by systematic reduction of the CSS codes protocol, which is exactly the same as BB 84 (up to minor cosmetic differences). For clarity, we have dropped the ' notation.

In summary, we have systematically proven the security of the BB84 quantum key distribution protocol, by starting with a manifestly secure scheme requiring perfect quantum computation and quantum memories, and systematically reducing it to BB84. By virtue of having only made modifications which manifestly leave Eve's quantum state (conditioned on all revealed classical information) unchanged, we conclude that BB84 is secure. Naturally, there are some caveats. This proof only applies to an ideal situation, where the states sent are those described.

In practice, qubit sources are imperfect; for example,
such sources are often lasers attenuated to approximately generate single photons, representing qubits (as described in Section 7.4.1). Furthermore, the proof does not place any bounds on the amount of effort Alice and Bob must go to in decoding; for practical key distribution, C_1 must be efficiently decodable. This proof also does not provide an upper bound on the tolerable eavesdropping; it utilizes CSS codes, which are not optimal. It is estimated that a rate of bit and phase errors up to 11% is acceptable using a protocol similar to BB84, but with the aid of quantum computers to encode and decode, higher error rates may be tolerable. The ultimate capability of quantum cryptography is an interesting open issue, and we expect such fundamental questions about the physical limits of computation and communication to continue to intrigue and challenge researchers in the future.

Exercise 12.38: Show that if you had the ability to distinguish non-orthogonal states, then it would be possible to compromise the security of BB84, and indeed, all of the QKD protocols we have described.

Problem 12.1: In this problem we will work through an alternate proof of the Holevo bound. Define the Holevo chi quantity,

$$\chi \equiv S(\rho) - \sum_x p_x S(\rho_x) \tag{12.208}$$

(1) Suppose the quantum system consists of two parts, A and B. Show that

$$\chi_A \leq \chi_{AB} \tag{12.209}$$

(Hint: Introduce an extra system which is correlated with AB, and apply strong subadditivity.)
(2) Let $\mathcal{E}$ be a quantum operation. Use the previous result to show that

$$\chi' \equiv S(\mathcal{E}(\rho)) - \sum_x p_x S(\mathcal{E}(\rho_x)) \leq \chi \equiv S(\rho) - \sum_x p_x S(\rho_x) \tag{12.210}$$

That is, the Holevo chi quantity decreases under quantum operations. This is an important and useful fact in its own right.
(3) Let E_y be a set of POVM elements. Augment the quantum system under consideration with an 'apparatus' system, M, with an orthonormal basis $|y\rangle$. Define a quantum operation by

$$\mathcal{E}(\rho \otimes |0\rangle\langle 0|) \equiv \sum_y \sqrt{E_y}\rho\sqrt{E_y} \otimes |y\rangle\langle y|, \tag{12.211}$$

where $|0\rangle$ is some standard pure state of M. Prove that after the action of $\mathcal{E}$, $\chi_M = H(X : Y)$. Use this and the previous two results to show that

$$H(X : Y) \leq S(\rho) - \sum_x p_x S(\rho_x) \tag{12.212}$$

which is the Holevo bound.
Problem 12.2: This result is an extension of the previous problem. Provide a proof of the no-cloning theorem by showing that a cloning process for non-orthogonal pure states would necessarily increase χ.

Problem 12.3: For a fixed quantum source and rate $R > S(\rho)$, design a quantum circuit implementing a rate R compression scheme.

Problem 12.4: (Linearity forbids cloning) Suppose we have a quantum machine with two slots, A and B. Slot A, the data slot, starts out in an unknown quantum state ρ. This is the

state to be copied. Slot B, the target slot, starts out in some standard quantum state, σ. We will assume that any candidate copying procedure is linear in the initial state,

$$\rho \otimes \sigma \rightarrow \mathcal{E}(\rho \otimes \sigma) = \rho \otimes \rho, \tag{12.213}$$

where $\mathcal{E}$ is some linear function. Show that if $\rho_1 \neq \rho_2$ are density operators such that

$$\mathcal{E}(\rho_1 \otimes \sigma) = \rho_1 \otimes \rho_1 \tag{12.214}$$

$$\mathcal{E}(\rho_2 \otimes \sigma) = \rho_2 \otimes \rho_2 \tag{12.215}$$

then any mixture of ρ_1 and ρ_2 is not copied correctly by this procedure.

Problem 12.5: (Classical capacity of a quantum channel - Research) Is the product state capacity (12.71) the true capacity of a noisy quantum channel for classical information, that is, the capacity when entangled inputs to the channel are allowed?

Problem 12.6: (Methods for achieving capacity - Research) Find an efficient construction for codes achieving rates near the product state capacity (12.71) of a noisy quantum channel for classical information.

Problem 12.7: (Quantum channel capacity - Research) Find a method to evaluate the capacity of a given quantum channel $\mathcal{E}$ for the transmission of quantum information.

9.5.25 Summary of Chapter 12: Quantum information theory

- No-cloning: No quantum device can be constructed which outputs $|\psi\rangle|\psi\rangle$, given $|\psi\rangle$, for arbitrary $|\psi\rangle$.
- Holevo's bound: The maximum accessible classical information when trying to distinguish between quantum states ρ_x sent with probability distribution p_x is

$$H(X:Y) \leq \chi \equiv S\left(\sum_x p_x \rho_x\right) - \sum_x p_x S(\rho_x)$$

- Schumacher's quantum noiseless channel coding theorem: $S(\rho)$ can be interpreted as the number of qubits needed to faithfully represent a quantum source described by ρ.
- The Holevo-Schumacher-Westmoreland theorem: The capacity of a noisy quantum channel $\mathcal{E}$ for classical information is given by:

$$C(\mathcal{E}) = \max_{\{p_x, |\psi_x\rangle\}} S\left(\sum_x p_x \mathcal{E}(|\psi_x\rangle\langle\psi_x|)\right) - \sum_x p_x S(\mathcal{E}(|\psi_x\rangle\langle\psi_x|)) \tag{12.216}$$

- Majorization condition for entanglement transformation: Alice and Bob can transform $|\psi\rangle$ to $|\varphi\rangle$ by local operations and classical communication if and only if $\lambda_\psi \prec \lambda_\varphi$, where λ_ψ is a vector of the eigenvalues of the reduced density matrix of $|\psi\rangle$ (similarly for λ_φ).
- Pure state entanglement distillation and dilution: Alice and Bob can convert between n copies of a joint state $|\psi\rangle$ and $nS(\rho)$ Bell pairs, by local operations and classical communication alone, as $n \rightarrow \infty$, where ρ is the reduced density matrix.
- Quantum cryptography: Provably secure key distribution is possible by communicating using non-orthogonal quantum states, with a protocol such as BB84. Eavesdropping on the channel will cause a detectable increase in the error rate, because information gain implies disturbance.

History and further reading

The book of Cover and Thomas [CT91] is a terrific introduction to classical information theory. The reader looking for a more advanced yet still readable treatment of information theory should consult Csiszár and Körner [CK81] . Also well worth the read are Shannon's original papers, among the most influential in twentieth century science. These have been reprinted together in a single volume by Shannon and Weaver [*SW*49]. Bennett and Shor [BS98] and Bennett and DiVincenzo [BD00] have written excellent review articles on quantum information theory.

The no-cloning theorem is due to Dieks [Die82] and to Wootters and Zurek [WZ82]. An enormous amount of work has been done extending these results. By far the majority of the papers consider various schemes for cloners which are interesting in some particular way - they optimize some measure of cloning fidelity, or some other property one might wish a cloner to have. We will not attempt to give a full review of this work here, but
note that many of these papers may be found on the internet at http://arXiv.org/ in the quant-ph archive. Some papers of especial interest include the work of Barnum, Caves, Fuchs, Jozsa and Schumacher [BCF+96] extending the range of application of the no-cloning theorem to mixed states and non-unitary cloning devices; by Mor [Mor 98] on the cloning of states of composite systems; by Westmoreland and Schumacher [WS98] on a possible equivalence between cloning and faster-than-light communication; and a rebuttal by van Enk [van 98 b].

The Holevo bound was conjectured by Gordon in 1964[Gor64], and proved by Holevo in 1973[Hol73]. The conceptually simple proof we have given is based upon the difficult-toprove strong subadditivity inequality, however Holevo used a more direct approach which has been simplified by Fuchs and Caves [*FC*94]. The approach via strong subadditivity is due to Yuen and Ozawa [YO93]; see also Schumacher, Westmoreland and Wootters [SWW96].

The classical noiseless channel coding theorem is due to Shannon [Sha48, *SW*49]. The quantum noiseless channel coding theorem is due to Schumacher [*Sch*95], and is described in a pioneering paper that introduced in an integrated fashion many of the fundamental notions of quantum information theory, including sources, fidelity measures, and the notion of quantum states as a resource that could be treated in information-theoretic terms. This last observation, simple but profound, was driven home by Schumacher's introduction in the paper of the now-ubiquitous term qubit, attributed to a conversation between Schumacher and Wootters. A paper by Jozsa and Schumacher [JS94] simplified Schumacher's original approach; this paper was published earlier than [Sch95], but was was written at a later time. These papers were based on the ensemble-average fidelity measure discussed in Exercise 12.8, rather than the entanglement fidelity based proof we have given here, which is based on the approach of Nielsen [Nie98]. A slight hole in the original papers by Schumacher, and Schumacher and Jozsa was filled by the work of Barnum, Fuchs, Jozsa and Schumacher [BFJS96]. M. Horodecki[Hor97] subsequently provided a more powerful proof of the same result that also points the way towards a theory of quantum data compression of ensembles of mixed states. The compression scheme described in Box 12.4, which is the quantum analogue of Cover's enumerative coding method [CT91], is originally attributed to Schumacher [Sch95], and quantum circuits for it are explicitly given by Cleve and DiVincenzo [CD96]. Braunstein, Fuchs, Gottesman, and Lo have generalized this to provide a quantum analogue to Huffman encoding[BFGL98], and Chuang and Modha to arithmetic coding[CM00].

The Holevo-Schumacher-Westmoreland (HSW) theorem has an interesting history. The problem it addresses was first discussed by Holevo [Hol79] in 1979, who made some partial progress on the problem. Unaware of this work, Hausladen, Jozsa, Schumacher, Westmoreland, and Wootters [HJS+96] solved a special case of the problem in 1996. Independently, and shortly thereafter, Holevo [Hol98] and Schumacher and Westmoreland[SW97] proved the HSW theorem giving the product state capacity of a noisy quantum channel for classical information. Fuchs

[Fuc97] has described some interesting examples of the product state capacity, where the ensemble of states maximizing the expression (12.71) for the capacity contains non-orthogonal members. King and Ruskai [$KR99$] have made some promising headway on the problem of showing that the product state capacity is the same as the capacity unrestricted to product states, but the general problem remains open.

The entropy exchange was defined by Lindblad [Lin 91], and rediscovered by Schumacher [$Sch96$ b], who proved the quantum Fano inequality. The coherent information was introduced by Lloyd [Llo97] and by Schumacher and Nielsen [SN96] in the context of the capacity of a noisy quantum channel; [SN96] proves the quantum data processing inequality. A table containing the inequalities mentioned in Exercise 12.15 may be found in Nielsen's Ph.D. dissertation [Nie98]. The as yet unsolved problem of determining the quantum channel capacity (Problem 12.7) has an interesting history. Initial work on the subject came from several different perspectives, as may be seen from the papers of Barnum, Nielsen and Schumacher [BNS98], of Bennett, DiVincenzo, Smolin, and Wootters [BDSW96], of Lloyd [Llo97] , of Schumacher [Sch96b] and of Schumacher and Nielsen [SN96]. The equivalence of several of these points of view has been understood through the work of Barnum, Knill and Nielsen[BKN98], and Barnum, Smolin and Terhal[BST98]. The capacity has been established for some specific channels (most notably the quantum erasure channel) by Bennett, DiVincenzo and Smolin [BDS97] , and a lower bound on the capacity of the depolarizing channel making intriguing use of degenerate quantum codes has been obtained by Shor and Smolin [$SS96$], and refined by DiVincenzo, Shor and Smolin [$DSS98$]. Zurek[Zur89], Milburn [Mil96], and Lloyd[Llo96] analyzed examples of quantum Maxwell's demons, though not in the context of error-correction. The analysis here is based on the work of Nielsen, Caves, Schumacher and Barnum [NCSB98]. This point of view has also been pursued by Vedral[Ved99] to obtain limits on entanglement distillation procedures. The quantum Singleton bound is due to Knill and Laflamme[KL97]. The proof we give is due to Preskill[Pre98b].

The study of entanglement has blossomed into a major area of research, and there are far too many papers on the subject to even begin to give an account here. Once again, see the quant-ph archive at http://arXiv.org/. The conditions for entanglement transformation based on majorization (Theorem 12.15) are due to Nielsen [Nie99]. Theorem 12.13 is due to Uhlmann[Uhl71, Uhl72, Uhl73]. Proposition 12.14 is due to Lo and Popescu[LP97]. Entanglement catalysis was discovered by Jonathan and Plenio [JP99]. Marshall and Olkin [MO79] is a comprehensive introduction to majorization, including the proof of Birkhoff's theorem. The limits for entanglement dilution and distillation are due to Bennett, Bernstein, Popescu and Schumacher [BBPS96]. Entanglement distillation protocols for mixed states were introduced by Bennett, Brassard, Popescu, Schumacher, Smolin and Wootters [$BBP^{+}96$], and the connection to quantum error-correction developed in a ground-breaking paper by Bennett, DiVincenzo, Smolin and Wootters[BDSW96] that has stimulated a lot of subsequent research. The example illustrated in Figure 12.11 was noted by Gottesman and Nielsen (unpublished). We mention just a few more papers on entanglement of exceptional interest that may serve as an entry-point to the literature; unfortunately many papers of note are omitted as a result. A series of papers by members of the Horodecki family (Michal, Pawel and Ryszard) have investigated the properties of entanglement in depth; of especial note are [HHH96, HHH98, HHH99a, HHH99b, HHH99c]. Also of great interest are the papers by Vedral and Plenio [$VP98$] and by Vidal [$Vid98$].

For an excellent (early) overview of quantum cryptography at the lay level see the article by Bennett, Brassard, and Ekert in Scientific American [$8BE92$]. Quantum cryptographic ideas were first put forward by Wiesner in the late 1960s. Unfortunately, Wiesner's ideas were not accepted for publication, and it wasn't until the early 1980s that the ideas became known. Wiesner proposed that (entangled) quantum states, if they could be stored for long periods of time, could be used as a kind of counterfeit-proof money[Wie, Wie83]. Bennett developed sev-

eral further protocols, one of which lead to the first experimental implementation, by Bennett, Bessette, Brassard, Salvail, and Smolin [BBB+92], which is
of historical interest (in principle) since it transmitted its information less than a meter and, moreover, eavesdropping was facilitated by a loud buzzing sound which emanated from the power supply whenever a 'one' was sent! The concept of privacy amplification was first introduced by Bennett, Brassard, and Robert [BBR88]. For information reconciliation protocols see [BBB+92] and [BS94]. Theorem 12.16 is stated and proved in Bennett, Brassard, Crèpeau, and Maurer [BBCM95], in a very readable general treatment of privacy amplification. Note that the information disclosed during reconciliation has an important impact on the threshold for privacy amplification, as bounded in Theorem 12.17, proven by Cachin and Maurer [CM97] . Privacy amplification has applications to classical key generation using distant correlated random sources such as starlight sensed by satellites[Mau93]. The four state protocol known as BB84 is named after the authors, Bennett and Brassard [BB84], and similarly, the two state B92 protocol is named after Bennett [Ben92] . The EPR protocol was devised by Ekert [Eke91]. The proof of the random sampling bound in Exercise 12.27 is due to Ambainis. The limitations and security of quantum cryptography have been discussed in depth in many publications. For a sample, see the works by Barnett and Phoenix [BP93] ; Brassard [Bra93] ; Ekert, Huttner, Palma, and Peres [EHPP94] ; also [Phy92] . The connection between coherent information and privacy was recognized by Schumacher and Westmoreland [SW98]. Numerous papers have been published on experimental implementations of quantum cryptographic systems. For a good introduction, see Hughes, Alde, Dyer, Luther, Morgan, and Schauer [HAD+95]; the demonstration of quantum cryptography under Lake Geneva was by Muller, Zbinden, and Gisin [MZG96]. The experiment described in Box 12.7 was performed at IBM, by Bethune and Risk [BR98, BR00], and we thank them for the schematic of their apparatus. A large number of proofs of the security of various quantum key distribution protocols, under different circumstances, have been presented. Of particular note is a complete (and extensive, but somewhat complicated) proof of the security of QKD with BB84 given by Mayers[May98]. Biham, Boyer, Brassard, van de Graaf, and Mor have also considered attacks against BB84 [BBB+98]. A simpler proof, which uses EPR states and requires perfect quantum computation has been given by Lo and Chau [LC99]; this is the protocol we began with in Section 12.6.5. Lo has simplified it to begin with a test which ascertains the error rate, before transmitting key material [Lo99]. The even simpler (and beautiful!) proof given in Section 12.6.5 is due to Shor and Preskill [SP00], who also give the 11% estimate mentioned in Section 12.6.5. Our presentation of this proof also benefited greatly from conversations with Gottesman.

10 Quantum Systems, Channels, Information by Holevo

10.0.1 Preface

Quantum information theory studies the general laws of transfer, storage, and processing of information in systems obeying the laws of quantum mechanics. It took shape as a self-consistent area of research in the 1990s, while its origin can be traced back to the 1950-1960s, which was when the basic ideas of reliable data transmission and of Shannon's information theory were developed. At the first stage, which covers the period 1960-1980, the main issue consisted of the fundamental restrictions on the possibilities of information transfer and processing caused by the quantum mechanical nature of its carrier. Modern technological developments, relying upon the achievements of quantum electronics and quantum optics, suggest that in the foreseeable future such restrictions will become the main obstacle limiting further extrapolation of existing technologies and principles of information processing.

The emergence, in the 1980-1990s, of the ideas of quantum computing, quantum cryptography, and the new communication protocols, on the other hand, allowed discussing not only the restrictions, but also the new possibilities created by the use of specific quantum resources, such as quantum entanglement, quantum complementarity, and quantum parallelism. Quantum information theory provides the clue to understanding these fundamental issues and stimulates the development of experimental physics, with potential importance to new, effective applications. At present, investigations in the area of quantum information science, including information theory, its experimental aspects, and technological developments, are ongoing in advanced research centers throughout the world.

The mathematical toolbox of "classical" information theory contains methods based on probability theory, combinatorics, and modern algebra, including algebraic geometry. For a mathematician sensible to the impact of his research on the natural sciences, information theory can be a source of deep ideas and new, challenging problems, with sound motivation and applications. This equally, if not to a greater extent, applies to quantum information theory, the scope of which turns out to be closely connected to multilinear algebra and noncommutative analysis, convexity, and asymptotic theory of finite-dimensional normed spaces, subtle aspects of positivity and tensor products in operator algebras, and the methods of random matrices. Nowadays, the intimate connections to operator spaces and so-called "quantum functional analysis" have been revealed and explored.

In 2002, the Moscow Independent University published the author's lecture notes (in Russian), in which an attempt was made at a mathematician's introduction to problems of quantum information theory. In 2010, a substantially expanded text was published with the title "Quantum systems, channels, information." The author's intention was to provide a widely accessible and self-contained introduction to the subject, starting from primary structures and leading up to nontrivial results with rather de-
tailed proofs, as well as to some open problems. The present English text is a further step in that direction, extending and improving the Russian version of 2010.

The exposition is organized in concentric circles, the N th round consisting of Parts I to N, where each circle is self-contained. The reader can restrict himself to any of these circles, depending on the depth of presentation that he or she demands. In particular, in Part I to Part IV, we consider finite-dimensional systems and channels, whereas the infinite-dimensional case is treated in the final Part V.

Part I starts with a description of the statistical structure of quantum theory. After introducing the necessary mathematical prerequisites in Chapter 1, the central focus in Chapters 2, 3 is on discussing the key features of quantum complementarity and entanglement. The former is reflected by the noncommutativity of the algebra of observables of the system, while the latter is reflected by the tensor product structure of composite quantum systems. Chapter 3 also contains the first applications of the information-theoretic approach to quantum systems.

In information theory, the notions of a channel and its capacity, giving a measure of ultimate information-processing performance of the channel, play a central role. In Chapter 4 of Part II, a review of the basic concepts and necessary results from classical information theory is provided, the quantum analogs of which are the main subject of the following chapters. The concepts of random coding and typicality are introduced and then extended to the quantum case in Chapter 5. That chapter contains direct and self-consistent proofs of the quantum information bound and of the primary coding theorems for the classical-quantum channels, which will later serve as a basis for the more advanced capacity results in Chapter 8.

Part III is devoted to the study of quantum channels and their entropy characteristics. In Chapter 6, we discuss the general concept and structure of a quantum channel, with the help of a variety of examples. From the point of view of operator algebras, these are normalized completely positive maps, the analog of Markov maps in noncommutative probability theory,

and they play the role of morphisms in the category of quantum systems. From the point of view of statistical mechanics, a channel gives an overall description of the evolution of an open quantum system interacting with an environment - a physical counterpart of the mathematical dilation theorem. Various entropic quantities essential to the characterization of the information-processing performance, as well as the irreversibility of the channel, are investigated in Chapter 7.

Part IV is devoted to the proofs of advanced coding theorems, which give the main capacities of a quantum channel. Remarkably, in the quantum case, the notion of the channel capacity splits, giving a whole spectrum of information-processing characteristics, depending on the kind of data transmitted (classical or quantum), as well as on the additional communication resources. In Chapter 8, we discuss the classical capacity of a quantum channel, i. e., the capacity for transmitting classical data. We touch upon the tremendous progress made recently in the solution of the related additivity problem and point out the remaining questions. Chapter 9 is devoted to the classical entanglement-assisted capacity and its comparison with unassisted capacity. In

Chapter 10, we consider reliable transmission of quantum information (i. e., quantum states), which turns out to be closely related to the private transmission of classical information. The corresponding coding theorems provide the quantum capacity and the private classical capacity of a quantum channel.

In Part V, we pass from finite-dimensional to separable Hilbert space. Chapter 11 deals with the new obstacles characteristic for infinite-dimensional channels - singular behavior of the entropy (infinite values, discontinuity) and the emergence of the input channel constraints (e.g., finiteness of the signal energy) and of the continuous optimizing state ensembles. Chapter 12 treats the bosonic Gaussian systems and channels on the canonical commutation relations (many experimental demonstrations of quantum information processing were realized in such "continuous-variables" systems, based in particular on the principles of quantum optics). We assume the reader has some minor background in the field and start with a rather extended introduction at the beginning of Chapter 12. Next, we describe and study in detail the Gaussian states and channels. The main mathematical problems here are the structure of the multimode quantum Gaussian channels and the computation of the various entropic quantities characterizing their performance. While the classical entanglementassisted capacity is, in principle, computable for a general Gaussian channel, the quantum capacity is found only for restricted classes of channels, and the unassisted classical capacity in general presents an open analytical problem, namely, that of verifying the conjecture of "quantum Gaussian optimizers," which is comparable in complexity to the additivity problem (also open for the class of Gaussian channels) and appears to be closely related to it.

This book does not intend to be an all-embracing text in quantum information theory and its content definitely reflects the author's personal research interests and preferences. For example, the important topics of entanglement quantification and error correction are mentioned only briefly. An interested reader can find an account of these in other sources, listed in the notes and references to the individual chapters. Quantum information theory is in a stage of fast development and new, important results continue to appear. Yet, we hope the present text will be a useful addition to the existing literature, particularly for mathematically inclined readers eager to penetrate the fascinating world of quantum information.

The basis for these lecture notes was a course taught by the author at the Moscow Institute of Physics and Technology, Moscow State University, and several Western institutions. The author acknowledges stimulating discussions, collaborations, and invaluable support of R. Ahlswede, A. Barchielli, C. H. Bennett, G. M. D'Ariano, C. Fuchs, V. Giovannetti, O. Hirota, R. Jozsa, L. Lanz, O. Melsheimer, H. Neumann, M. B. Ruskai, P. W. Shor, Yu. M. Suhov, K. A. Valiev, R. Werner, A. Winter, and M. Wolf.

I extend special thanks to my colleagues Maxim Shirokov and Andrey Bulinsky for their careful reading of the manuscript and the suggestions for numerous improvements.

This work was supported by the Russian Foundation for Basic Research, Fundamental Research Programs of the Russian Academy of Sciences, and the Cariplo Fellowship organized by the Landau Network - Centro Volta.

10.0.2 Preface to the Second Edition

A major change in the second edition of the book is Chapter 12. The new version includes a solution of the long-standing problem of quantum Gaussian optimizers, which appeared soon after publication of the first edition. This result enables one to explicitly compute the classical capacity for the most usable mathematical models of quantum communication channels in continuous-variables systems, making the whole content of the book more complete.

In Chapters 1-11 several textual amendments were made. Circa thirty new references were added which are strictly relevant to the main content of the monograph. The author is grateful to Maxim Shirokov, whose careful reading and comments contributed substantially to the improvement of the presentation.

10.1 1 Vectors and Operators

We will deal with quantum-mechanical systems described by finite-dimensional Hilbert spaces. On the one hand, one can see already in that case, and perhaps most manifestly, the distinctive features of quantum statistics. On the other hand, finite-level systems are of the main interest for applications such as quantum communication, cryptography, and computing (although in the field of quantum information theory attention was recently attracted by the "continuous-variables systems," which are described by infinite-dimensional spaces; see Chapters 11, 12).

10.1.1 1.1 Hilbert Space

Let $\mathcal{H}$ be a d-dimensional complex linear space, $\dim \mathcal{H} = d < \infty$, with the inner product $\langle \phi \mid \psi \rangle, \phi, \psi \in \mathcal{H}$, satisfying the axioms of unitary space (see, e. g., [156]). However, following physical rather than mathematical traditions, we assume $\langle \phi \mid \psi \rangle$ to be linear with respect to the second argument ψ and antilinear with respect to ϕ. Again following a tradition in physics literature, we shall call it a Hilbert space (although emphasis of the mathematical Hilbert space theory is on the infinite-dimensional case).

We shall use Dirac's notations: a vector $\psi \in \mathcal{H}$ (which conventionally should be thought of as a column vector) will often be denoted as $|\psi\rangle$. Correspondingly, $\langle \phi|$ will denote the linear function on $\mathcal{H}$, defined by the inner product

$$\langle \phi| : \psi \to \langle \phi \mid \psi \rangle, \quad \psi \in \mathcal{H}$$

These linear functions themselves form another Hilbert space-the dual space $\mathcal{H}^*$ of $\mathcal{H}$ (they should be thought of as row vectors $\langle \phi| = |\phi\rangle^*$, the Hermitian conjugate [adjoint] to $|\phi\rangle$). The space $\mathcal{H}^*$ is antiisomorphic to $\mathcal{H}$ via the correspondence $|\psi\rangle \leftrightarrow \langle \psi|$. Then the inner product $\langle \phi \mid \psi \rangle$ is naturally thought of as the product of the "bra" and "ket" vectors $\langle \phi|$ and $|\psi\rangle$. The square of the norm, both in $\mathcal{H}$ and $\mathcal{H}^*$, is $\langle \psi \mid \psi \rangle = \|\psi\|^2$.

This notation also allows for a convenient description of operators. For example, the "outer product" of "ket" and "bra" vectors $A = |\psi\rangle\langle\phi|$ describes the rank one operator, which acts onto vector $|\chi\rangle$ according to the formula $A|\chi\rangle = |\psi\rangle\langle\phi \mid \chi\rangle$. Let $\{e_i\}_{i=1,d}$ be an orthonormal basis in $\mathcal{H}$. The decomposition of arbitrary vector $\psi \in \mathcal{H}$ can then be written as

$$|\psi\rangle = \sum_{i=1}^{d} |e_i\rangle \langle e_i \mid \psi\rangle \tag{1.1}$$

which is the same as

$$\sum_{i=1}^{d} |e_i\rangle \langle e_i| = I \tag{1.2}$$

where I is the unit operator in $\mathcal{H}$.

Exercise 1.1 Write the matrix representation for operators in $\mathcal{H}$, similar to the representation (1.1) for vectors.

An additional advantage of Dirac's notations is that we do not need to write the symbol of the vector, leaving only the label(s), e. g., we may write $|i\rangle$ instead of $|e_i\rangle$.

Sometimes we shall consider a real Hilbert (i. e., Euclidean) space. A fundamental difference with the complex case is revealed by the polarization identity

$$\beta(\phi, \psi) = \frac{1}{4} \sum_{k=0}^{3} (-i)^k \beta\left(\phi + i^k \psi, \phi + i^k \psi\right), \tag{1.3}$$

which allows us to uniquely restore all values of the form $\beta(\phi, \psi)$, which is linear with respect to the second argument and antilinear with respect to the first, from its diagonal values $\beta(\psi, \psi), \psi \in \mathcal{H}$ (in the real case, such a restoration is possible only for symmetric forms). Due to this, in order to prove an operator equality $A = B$, it is sufficient to establish the equality for all diagonal values, i. e., $\langle \psi \mid A\psi\rangle = \langle \psi \mid B\psi\rangle, \psi \in \mathcal{H}$.

10.1.2 1.2 Operators

If A is an operator in $\mathcal{H}$ (throughout this book we deal only with linear operators), then A^* denotes its adjoint, defined by

$$\langle \phi \mid A^*\psi\rangle = \langle A\phi \mid \psi\rangle, \quad \phi, \psi \in \mathcal{H}. \tag{1.4}$$

An operator A is called Hermitian if $A = A^*$. An (orthogonal) projector is a Hermitian operator P such that $P^2 = P$. The range of projector P is the subspace

$$\mathcal{L} = \{\psi : P|\psi\rangle = |\psi\rangle\}.$$

If $\|\psi\| = 1$, then $|\psi\rangle\langle\psi|$ is the projector onto the unit vector $|\psi\rangle$. More generally, for an orthonormal system $\{e_i\}_{i\in I}$, the operator $\sum_{i\in I} |e_i\rangle \langle e_i| = P$ is the projector onto the subspace generated by $\{e_i\}_{i\in I}$.

A unitary operator is an operator U such that $U^*U = I$. In the finite-dimensional case, which we here consider, this implies $UU^* = I$. A partial isometry is an operator U such that $U^*U = P$ is a projector. In this case $UU^* = Q$ also is a projector; U maps the range of P onto the range of Q isometrically, i. e., preserving inner products and norms of vectors.

Theorem 1.2 (Spectral decomposition). For a Hermitian operator A, there is an orthonormal basis of eigenvectors to which correspond real eigenvalues a_i, such that

$$A = \sum_{i=1}^{d} a_i |e_i\rangle \langle e_i| . \tag{1.5}$$

Another useful form of the spectral decomposition is obtained if we consider the distinct eigenvalues $\{a\}$ and the corresponding spectral projectors, i.e.,

$$E_a = \sum_{i:a_i=a} |e_i\rangle \langle e_i| .$$

The collection of distinct eigenvalues $\mathrm{spec}(A) = \{a\}$ is called the spectrum of the operator A. Then

$$A = \sum_{a\in \mathrm{spec}(A)} aE_a. \tag{1.6}$$

This representation is unique up to the ordering of the eigenvalues. The collection of projectors $\{E_a\}$ forms an orthogonal resolution of the identity, i.e.,

$$E_a E_{a'} = \delta_{aa'} E_a, \qquad \sum_{a\in \mathrm{spec}(A)} E_a = I. \tag{1.7}$$

The Hilbert space $\mathcal{H}$ splits into the direct orthogonal sum of the ranges of the projectors $\{E_a\}$, on which A acts as multiplication by a.

Both unitary and Hermitian operators are special cases of normal operators, satisfying $A^*A = AA^*$. For normal operators, the spectral decomposition (1.5) holds, with complex eigenvalues a_i.

10.1.3 1.3 Positivity

A Hermitian operator A is called positive, $A \geq 0$, if $\langle \psi \mid A\psi \rangle \geq 0$ for all $\psi \in \mathcal{H}$. The eigenvalues of a positive operator are all nonnegative, i.e., $a \geq 0$ for $a \in \mathrm{spec}(A)$.

The operator is positive if and only if it can be represented as $A = B^*B$ for some operator B. A positive operator has a unique positive square root, i. e., for any positive operator A there exists one and only one positive operator B, denoted by $\sqrt{A} = A^{1/2}$ such that $B^2 = A$.

For an arbitrary Hermitian operator A, we have

$$A = A_+ - A_-, \tag{1.8}$$

where $A_+ = \sum_{a>0} aE_a, A_- = -\sum_{a<0} aE_a$ are positive operators called the positive and negative part of the operator A.

Theorem 1.3 (Polar decomposition). Any operator A in $\mathcal{H}$ allows the decomposition

$$A = U|A| = |A^*|\, U, \tag{1.9}$$

where $|A| = \sqrt{A^*A}$ is a positive operator and U is unitary.

The support $\mathrm{supp}\, A$ of a positive operator A is the span of eigenvectors of A corresponding to positive eigenvalues. In the polar decomposition, the unitary operator is uniquely defined only on $\mathrm{supp}\, A$.

Occasionally, we will make use of a real Hilbert space, i. e., Euclidean space, and the operators in it. In that case, the Hermitian operators are replaced by symmetric operators, and unitary operators by orthogonal ones, with formally similar definitions. The polar decomposition of an operator A holds, with $|A|$ symmetric positive and U an orthogonal operator.

10.1.4 1.4 Trace and Duality

The trace of an operator T is defined by

$$\mathrm{Tr}\, T = \sum_{i=1}^{d} \langle e_i \mid Te_i \rangle , \tag{1.10}$$

where $\{e_i\}$ is an arbitrary orthonormal basis.

Exercise 1.4 Show that the definition does not depend on the choice of basis and that

$$\operatorname{Tr} A^* = \overline{\operatorname{Tr} A}, \quad \operatorname{Tr} AB = \operatorname{Tr} BA, \tag{1.11}$$

where the bar denotes the complex conjugate. Show that

$$\operatorname{Tr} |\psi\rangle\langle\varphi| A = \langle\varphi \mid A\psi\rangle. \tag{1.12}$$

Show that for $A, B \geq 0$

$$\operatorname{Tr} AB \geq 0, \tag{1.13}$$

with equality if and only if $AB = 0$.

The expression

$$\|T\|_1 = \operatorname{Tr} |T| \tag{1.14}$$

defines the trace norm on the complex linear space of all operators in $\mathcal{H}$. Note that for Hermitian T

$$\|T\|_1 = \sum_{i=1}^{d} |t_i| \tag{1.15}$$

where t_i are the eigenvalues of T. Another important norm is the operator norm

$$\|A\| \equiv \|A\|_\infty = \max_{\psi:\|\psi\|=1} \|A\psi\| \tag{1.16}$$

which for a Hermitian A is equal to

$$\|A\| = \max_{a \in \operatorname{spec}(A)} |a|. \tag{1.17}$$

There is an important inequality,

$$|\operatorname{Tr} TA| \leq \|T\|_1 \|A\|, \tag{1.18}$$

where equality can be attained either for any fixed T or for any fixed A : for a fixed T take $A = U^*$, where U is the unitary from the polar decomposition $T = U|T|$. Thus,

$$\|T\|_1 = \max_U |\operatorname{Tr} TU| = \max_{\|A\|=1} |\operatorname{Tr} TA|. \tag{1.19}$$

Similarly, for given A equality is attained for $T = |\psi\rangle\langle\psi|U^*$, where U is the unitary from the polar decomposition $A = U|A|$, and ψ is the normalized eigenvector of $|A|$, with the maximal eigenvalue. It follows that

$$\|A\| = \max_{\|T\|_1=1} |\operatorname{Tr} TA|. \tag{1.20}$$

These facts underly an important duality relation. The space of all operators in $\mathcal{H}$, equipped with the trace norm, becomes the complex Banach space $\mathfrak{T}(\mathcal{H})$. The same space equipped with the operator norm (and the product operation) is the Banach algebra $\mathfrak{B}(\mathcal{H})$. These two Banach spaces are in mutual duality, which means that every linear function on $\mathfrak{T}(\mathcal{H})$ has the form $T \to \operatorname{Tr} TA$ for some $A \in \mathfrak{B}(\mathcal{H})$, with the norm given by (1.20), and, conversely, every linear function on $\mathfrak{B}(\mathcal{H})$ has the form $A \to \operatorname{Tr} TA$ for some $T \in \mathfrak{T}(\mathcal{H})$ with the norm (1.19).

The subscript h will be applied to spaces of operators to denote the corresponding real Banach spaces of Hermitian operators. Then the real Banach spaces $\mathfrak{T}_h(\mathcal{H})$ and $\mathfrak{B}_h(\mathcal{H})$ are again in the mutual duality, provided by the bilinear form $T, A \to \operatorname{Tr} TA$. It follows from (1.11) that this form is real-valued for Hermitian T, A.

In the finite-dimensional case the spaces $\mathfrak{T}(\mathcal{H})$ and $\mathfrak{B}(\mathcal{H})$ coincide with the space of all operators in $\mathcal{H}$ and differ only by the norms. In the infinite-dimensional case, however, they are substantially different (just as the classical l^1 and l^∞ spaces over finite versus infinite sets).

Exercise 1.5 Show that the complex dimensionality of the space of all operators in $\mathcal{H}$ is d^2, while the real dimensionality of the subspace of all Hermitian operators in $\mathcal{H}$ is again d^2. If $\mathcal{H}$ is a real d-dimensional Hilbert space, the dimensionality of the space of all operators in $\mathcal{H}$ is d^2, while the dimensionality of the subspace of all symmetric operators in $\mathcal{H}$ is $d(d+1)/2$.

10.1.5 1.5 Convexity

A subset $\mathfrak{S}$ of a real linear space is convex if, for any finite collection of points $\{S_j\} \subset \mathfrak{S}$ and any probability distribution $\{p_j\}$, the convex combination $S = \sum_{j=1} p_j S_j$ is in $\mathfrak{S}$ (it is sufficient to impose this requirement only on collections of two points, which means that if the set $\mathfrak{S}$ contains two points, it must contain the whole segment connecting these points). In a convex set, a special role is played by extreme points, which cannot be represented as a nontrivial convex combination of other points. This is equivalent to the fact that $S = pS_1 + (1-p)S_2, 0 < p < 1$, implies $S = S_1 = S_2$, which means that there is no segment in $\mathfrak{S}$ containing S as its interior point. We denote by $\operatorname{ext}(\mathfrak{S})$ the set of all extreme points of a convex set $\mathfrak{S}$. The following general result holds.

Theorem 1.6 (Carathéodory). Let $\mathfrak{S}$ be a compact convex subset of $\mathbb{R}^n$. Then every point $S \in \mathfrak{S}$ can be represented as a convex combination of at most $n+1$ extreme points $S_j \in \operatorname{ext}(\mathfrak{S})$. We have

$$S = \sum_{j=1}^{n+1} p_j S_j, \quad S_j \in \operatorname{ext}(\mathfrak{S}). \tag{1.21}$$

As an example, consider the convex set $\mathfrak{P}_n$ of all probability distributions $P = \{p_1, \ldots, p_{n+1}\}$ on a set of $n+1$ points. Its extreme points are the degenerate distributions, for which all p_j are zero, except for one which is equal to 1 . There are $n+1$ extreme points and every point of $\mathfrak{P}_n$ is uniquely represented as their convex combination, with the coefficients p_j. This set is called simplex, and uniqueness of the representation is the characteristic feature of this convex set.

A real function $\mathcal{F}$ on a convex subset $\mathfrak{S}$ of a finite-dimensional linear space is convex (concave) if

$$\mathcal{F}\left(\sum_j p_j S_j\right) \leq (\geq) \sum_j p_j \mathcal{F}(S_j),$$

for an arbitrary convex combination of points $S_j \in \mathfrak{S}$. It is affine if it is both convex and concave. More generally, a map $\mathcal{F}$ from one convex set into another is called affine if it preserves convex combinations, i.e.,

$$\mathcal{F}\left(\sum_j p_j S_j\right) = \sum_j p_j \mathcal{F}(S_j).$$

Exercise 1.7 A continuous convex (in particular, affine) function on a compact convex set $\mathfrak{S}$ attains its maximum at an extreme point of this set.

10.1.6 1.6 Notes and References

The basics of the operator formalism of quantum mechanics were laid down in Dirac's classical treatise [64]. An excellent introduction to finite quantum systems is given in

Feynman's lectures [70]. From the vast variety of textbooks on linear algebra, we mention the modern course of Kostrikin and Manin [156], which takes into account the needs of quantum theory, and the book of Glazman and Ljubich [83], which is aimed at the active study of noncommutative, finite-dimensional analysis through solving problems. A variety of topics in modern matrix analysis, including many matrix inequalities, is covered in the book of Bhatia [31]. The fundamentals of convex analysis are exposed in, e.g., the books of Magaril-Il'jaev and Tikhomirov [172] and Rockafellar [194].

10.2 2 States, Observables, Statistics

10.2.1 2.1 Structure of Statistical Theories

10.2.2 2.1.1 Classical Systems

A classical system is described in terms of its phase space Ω, the points ω of which label deterministic states of the system. For simplicity, we consider in what follows finite sets Ω. By classical (statistical) state we denote a probability distribution $P = \{p_\omega\}$ on Ω. The collection of all probability distributions is the simplex $\mathfrak{P}(\Omega)$, in which every point is uniquely represented as a convex combination of extreme points - pure states, given by probability distributions that are degenerated in the points $\omega \in \Omega$. The simplest nontrivial system is the bit, the system with two pure states 0,1 , for which the set of statistical states is isomorphic to the unit segment of the real line.

Any random variable is a function $X = \{x_\omega\}$ on the phase space Ω, defining a decomposition of the space Ω into nonintersecting subsets Ω_x, in which X takes on the values x. The indicators $E_x(\omega)$ of these subsets satisfy the conditions

$$E_x(\omega)E_y(\omega) = \delta_{x,y}E_x(\omega), \quad \sum_x E_x(\omega) \equiv 1.$$

Along with random variables, which will henceforth be called sharp observables, one can consider unsharp observables which take the values x with probabilities $M(x \mid \omega)$ (such as observables with random error or intentionally randomized). The collection of conditional probabilities $M = \{M(x \mid \omega)\}$ is characterized by the properties

$$M(x \mid \omega) \geq 0, \quad \sum_x M(x \mid \omega) = 1.$$

For a sharp observable the probabilities $M(x \mid \omega) = E_x(\omega)$ are equal to 0 or 1 , i.e., $M(x \mid \omega)^2 = M(x \mid \omega)$.

The probability distribution for the observable M in the state P is given by the formula

$$\mu_P^M(x) = \sum_\omega p_\omega M(x \mid \omega). \tag{2.1}$$

For a smooth transition to quantum systems it is useful to introduce a matrix representation of the classical quantities. Consider the Hilbert space spanned by a fixed orthonormal basis $\{|\omega\rangle; \omega \in \Omega\}$. Given any function f_ω defined on Ω, we consider the diagonal operator

$$f = \sum_\omega f_\omega |\omega\rangle\langle\omega|.$$

Then a classical state gives rise to the operator $P = \sum_\omega p_\omega |\omega\rangle\langle\omega|$, characterized by the properties

$$P \geq 0, \quad \operatorname{Tr} P = 1. \tag{2.2}$$

A classical observable gives rise to the resolution of the identity, i. e., a collection of operators $M = \{M_x\}$, where

$$M_x = \sum_\omega M(x \mid \omega)|\omega\rangle\langle\omega|,$$

satisfying the conditions

$$M_x \geq 0, \quad \sum_x M_x = I. \tag{2.3}$$

For a sharp observable, the operators $M_x = E_x$ are pairwise orthogonal projectors. The relation (2.1) for the probability distribution of an observable can be rewritten as

$$\mu_P^M(x) = \operatorname{Tr} P M_x. \tag{2.4}$$

10.2.3 2.1.2 Axioms of Statistical Description

At the basis of the mathematical structure of quantum theory, as well as of any other statistical theory, lies the separation of a statistical experiment into the two stages of preparation and measurement, which underlies the duality between states and observables (Figure 2.1). The following set of axioms, which is applicable to any statistical theory, stresses the parallel between the statistical description of classical and quantum systems.

Figure 2.1: A quantum state described by a density operator S characterizes the preparation of a system, whereas the statistics of a measurement is described by a probability measure $\mu_S^M(x)$, where x labels the possible outcomes.

Axiom 1. Let there be a given set $\mathfrak{S}$, whose elements are called states, and a set $\mathfrak{M}$, whose elements are called (finite-valued) observables. For arbitrary $M \in \mathfrak{M}$, there is a finite set $\mathcal{X}^M$ of outcomes. For arbitrary $S \in \mathfrak{S}$ and $M \in \mathfrak{M}$, there is a probability distribution μ_S^M on $\mathcal{X}^M$, called the probability distribution of the observable M in the state S.

The state S is interpreted as a more or less detailed description of the preparation of a statistical ensemble, i. e., a sample of independent individual representatives of the system under consideration, and the observable M, as a quantity that can be measured by a definite apparatus for each representative in the given ensemble. Axiom 1 thus presupposes the reproducibility of the individual experiments and the stability of frequencies under independent repetitions.

The following axiom expresses the possibility of the mixing of statistical ensembles.

Axiom 2. For arbitrary $S_1, S_2 \in \mathfrak{S}$ and an arbitrary number $p, 0 < p < 1$, there exists an $S \in \mathfrak{S}$ such that $\mu_S^M = p\mu_{S_1}^M + (1-p)\mu_{S_2}^M$ for all $M \in \mathfrak{M}$; S is called the mixture of states S_1 and S_2 with weights $p, 1-p$.

The next axiom describes the possibility of processing the information obtained from a measurement of an observable. Let $M_1, M_2 \in \mathfrak{M}$, and let f be a function from $\mathcal{X}^{M_1}$ to $\mathcal{X}^{M_2}$ such that, for all $S \in \mathfrak{S}$,

$$\mu_S^{M_2}(y) = \sum_{x:f(x)=y} \mu_S^{M_1}(x)$$

where observable M_2 is called the coarse-graining of the observable M_1. In this case, we write $M_2 = f \circ M_1$.

Axiom 3. For an arbitrary observable $M_1 \in \mathfrak{M}$ and an arbitrary (necessarily, finitevalued) function f on $\mathcal{X}^{M_1}$, there exists an observable $M_2 \in \mathfrak{M}$, such that $M_2 = f \circ M_1$.

A pair of nonempty sets $(\mathfrak{S}, \mathfrak{M})$ satisfying Axioms $1 - 3$ will be called statistical model. The statistical model is said to be separated if the following Axiom holds.

Axiom 4. From the fact that $\mu_{S_1}^M = \mu_{S_2}^M$ for all $M \in \mathfrak{M}$ it follows that $S_1 = S_2$, and from $\mu_S^{M_1} = \mu_S^{M_2}$ for all $S \in \mathfrak{S}$ it follows that $M_1 = M_2$.

For a separated model both the operation of mixing in $\mathfrak{S}$ and the coarse-graining in $\mathfrak{M}$ are uniquely defined. Thus, the set of states $\mathfrak{S}$ obtains a convex structure, and the set of observables $\mathfrak{M}$ has the structure of a partial order.

Observables $M_1, \ldots, M_m$ are called compatible if they are all coarse-grainings of some observable M, that is, $M_j = f_j \circ M$ for $j = 1, \ldots, m$. The outcome of compatible observables can be obtained as a result of data post-processing in a single-measurement experiment. Statistical models in which all observables are compatible are, in fact, classical.

Proposition 2.1. Let $(\mathfrak{S}, \mathfrak{M})$ be a separated statistical model in which there exists the maximal observable M^*, such that all other observables are obtained by coarsegrainings of this maximal observable. Then there exist a finite set Ω, a one-to-one affine map $S \to P_S$ of the convex set of states $\mathfrak{S}$ into the set of all probability distributions on Ω, and a one-to-one map $M \to f_M$ of the set of observables $\mathfrak{M}$ onto a subset of random variables on Ω, preserving the relation of coarse-graining, such that

$$\mu_S^M(x) = \sum_{\omega:f_M(\omega)=x} P_S(\omega) \tag{2.5}$$

Proof. Let Ω be the set of outcomes of the maximal observable M^*, and let $P_S(\omega)$ be its probability distribution in a state S. According to the assumption of maximality, for any observable M there is a function f_M, such that the relation (2.5) holds. The fact that the maps $S \to P_S$ and $M \to f_M$ are one-to-one follows from the separatedness of the model. Checking the properties of the maps is left as an exercise to the reader. $\square$

Thus the outcome of this "maximal observable" constitutes the phase space Ω of the system, and all states are represented by probability measures on Ω. The main classical model is the Kolmogorov model, in which the set of states is a collection of all probability distributions $\mathfrak{P}(\Omega)$, and observables are described by random variables on Ω. The above proposition means that a statistical model in which all the observables are compatible can be embedded into the Kolmogorov model.

Another important classical model, which we call the Wald model, differs from Kolmogorov's model in that it embraces "unsharp" or "randomized" classical observables (see Section 2.1.1; randomization was consistently used by Wald in statistical decision theory and by von Neumann in game theory). To obtain a result similar to Proposition 2.1, one should introduce stochastic versions of coarse-graining and compatibility. Let $M_1, M_2 \in \mathfrak{M}$, and let Π be a transition probability from $\mathcal{X}^{M_1}$ to $\mathcal{X}^{M_2}$, such that for all $S \in \mathfrak{S}$

$$\mu_S^{M_2}(y) = \sum_x \Pi(y \mid x) \mu_S^{M_1}(x).$$

In this case, observable M_2 is called the stochastic coarse-graining of the observable M_1. Observables $M_1, \ldots, M_m$ are stochastically compatible, if they are all stochastic coarse-grainings of one observable M. In the Wald model, all observables are stochastically compatible and any separated model with this property can be embedded within a Wald model.

In the statistical model of quantum mechanics, states and observables are described by operators in a Hilbert space. Many efforts were spent on obtaining a reasonable axiomatic scheme, leading to the Hilbert space formalism of quantum mechanics. However, this is not our goal here and we will proceed in a different way. We take for granted the description of quantum states as density operators in a Hilbert space and derive from it the most general concept of quantum observable (including both "sharp" and "unsharp" observables), following from the axioms of the statistical model.

10.2.4 2.2 Quantum States

A state of a quantum-mechanical system represents a statistical ensemble of independent, identically prepared copies of the system.

Definition 2.2. A quantum state is described by a density operator, i.e., a Hermitian operator S in a Hilbert space $\mathcal{H}$ of the system, satisfying the conditions

$$S \geq 0, \quad \operatorname{Tr} S = 1.$$

Let $\mathfrak{S}(\mathcal{H})$ be the set of all density operators. It is a convex subset of the real linear space of all Hermitian operators in $\mathcal{H}$. A convex combination $S = \sum_j p_j S_j$ of density operators will describe the mixture of the corresponding statistical ensembles, obtained by taking ensembles prepared in the states S_j and mixing them with weights p_j. In a quantum-statistical ensemble there are two kinds of randomness. One is due to fluctuations in the classical parameters of the preparation procedure. The other one is the intrinsically quantum irreducible randomness, present in any quantum state. The following theorem characterizes states without classical randomness.

Theorem 2.3. Extreme points of the set of quantum states $\mathfrak{S}(\mathcal{H})$, called pure states, are precisely one-dimensional projectors.

Proof. The spectral decomposition of the Hermitian operator S reads

$$S = \sum_{i=1}^{d} s_i \left|e_i\right\rangle \left\langle e_i\right|, \quad s_j \geq 0, \sum s_j = 1 \tag{2.6}$$

where s_i are the eigenvalues and $|e_i\rangle$ are the eigenvectors of S. If S is extreme, this sum can contain only one nonzero term, implying that S is a one-dimensional projector. Conversely, let S be a one-dimensional projector, and

$$S = pS_1 + (1-p)S_2, \quad 0 < p < 1$$

Taking the square, we obtain

$$0 = S - S^2 = pS_1\left(I - S_1\right) + (1-p)S_2\left(I - S_2\right) + p(1-p)\left(S_1 - S_2\right)^2. \tag{2.7}$$

This equation is the sum of three positive operators, each of which must therefore be equal to zero. But this implies $S_1 = S_2 = S$, i. e., S is extreme.

From the viewpoint of probability theory, one-dimensional projectors are the noncommutative analog of distributions that are degenerated at some phase space point, while the role of the uniform distribution is played by the chaotic state, with the density operator $S = \frac{1}{d} I$.

Exercise 2.4 Show that if $\dim \mathcal{H} = d, \mathfrak{S}(\mathcal{H})$ can be embedded into the real vector space of dimensionality $n = d^2 - 1$. If $\mathcal{H}$ is a Euclidean (real Hilbert) space, then $n = d(d+1)/2 - 1$.

The spectral decomposition (2.6) shows that every quantum state is a mixture of no more than d pure states, where $d = \dim \mathcal{H}$. Thus, in the case of a set of quantum states, the Carathéodory theorem overestimates the number of extreme points that are actually present in the mixture(1.21). On the other hand, this theorem gives the exact value for the simplex of probability distributions on a "phase space" $\Omega = \{1, \dots, n+1\}$, representing the statistical states of a classical system. This suggests an idea of interpreting quantum theory as a probabilistic model with specific nonclassical constraints (a hidden-variable theory). For a single quantum system, such a viewpoint is possible, although up to now it did not prove to be productive compared to standard quantum mechanics. On the other hand, for composite systems this viewpoint leads to an inevitable contradiction with the physical principle of locality (separability) (see Section 3.2.1).

The simplest, and yet fundamental example is qubit - a two-level quantum system, $\dim \mathcal{H} = 2$. We use the canonical basis, i.e., $\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}$. It is convenient to introduce the basis in the real space of 2×2 Hermitian matrices, called Pauli matrices,

$$I \equiv \sigma_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

In particular, a density operator $S \in \mathfrak{S}(\mathcal{H})$ can be represented as

$$S = \frac{1}{2}\left(I + a_x\sigma_x + a_y\sigma_y + a_z\sigma_z\right) = \frac{1}{2}\begin{bmatrix} 1+a_z & a_x - ia_y \\ a_x + ia_y & 1-a_z \end{bmatrix}. \tag{2.8}$$

The condition $\det S \geq 0$ imposes the following constraint onto the Stokes parameters $\vec{a} = (a_x, a_y, a_z)$:

$$|\vec{a}|^2 \equiv a_x^2 + a_y^2 + a_z^2 \leq 1.$$

Thus, $\mathfrak{S}(\mathcal{H})$ as a convex set is isomorphic to the unit ball in $\mathbb{R}^3$, which we shall call the Bloch ball.

Exercise 2.5 Show that the density operator (2.8) has the eigenvalues $\frac{1 \pm |\vec{a}|}{2}$.

The pure states are characterized by the condition $a_x^2 + a_y^2 + a_z^2 = 1$ and form the Bloch sphere. By introducing Euler angles θ, ϕ, so that $a_z = \cos\theta, a_x + ia_y = \sin\theta e^{i\phi}$, we have $S = |\psi(\vec{a})\rangle\langle\psi(\vec{a})|$, where

$$|\psi(\vec{a})\rangle = \begin{bmatrix} \cos\frac{\theta}{2}e^{-i\phi/2} \\ \sin\frac{\theta}{2}e^{i\phi/2} \end{bmatrix}. \tag{2.9}$$

For an electron, which is a spin-1/2 particle, the vector $\psi(\vec{a})$ describes the pure state with the spin direction $\vec{a}$ produced by a Stern-Gerlach filter with this direction
of the magnetic field gradient. The mixed state, with $a_x = a_y = a_z = 0$, described by the density operator $S = \frac{1}{2}I$ for which all spin directions are equiprobable, is the chaotic state (see the Feynman lectures [70] for more detail).

Another important example of a two-level system is the polarization of a monochromatic photon, as visualized in classical optics experiments. In this case, the parameter $\frac{\theta}{2}$ is the angle of linear polarization, while $\frac{\phi}{2}$ characterizes circular polarization. For a linearly polarized photon $\phi = 0$. In particular, for a vertically polarized photon $\theta = 0$, while for a horizontally polarized one $\theta = \pi$.

10.2.5 2.3 Quantum Observables

10.2.6 2.3.1 Quantum Observables from the Axioms

Consider a statistical model in which the state space is the convex set $\mathfrak{S}(\mathcal{H})$ of all density operators in a Hilbert space $\mathcal{H}$. Let M be an observable. Now, by Axiom 2, the probabilities of the outcome of the measurement $\mu_S^M(x)$ should be affine functions of state.

Theorem 2.6. Let the map $S \to \mu_S$ be an affine function on $\mathfrak{S}(\mathcal{H})$ such that $0 \le \mu_S \le 1$. Then there exists an operator M on $\mathcal{H}$ with $0 \le M \le I$ such that, for every $S \in \mathfrak{S}(\mathcal{H})$,

$$\mu_S = \operatorname{Tr} SM \tag{2.10}$$

Proof (Sketch). Let us show that it is possible to extend the map $S \to \mu_S$ to a welldefined linear function on the space $\mathfrak{T}_h(\mathcal{H})$ of all Hermitian operators in $\mathcal{H}$.

First, we note that by separating positive and negative parts in the spectral decomposition (1.6), every Hermitian operator A can be represented as the difference of two positive operators, e. g., as in (1.8). Normalizing by the traces, we can always write

$$A = t_+ S_+ - t_- S_-, \quad t_\pm \ge 0, \quad S_\pm \in \mathfrak{S}(\mathcal{H}). \tag{2.11}$$

The representation of an operator A in the form of (2.11) is, of course, not unique.

Exercise 2.7 Using the affinity of the function $S \to \mu_S$, show that the value $\mu_A = t_+\mu_{S_+} - t_-\mu_{S_-}$ is uniquely defined (i.e., depends solely on the operator A, but not on the concrete decomposition of A into the difference of positive operators), and that $A \to \mu_A$ is a real, linear function.

Next, every operator A can be represented as $A = A_1 + iA_2$, where $A_1 = \frac{1}{2}(A + A^*)$, $A_2 = \frac{1}{2i}(A - A^*)$ are Hermitian operators. This representation is unique, and by setting $\mu_A = \mu_{A_1} + i\mu_{A_2}$, we obtain the unique complex linear extension of the function μ_A to the space of all linear operators in $\mathcal{H}$. Any such function apparently has the form

$$\mu_A = \operatorname{Tr} AM \tag{2.12}$$

where M is an operator in H. Taking $A = |\psi\rangle\langle\psi|$, where ψ is a unit vector and using (1.12), we have, by assumption, $0 \le \langle\psi \mid M\psi\rangle \le 1$ for all ψ, hence $0 \le M \le I$. □

A collection of operators $\{M_x, x \in \mathcal{X}\}$ is called the resolution of the identity or probability operator-valued measure [1] (POVM) on $\mathcal{X}$ if

$$M_x^* = M_x \ge 0, \quad \sum_x M_x = I$$

Corollary 2.8. Let $S \to \{\mu_S(x), x \in \mathcal{X}\}$ be an affine map of the convex set of quantum states $\mathfrak{S}(\mathcal{H})$ into the set of probability distributions on a finite set $\mathcal{X}$. Then there exists a POVM $M = \{M_x\}$ in $\mathcal{H}$ such that

$$\mu_S(x) = \operatorname{Tr} SM_x, \quad x \in \mathcal{X}. \tag{2.13}$$

The proof of the corollary is left as an exercise to the reader. This corollary leads to the following.

Definition 2.9. A quantum observable with outcomes in $\mathcal{X}$ is described by a POVM $\{M_x, x \in \mathcal{X}\}$. The probability distribution μ_S^M of the observable $M = \{M_x\}$ in a state S is given by formula (2.13).

By accepting this definition of a quantum observable, we introduce the maximal statistical model, with the state space coinciding with the set of all density operators and with the set of

observables consisting of all POVMs in $\mathcal{H}$. In the standard expositions of quantum mechanics, the more restricted notion of quantum observable is used.

Definition 2.10. The quantum observable is called sharp if all operators $M_x = E_x$ are projectors, i. e., $E_x^2 = E_x$.

Exercise 2.11 Show that the condition $E_x^2 = E_x$, for all outcomes x, is equivalent to $E_x E_y = \delta_{xy} E_x$ for all x, y, i. e., the projectors E_x are mutually orthogonal.

The corresponding resolutions of the identity are called orthogonal. Sharp observables are thus described by orthogonal resolutions of the identity in $\mathcal{H}$. Observables for which the outcomes are real numbers, i.e., $\mathcal{X} \subset \mathbb{R}$, are called real. The spectral decomposition

$$X = \sum_{x \in \mathcal{X}} x E_x$$

sets a one-to-one correspondence between sharp real observables $E = \{E_\chi\}$ and Hermitian operators X in $\mathcal{H}$ (which are also called observables). Coarse-graining for such

observables takes the form of functional calculus. Namely, for a function $f : \mathbb{R} \to \mathbb{R}$, an observable $f \circ E$ corresponds to the Hermitian operator $f(X)$ (exercise).

The expectation (mean value) of a sharp real observable X in the state S is given by the Born-von Neumann statistical formula

$$\mathrm{E}_S(X) = \sum x \mu_S^E(x) = \mathrm{Tr}\, SX.$$

The relation (2.13) can be regarded as an extension of this formula.
The statistical model in which states are described by density operators and observables - by Hermitian (self-adjoint) operators - was considered in great detail by von Neumann [237].

10.2.7 2.3.2 Compatibility and Complementarity

Definition 2.12. The commutator of the operators X, Y is $[X, Y] = XY - YX$. Operators X, Y commute if $[X, Y] = 0$.

Theorem 2.13. Let $E = \{E_x\}$ and $F = \{F_y\}$ be sharp observables. In this case, the following are equivalent:
i. E, F are compatible;
ii. projectors E_x and F_y commute for all x, y.

If E, F are real observables, this is equivalent to
iii. the corresponding Hermitian operators $X = \sum_x x E_x, Y = \sum_y y F_y$ commute.

Proof. ii $\Rightarrow$ i Put $M_{x,y} = E_x F_y = F_y E_x$. Since the product of commuting projections is a projector, $M = \{M_{x,y}\}$ is a (sharp) observable. Moreover, $E = f \circ M, F = g \circ M$, where $f(x, y) = x, g(x, y) = y$. Thus, E, F are compatible.
i $\Rightarrow$ ii If E, F are compatible, there exists an observable $M = \{M_z\}$ such that

$$E_x = \sum_{z : f(z) = x} M_z, \quad F_y = \sum_{z : g(z) = y} M_z$$

for some functions f, g (we agree to set M_z to zero if there is no z satisfying the condition in question).

Lemma 2.14. Let $0 \leq A \leq P$, where P is a projector. Then $[A, P] = 0$.
Proof. We have $(I - P)A(I - P) = 0$, hence $\sqrt{A}(I - P) = 0$, hence $A(I - P) = 0$, hence $A = AP$, hence $PA = (AP)^* = AP$. $\square$

[0]1 The term "positive operator-valued measure" is also used in the literature, which is however less precise, as it does not reflect the normalization of the measure.

Now, if $f(z) = x$, then $E_x \geq M_z$ and by Lemma 2.14 $[E_x, M_z] = 0$. If $f(z) \neq x$, $I - E_x \geq M_z$, and again $[E_x, M_z] = 0$. Thus, E_x commute with all M_z and hence with $F_y = \sum_{z:g(z)=y} M_z$.
ii $\Rightarrow$ iii This is obvious. Conversely, let $[X, Y] = 0$. In this case, $[f(X), g(Y)] = 0$ for arbitrary polynomials f, g. Taking the polynomials, which vanish at all points of the corresponding spectra except x (resp. y), we obtain $[E_x, F_y] = 0$. $\square$

If E, F are compatible, then denoting $\hat{M}_{xy} = \sum_{z:f(z)=x,g(z)=y} M_z$, we have

$$E_x = \sum_y \hat{M}_{xy}, \quad F_y = \sum_x \hat{M}_{xy}.$$

Observable $\hat{M}$ describes the statistics of joint measurement of E, F. Their joint probability distribution in the state S is given by

$$\mu_S^{EF}(x, y) = \operatorname{Tr} S\hat{M}_{xy}.$$

One can similarly define a joint measurement and probability distribution for an arbitrary finite collection of compatible observables.

Exercise 2.15 Show that the only observable compatible with all quantum observables is a constant, i.e., the observable equal to a scalar multiple of the unit operator.

Existence of (the vast variety of) incompatible observables is a manifestation of the quantum feature of complementarity. Physical measurements on micro-objects are implemented by macroscopic experimental devices, each of which requires a specific organization of the environment in space and time (such as, e.g., Stern-Gerlach experiments). Different ways of organization, corresponding to measurements of different observables, may be mutually exclusive (despite the fact that they relate to the identically prepared micro-object), i. e., complementary. Complementarity is the first fundamental distinction between quantum and classical statistical models.

Example 2.16. Consider a spin-1/2 particle, and let the unit vector $\vec{a} = (a_x, a_y, a_z)$ give a direction. Then

$$\sigma(\vec{a}) = a_x\sigma_x + a_y\sigma_y + a_z\sigma_z = \begin{bmatrix} a_z & a_x - ia_y \\ a_x + ia_y & -a_z \end{bmatrix} \tag{2.14}$$

is the observable of the projection of the spin[2] onto the direction $\vec{a}$. Indeed, the operator $\sigma(\vec{a})$ has the eigenvalues ± 1 (spin along and opposite the direction $\vec{a}$), and the spectral decomposition is given by

$$\sigma(\vec{a}) = |\psi(\vec{a})\rangle\langle\psi(\vec{a})| - |\psi(-\vec{a})\rangle\langle\psi(-\vec{a})|. \tag{2.15}$$

Recall that $\vec{a}$ has the Euler angles (θ, ϕ), and $\psi(\vec{a})$, given by (2.9), is the vector of the pure state in $\mathcal{H}$, with the spin direction $\vec{a}$. The corresponding density operator, which is the one-dimensional projector onto $\psi(\vec{a})$, is

$$S(\vec{a}) = |\psi(\vec{a})\rangle\langle\psi(\vec{a})| = \frac{I + \sigma(\vec{a})}{2}.$$

Exercise 2.17 Prove

$$\sigma(\vec{a}_1)\,\sigma(\vec{a}_2) = (\vec{a}_1 \cdot \vec{a}_2) / + i\sigma(\vec{a}_1 \times \vec{a}_2). \tag{2.16}$$

Written for the basis vectors this amounts to

[0]2 In physical applications there is a dimensional factor $\hbar/2$, which can be removed by an appropriate choice of units.

$$\sigma_x^2 = I, \qquad \sigma_y^2 = I, \qquad \sigma_z^2 = I$$
$$\sigma_x\sigma_y = i\sigma_z, \qquad \sigma_y\sigma_z = i\sigma_x, \qquad \sigma_z\sigma_x = i\sigma_y \tag{2.17}$$

Taking into account that $\operatorname{Tr}\sigma(\vec{a}) = 0$, the relation (2.16) implies the following formula for the mean value of $\sigma(\vec{b})$:

$$\operatorname{Tr} S(\vec{a})\sigma(\vec{b}) = \vec{a}\cdot\vec{b}$$

Another corollary of (2.16) is

$$[\sigma(\vec{a}_1), \sigma(\vec{a}_2)] = 2i\sigma(\vec{a}_1 \times \vec{a}_2), \tag{2.18}$$

which implies that $\sigma(\vec{a}_1), \sigma(\vec{a}_2)$ are compatible if and only if $\vec{a}_1 = \pm\vec{a}_2$. In particular, the spin components $\sigma_x, \sigma_y, \sigma_z$ are incompatible observables.

10.2.8 2.3.3 The Uncertainty Relation

If X, Y are two operators, we can write

$$XY = X \circ Y + \frac{1}{2}[X, Y]$$

where $X \circ Y = \frac{1}{2}(XY + YX)$ is the symmetrized or Jordan product of X, Y.
Let S be some state. For an arbitrary collection $X = \{X_1, \ldots, X_n\}$ of sharp, real observables we introduce two real matrices, one symmetric and another skew-symmetric,

$$\mathrm{B}_S(X) = \left[\operatorname{Tr} SX_j^0 \circ X_k^0\right]_{j,k=1,\ldots,n}, \quad \mathrm{C}_S(X) = \left[i\operatorname{Tr} S[X_j, X_k]\right]_{j,k=1,\ldots,n}, \tag{2.19}$$

where $X_j^0 = X_j - I\mathrm{E}_S(X_j)$. The matrix $\mathrm{B}_S(X)$ is called the covariance matrix, while $\mathrm{C}_S(X)$ is called the commutation matrix of X. We have

$$\mathrm{B}_S(X) \geq \pm\frac{i}{2}\mathrm{C}_S(X) \tag{2.20}$$

in the sense of an inequality between complex Hermitian matrices. Indeed, the Hermitian matrix

$$\mathrm{B}_S(X) - \frac{i}{2}\mathrm{C}_S(X) = \left[\operatorname{Tr} SX_j^0X_k^0\right]_{j,k=1,\ldots,n}$$

is positive definite, since for arbitrary $c_j \in \mathbb{C}$

$$\sum_{j,k=1}^{n} \bar{c}_j c_k \operatorname{Tr} SX_j^0X_k^0 = \operatorname{Tr} SZ^*Z \geq 0$$

where $Z = \sum_{j=1}^n c_jX_j^0$. This produces inequality (2.20) with the $+$sign. The inequality with the minus sign follows after taking the transposes.

For two observables $X_1 = X - I\mathrm{E}_S(X)$ and $X_2 = Y - I\mathrm{E}_S(Y)$, inequality (2.20) is equivalent to the Schrödinger-Robertson uncertainty relation

$$D_S(X)D_S(Y) \geq \{E_S((X - IE_S(X)) \circ (Y - IE_S(Y)))\}^2 + \frac{1}{4}|E_S[X, Y]|^2, \tag{2.21}$$

where

$$\mathrm{D}_S(X) = \mathrm{Tr}\, S\left(X - I\mathrm{E}_S(X)\right)^2 \tag{2.22}$$

is the variance of the sharp real observable X in the state S. The quantity

$$\mathrm{E}_S\left(X - I\mathrm{E}_S(X)\right) \circ \left(Y - I\mathrm{E}_S(Y)\right) \tag{2.23}$$

represents the covariance of X, Y in the state S. If the observables X, Y are compatible, this quantity coincides with the covariance of random variables, in the sense of probability theory, with respect to their joint probability distribution. In this case, $\mathrm{E}_S[X, Y] = 0$ and (2.21) reduces to the Cauchy-Schwarz inequality for the covariance of random variables. However, if X, Y are not compatible, X, Y are not measurable in a single experiment and the variances $\mathrm{D}_S(X), \mathrm{D}_S(Y)$ in the uncertainty relation refer to the two different measurements performed over different representatives of the same statistical ensemble, while the covariance is just a formal characteristic of the state.

Exercise 2.18 Prove the noncommutative Cauchy-Schwarz inequality

$$\left|\mathrm{Tr}\, SX^*Y\right|^2 \leq \mathrm{Tr}\, SX^*X\ \mathrm{Tr}\, SY^*Y, \tag{2.24}$$

for arbitrary state S and operators X, Y in $\mathcal{H}$.

10.2.9 2.3.4 Convex Structure of Observables

The set of all (finite-valued) quantum observables in a Hilbert space $\mathcal{H}$ will be denoted by $\mathfrak{M}(\mathcal{H})$. Given a Hilbert space $\mathcal{H}$, the sets $\mathfrak{S}(\mathcal{H})$ of quantum states and $\mathfrak{M}(\mathcal{H})$ of quantum observables, by construction, together with the generalized Born-von Neumann statistical rule (2.13), satisfy the axioms of separated statistical models. However, this model has an additional convexity structure in $\mathfrak{M}(\mathcal{H})$, which is to some extent similar to that of $\mathfrak{S}(\mathcal{H})$.

Let $\{M^j\}$ be a finite collection of observables with the same space of outcomes $\mathcal{X}$. Given a probability distribution $\{p_j\}$, we can define the mixture $M = \{M_x; x \in \mathcal{X}\}$ of these observables in an obvious way, i.e.,

$$M_x = \sum_j p_j M_x^j, \quad x \in \mathcal{X}. \tag{2.25}$$

Thus, the set $\mathfrak{M}_\mathcal{X}$ of all observables with a given space of outcomes $\mathcal{X}$ is a convex set. Similar to what is the case with states, mixtures of observables describe measurements with fluctuations in the classical parameters of the measuring procedure.

The following result describes the relation between observables without classical randomness and sharp observables.

Theorem 2.19. Any sharp observable $M \in \mathfrak{M}_\mathcal{X}$ is an extreme point of $\mathfrak{M}_\mathcal{X}$. In the reverse direction, an extreme observable $M \in \mathfrak{M}_\mathcal{X}$, with commuting components, $[M_X, M_{X'}] \equiv 0$, is sharp.

Proof. Let M be sharp, and assume $M = pM^1 + (1-p)M^2, 0 < p < 1$. In this case, similar to (2.7),

$$pM_x^1\left(I - M_x^1\right) + (1-p)M_x^2\left(I - M_x^2\right) + p(1-p)\left(M_x^1 - M_x^2\right)^2 = 0, \tag{2.26}$$

and therefore $M_x^1 \equiv M_x^2 \equiv M_x$, and M is extreme.
Now note that in all cases, $M_x \leq I$ and hence $M_x^2 \leq M_x$. Taking some $x \in \mathcal{X}$ we have

$$M_x = \frac{1}{2}M_x^2 + \frac{1}{2}\left(2M_x - M_x^2\right), \tag{2.27}$$

$$M_{x'} = \frac{1}{2}M_{x'}\left(I + M_x\right) + \frac{1}{2}M_{x'}\left(I - M_x\right), \quad x' \neq x. \tag{2.28}$$

If $[M_x, M_{x'}] \equiv 0$, these relations represent M as a convex combination (with equal weights) of two other observables. If M is extreme, they should coincide with M, in particular $M_x^2 = M_x$. Hence, M is sharp. $\square$

It follows that in the classical case extreme observables coincide with the sharp ones, giving them a very clear characterization as observables without randomness in the measuring procedure. In the quantum statistical model, things are not so simple (and much more interesting). We call the two-valued observables tests (they are also called propositions, questions, effects in the literature, and they play a central role in various axiomatic approaches although, they have a rather special property
as concerns the important issue of extremity). The set of extreme quantum observables is exhausted by sharp observables only in this case of two outcomes. This fact follows from the theorem, because any test necessarily has commuting components $\{M_0, M_1 = I - M_0\}$. Thus, any extreme test is completely determined by the projector $P = M_0$.

For observables with more than two values, we consider the following construction.

Definition 2.20. Let $\{|\psi_x\rangle\}$ be an arbitrary finite collection of not necessarily normalized vectors in $\mathcal{H}$ such that $\sum_x |\psi_x\rangle \langle\psi_x| = I$. Such a collection is called an overcomplete system.

If $\{|\psi_x\rangle\}$ is an overcomplete system, an arbitrary vector $|\psi\rangle \in \mathcal{H}$ can be represented as a linear combination

$$|\psi\rangle = \sum_x c_x |\psi_x\rangle \qquad \text{with } c_x = \langle\psi_x \mid \psi\rangle, \tag{2.29}$$

where the coefficients $\{c_x\}$ need not be unique, because the vectors $|\psi_x\rangle$ may be linearly dependent. There also is a corresponding matrix representation of the operators. In a d-dimensional Hilbert space, overcomplete systems with more than d vectors always exist, and they can be built from any complete (possibly, linearly dependent) system as follows. Let $\{|\phi_x\rangle\}$ be a complete system of vectors in $\mathcal{H}$. The corresponding Gram operator is defined by

$$G = \sum_x |\phi_x\rangle \langle\phi_x|. \tag{2.30}$$

Completeness implies that G is nondegenerate. Now, $\{|\psi_x\rangle\}$, with $|\psi_x\rangle = G^{-1/2}|\phi_x\rangle$, is an overcomplete system because

$$\sum_x |\psi_x\rangle \langle\psi_x| = G^{-1/2} \sum_x |\phi_x\rangle \langle\phi_x| G^{-1/2} = I. \tag{2.31}$$

An overcomplete system determines a quantum observable M with the components

$$M_x = |\psi_x\rangle \langle\psi_x|, \quad x \in \mathcal{X}. \tag{2.32}$$

In particular, for any orthonormal basis $\{e_x\}$, the observable $M = \{|e_x\rangle \langle e_x|\}$ is sharp and, hence, an extreme observable.

Theorem 2.21. An observable (2.32) is extreme if and only if the operators M_x are linearly independent in the real vector space $\mathfrak{B}_h(\mathcal{H})$.

Proof. Let M be extreme and assume that

$$\sum_x c_x \left|\psi_x\right\rangle \left\langle\psi_x\right| = 0 \tag{2.33}$$

For $\epsilon > 0$ small enough, we define

$$M_x^{\pm} = (1 \pm \epsilon c_x)\, M_x \geq 0, \quad x \in \mathcal{X}.$$

Then $M^{\pm}$are observables and, by construction, $M = \frac{1}{2}M^+ + \frac{1}{2}M^-$. Therefore, $M_x^+ = M_x^- = M_x$ since M is extreme. Thus, (2.33) implies $c_x = 0$, i. e., the components of M are linearly independent.

Conversely, let

$$\left|\psi_x\right\rangle \left\langle\psi_x\right| = pM_x^1 + (1-p)M_x^2$$

be a convex decomposition of M. In this case, $0 \leq pM_x^1 \leq \left|\psi_x\right\rangle \left\langle\psi_x\right|$. By Lemma 2.14,

$$M_x^1 \left|\psi_x\right\rangle \left\langle\psi_x\right| = \left|\psi_x\right\rangle \left\langle\psi_x\right| M_x^1 = \left\langle\psi_x \mid \psi_x\right\rangle M_x^1,$$

whence $M_x^1 = \lambda_x \left|\psi_x\right\rangle \left\langle\psi_x\right|$, with $\lambda_x = \left\langle\psi_x\right| M_x^1 \left|\psi_x\right\rangle / \left\langle\psi_x \mid \psi_x\right\rangle^2$. Now, $\sum_x \lambda_x \left|\psi_x\right\rangle \left\langle\psi_x\right| = I$, i. e.,

$$\sum_x (\lambda_x - 1) \left|\psi_x\right\rangle \left\langle\psi_x\right| = 0.$$

Due to the linear independence of M_x, we must have $\lambda_x = 1$, and $M_x^1 = M_x$ for all x, which means that M is extreme.

From the result of Exercise 1.5, it follows that the dimensionality of the real space of Hermitian operators is equal to d^2. Thus, all overcomplete systems with n linearly independent components, $d < n \leq d^2$, determine unsharp extremal observables. A concrete example of such an observable with $n = 3, d = 2$ will be considered in the next section.

10.2.10 2.4 Statistical Discrimination Between Quantum States

10.2.11 2.4.1 Formulation of the Problem

In this section, we consider a statistical decision problem which will allow us to pass to the optimal information transmission via quantum channels in Part II of the book.

Let a quantum system be prepared in one of the states $S_x, x = 1, \ldots, n$. The observer is allowed to perform arbitrary measurements aimed at determining, in the best possible way, in which of these states, given a priori, the system was actually prepared. This kind of decision problem is typical for mathematical statistics and its applications in communication theory, where we deal with the optimal signal detection or estimation (see Section 3.3.1). On the other hand, in high-precision experiments, researchers are already able to operate with elementary quantum systems such as single ions, atoms, and photons. This leads to potentially important applications, such as quantum communication and quantum cryptography. A quite important issue is that of extracting the maximum possible information about the state of a given quantum system. In proposals currently under discussion for application to quantum computing, the information is written into states of elementary quantum cells, qubits, and is read via quantum measurements. From a statistical point of view, a measurement gives an estimate for the quantum state, either as a whole, or for some of its components (parameters), and the problem of finding the most informative measurement arises.

The statistic of the whole measurement procedure is described by an observable, i. e., by resolution of the identity $M = \{M_x\}$ in the system space $\mathcal{H}$. The probability to make a decision y, under the condition that the system was in the state S_x, is equal to $p_M(y \mid x) = \operatorname{Tr} S_x M_y$. In particular, the probability of making a correct decision is equal to $p_M(x \mid x)$. Let us additionally assume that the states S_x appear with probabilities π_x (e.g., in the case of equiprobable states $\pi_x = 1/n$). In this case, the average probability of making a correct decision is equal to

$$\mathcal{P}\{M\} = \sum_{x=1}^{n} \pi_x p_M(x \mid x)$$

and the problem is to maximize it with respect to all possible observables M.

10.2.12 2.4.2 Optimal Observables

Denoting by $W_x = \pi_x S_x \geq 0$ the average probability of a correct decision can be written explicitly as an affine function,

$$\mathcal{P}\{M\} = \sum_{x=1}^{n} \operatorname{Tr} W_x M_x$$

on the convex set of observables with n outcomes

$$\mathfrak{M}_n = \left\{ M = \{M_x\}_{x=1,\ldots,n} : M_x \geq 0, \sum_{x=1}^{n} M_x = I \right\}.$$

Maximization of an affine function defined on a compact convex set is a typical convex programming problem.

Theorem 2.22. The average probability of a correct decision $\mathcal{P}\{M\}$ attains its maximum at an extreme point of the set $\mathfrak{M}_n$. An observable M^0 is optimal if and only if there exists a Hermitian operator Λ, such that

i. $(\Lambda - W_x)\, M_x^0 = 0$;

ii. $\Lambda \geq W_x$.

The following duality relation holds:

$$\max\{\mathcal{P}\{M\} : M \in \mathfrak{M}_n\} = \min\{\operatorname{Tr}\Lambda : \Lambda \geq W_x, x = 1, \ldots, n\} \tag{2.34}$$

Proof. Since $\mathcal{P}\{M\}$ is a continuous affine function on a compact convex set $\mathfrak{M}_n$, the first statement follows from the result of Exercise 1.7.

Let us first prove the sufficiency of the conditions i, ii. Let Λ be a Hermitian operator satisfying the conditions i, ii. By using these conditions and the property (1.13), we obtain

$$\mathcal{P}\{M\} = \operatorname{Tr} \sum_x W_x M_x \leq \operatorname{Tr} \sum_x \Lambda M_x = \operatorname{Tr}\Lambda. \tag{2.35}$$

From i , we have $\Lambda M_x^0 = W_x M_x^0$. If we sum over x and take the trace of the resulting equation, we obtain

$$\operatorname{Tr}\Lambda = \operatorname{Tr}\Lambda \sum_x M_x^0 = \operatorname{Tr} \sum_x W_x M_x^0 = \mathcal{P}\left\{M^0\right\}. \tag{2.36}$$

Hence, we obtain

$$\mathcal{P}\{M\} \leq \mathcal{P}\left\{M^0\right\}, \quad \text{for all } M, \tag{2.37}$$

and therefore M^0 maximizes $\mathcal{P}$. Note that

$$\Lambda = \sum_x W_x M_x^0 = \sum_x M_x^0 W_x.$$

Now, we prove the necessity. Put $M_x = A_x^2$, where A_x are Hermitian operators satisfying the condition $\sum_x A_x^2 = I$. Applying the method of Lagrange multipliers, we can reduce the problem of maximizing $\mathcal{P}\{M\}$ on the set $\mathfrak{M}_n$ to the problem of maximizing the function

$$\operatorname{Tr} \sum_x W_x A_x^2 - \operatorname{Tr} \Lambda \left(\sum_x A_x^2 - I \right), \tag{2.38}$$

where Λ is a Hermitian operator, over all collections of Hermitian operators A_x. Here, the matrix elements of the Hermitian operator Λ represent the array of the Lagrange multipliers for this problem. Let A_x^0 be the optimal collection. In addition, let $A_x = A_x^0 + \epsilon Y_x$, with Hermitian Y_x, and consider (2.38) as a function of ϵ. By considering the coefficients of ϵ and ϵ^2, we obtain the conditions

$$\operatorname{Tr} \left[(W_x - \Lambda) A_x^0 + A_x^0 (W_x - \Lambda) \right] Y_x = 0$$
$$\operatorname{Tr} (W_x - \Lambda) Y_x^2 \leq 0$$

for an arbitrary Hermitian Y_χ, i.e.,

$$(W_x - \Lambda) A_x^0 + A_x^0 (W_x - \Lambda) = 0, \quad \Lambda - W_x \geq 0.$$

The second inequality is just condition ii of the theorem. By putting $M_x^0 = (A_x^0)^2$, the first relation implies $\operatorname{Tr} (\Lambda - W_x) M_x^0 = 0$, which, together with the second inequality, leads to condition i. □

Exercise 2.23 Prove that the operator Lagrange multiplier Λ is the unique solution Λ^0 of the dual problem on the right side of (2.34).

Let us illustrate the meaning and applications of these conditions with some examples.

Example 2.24. Consider the classical case where all density operators S_x, and hence the operators W_x, commute. In this case, there is a common orthonormal basis $\{|\omega\rangle\}$ in which they are all diagonal,

$$W_x = \sum_\omega W_x(\omega) |\omega\rangle\langle\omega|.$$

In this case, the dual problem has the unique solution

$$\Lambda^0 = \sum_\omega \max_x W_x(\omega) |\omega\rangle\langle\omega|,$$

where $\max_x W_x(\omega)$ is the upper envelope of the family of functions $W_x(\omega), x = 1, \ldots, n$. A solution of the initial problem is given by the formula

$$M_x^0 = \sum_\omega \mathbf{1}_{\Omega_x}(\omega) |\omega\rangle\langle\omega|,$$

where $\mathbf{1}_{\Omega_x}$ denotes the indicator of the subset Ω_x, where subsets $\Omega_x \subseteq \{\omega : \Lambda^0(\omega) = W_X(\omega)\}$ are assumed to be nonintersecting and to constitute a partition of the set $\Omega = \{\omega\}$.

This solution amounts to the principle of maximal likelihood in classical statistics. The decision x should be taken for those observations ω for which the posterior gain $W_x(\omega)$ is maximal. Thus, in the classical case, the optimal observable can always be chosen sharp. This is directly related to the fact that in the commutative case extreme points of the set $\mathfrak{M}_n$ are precisely the orthogonal resolutions of the identity (cf. Theorem 2.19).

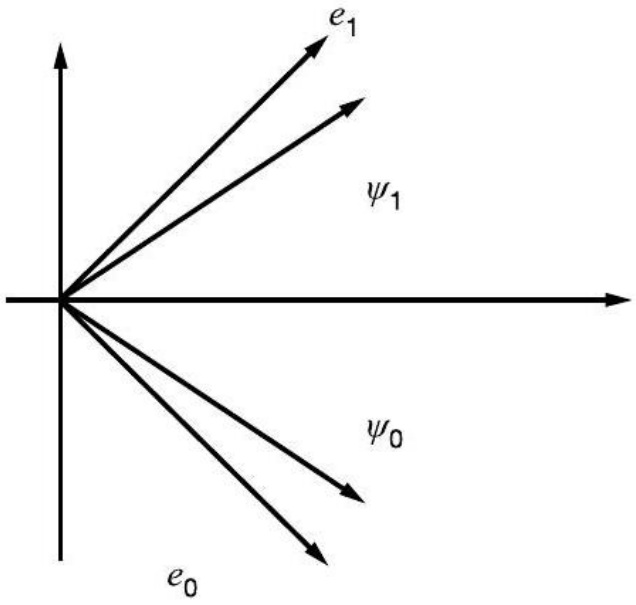


Figure 2.2: Discrimination between two pure states.

Example 2.25 (Discrimination Between the Two States). Let S_0, S_1 be two density operators, with π_0, π_1 their a priori probabilities. An observable (test) is given by resolution of the identity $\{M_0, M_1\}$, so that $M_0 + M_1 = I$. This case can be reduced to the previous one, by representing

$$W_0 = \pi_1 S_1 + W_0', \quad W_1 = \pi_1 S_1 + W_1',$$

where the operators $W_0' = \pi_0 S_0 - \pi_1 S_1, W_1' = 0$ commute. Thus

$$\mathcal{P}\{M\} = \pi_1 + \mathrm{Tr}\,(W_0' M_0 + W_1' M_1)\,, \tag{2.39}$$

and

$$\Lambda^0 = \max\{\pi_0 S_0 - \pi_1 S_1, 0\} = (\pi_0 S_0 - \pi_1 S_1)_+\,. \tag{2.40}$$

Any optimal M_0^0 has the form

$$M_0^0 = \mathbf{1}_{(0,\infty)}\,(\pi_0 S_0 - \pi_1 S_1) + X_0, \tag{2.41}$$

where the first term is the projector onto the positive part of the spectrum of $\pi_0 S_0 - \pi_1 S_1$, and the second is an operator supported by the null subspace of $\pi_0 S_0 - \pi_1 S_1$, such that $0 \le X_0 \le I$. The maximum is given by

$$\mathcal{P}\{M\} = \pi_1 + \mathrm{Tr}\,(\pi_0 S_0 - \pi_1 S_1)_+\,. \tag{2.42}$$

By using the relation

$$(\pi_0 S_0 - \pi_1 S_1)_+ = \frac{1}{2}\,|\pi_0 S_0 - \pi_1 S_1| + \frac{1}{2}\,(\pi_0 S_0 - \pi_1 S_1)\,,$$

we obtain

$$\max \mathcal{P}\{M\} = \frac{1}{2}\,(1 + \|\pi_0 S_0 - \pi_1 S_1\|_1)\,.$$

In particular, taking $\pi_0 = \pi_1 = \frac{1}{2}$, we have

$$\max \mathcal{P}\{M\} = \frac{1}{2}\left(1 + \frac{1}{2}\left\|S_0 - S_1\right\|_1\right),$$

so that the more distinguishable the density operators S_0 and S_1 are in the sense of the trace norm, the greater the maximum will be.

Proposition 2.26. Let $S_0 = |\psi_0\rangle\langle\psi_0|, S_1 = |\psi_1\rangle\langle\psi_1|$ be pure states. In this case, the maximum of $\mathcal{P}\{M\}$ is given by

$$\max_M \mathcal{P}\{M\} = \frac{1}{2}\left(1 + \sqrt{1 - 4\pi_0\pi_1 |\langle\psi_0 \mid \psi_1\rangle|^2}\right), \tag{2.43}$$

and is achieved on a sharp observable. In particular, if $\pi_0 = \pi_1 = 1/2$, the maximum is equal to

$$\max_M \mathcal{P}\{M\} = \frac{1}{2}\left(1 + \sqrt{1 - |\langle\psi_0 \mid \psi_1\rangle|^2}\right). \tag{2.44}$$

Proof. Consider the eigenvalue problem for the rank two operator

$$\pi_0 |\psi_0\rangle\langle\psi_0| - \pi_1 |\psi_1\rangle\langle\psi_1|.$$

This operator may have eigenvalue zero, corresponding to the orthogonal complement to its support, which is just the linear span $\mathcal{L}$ of the vectors $|\psi_0\rangle, |\psi_1\rangle$. The relevant part of the optimal observable is also supported by $\mathcal{L}$, so we can restrict ourselves to the eigenvectors that are linear combinations, i.e.,

$$|\psi\rangle = c_0 |\psi_0\rangle + c_1 |\psi_1\rangle.$$

Substituting this into the eigenvector equation results in

$$\pi_0 (c_0 + \langle\psi_0 \mid \psi_1\rangle c_1) = \lambda c_0 \tag{2.45}$$
$$-\pi_1 (\langle\psi_1 \mid \psi_0\rangle c_0 + c_1) = \lambda c_1 \tag{2.46}$$

whence the eigenvalues are

$$\lambda_{0,1} = \frac{1}{2}\left[\pi_0 - \pi_1 \pm \sqrt{1 - 4\pi_0\pi_1 |\langle\psi_0 \mid \psi_1\rangle|^2}\right]$$

with the corresponding orthonormal basis of eigenvectors $|e_0\rangle, |e_1\rangle$. Now,

$$\|\pi_0 |\psi_0\rangle\langle\psi_0| - \pi_1 |\psi_1\rangle\langle\psi_1|\|_1 = \lambda_0 - \lambda_1 = \sqrt{1 - 4\pi_0\pi_1 |\langle\psi_0 \mid \psi_1\rangle|^2}$$

and we get (2.43).

The sharp optimal observable in the subspace $\mathcal{L}$ is just $\{|e_0\rangle\langle e_0|, |e_1\rangle\langle e_1|\}$. If $\pi_0 = \pi_1 = 1/2$, the optimal basis is situated symmetrically with respect to $|\psi_0\rangle, |\psi_1\rangle$ (see Figure 2.2).

Example 2.27. On a plane (considered as a real subspace of two-dimensional complex space), consider an "equiangular" configuration of the three vectors (see Figure 2.3)

$$|\psi_j\rangle = \begin{bmatrix} \cos\frac{2j\pi}{3} \\ \sin\frac{2j\pi}{3} \end{bmatrix}, \quad j = 0, 1, 2 \tag{2.47}$$

The corresponding density matrices $S_j = |\psi_j\rangle\langle\psi_j|$ describe the states of a two-level quantum system such as a linearly polarized photon or a spin-1/2 particle.

We have

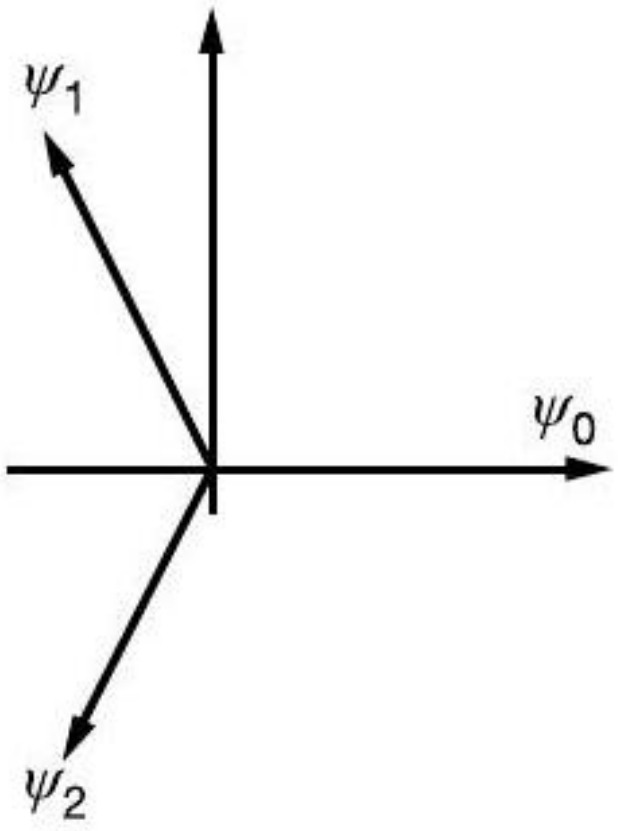


Figure 2.3: Trine on the plane.

$$S_j = \frac{1}{2}\left(I + \begin{bmatrix} \cos\frac{4j\pi}{3} & \sin\frac{4j\pi}{3} \\ \sin\frac{4j\pi}{3} & -\cos\frac{4j\pi}{3} \end{bmatrix}\right), \tag{2.48}$$

so that

$$\sum_{j=0}^{2} S_j = \frac{3}{2} I$$

because $\sum_{j=0}^{2} e^{i\frac{4\pi j}{3}} = 0$.

It follows that $M_k^0 = \frac{2}{3} S_k, k = 0, 1, 2$, is the resolution of the identity that corresponds to the overcomplete system $\left\{\sqrt{\frac{2}{3}}\,|\psi_k\rangle\,; k = 0, 1, 2\right\}$. The corresponding observable is extremal, since it satisfies the conditions of Theorem 2.21.

Let us show that, in the case of equiprobable states $\pi_j = 1/3$, observable $\{M_k^0\}$ is optimal, by checking the conditions of Theorem 2.22. Since $S_j^2 = S_j$,

$$\Lambda^0 = \sum_{j=0}^{2} \frac{1}{3} S_j M_j^0 = \frac{2}{9} \sum_{j=0}^{2} S_j = \frac{1}{3} I$$

so that condition ii is satisfied; $I/3 = \Lambda^0 \geq S_j/3$. Condition i is also satisfied since

$$\left(\Lambda^0 - \frac{1}{3} S_j\right) M_j^0 = \frac{1}{3}\left(I - S_j\right) S_j = 0.$$

Thus, $\max \mathcal{P}\{M\} = \operatorname{Tr} \Lambda^0 = 2/3$. Let us now find the maximum over all sharp observables with three outcomes. A nontrivial orthogonal resolution of the identity with three components

in the two-dimensional space has the form $M_0 = |e_0\rangle\langle e_0|$, $M_1 = |e_1\rangle\langle e_1|, M_2 = 0$, where $|e_0\rangle, |e_1\rangle$ is an arbitrary basis. Thus, the problem reduces to the optimal discrimination of the two equiprobable states S_0, S_1. Applying relation (2.44) to the case $\langle\psi_0 \mid \psi_1\rangle = -\frac{1}{2}$, we obtain

$$\max_{M-\text{ sharp}} \mathcal{P}\{M\} = \frac{2}{3}\frac{1+\sqrt{3}/2}{2} < \frac{2}{3} = \max_{M\in\mathfrak{M}} \mathcal{P}\{M\}.$$

Thus, in the quantum state discrimination, using unsharp observables can lead to an improvement in comparison with the sharp ones. Let us stress that in the similar classical problem (of discrimination between probability distributions) unsharpness or randomization can never lead to such an improvement. From a geometrical point of view, the reason for this phenomenon is, of course, that in the quantum case not all extremal observables (among which the optimal one is found) are sharp ones.

10.2.13 2.5 Notes and References

1. Among the texts devoted to the mathematical foundations of quantum mechanics let us mention the monographs of von Neumann [237], Mackey [171], Segal [204], Faddeev and Yakubovsky [68]. A survey of axiomatic approaches is given in the paper of Wightman [246] and also in the Comments to Chapter VIII of the book of Reed and Simon [193]. One aim of any axiomatics that is longed for is a derivation of the Hilbert space formalism. Such a derivation within the framework of the operational approach (see below) was realized, in the finite-dimensional case, in the paper of Araki [8] (for a more recent approach, see Hardy [92]). However, this is a separate topic; for our purposes it will suffice to postulate the state space $\mathfrak{S} = \mathfrak{S}(\mathcal{H})$.

The description of mixed states by density operators (matrices) was introduced independently by von Neumann, Weyl, and Landau (see footnote 172 in Section IV. 2 of von Neumann's book [237]).

The axiomatic approach, in which the central role is played by the duality between the two partially ordered linear spaces, generated by a convex set of quantum states, and by the order interval $[0, I]$ of two-valued observables (effects or tests), was developed by the school of Ludwig [170], [73]; see also Davies [56] (this approach is usually called operational). A detailed investigation of the statistical structure of quantum theory, based on the operational approach, is undertaken in the books [122], [115], where one can find a detailed bibliography.

In Proposition 2.1, we had to assume the existence of the maximal observable for the sole reason that, for simplicity, from the beginning we restricted ourselves to observables with finite sets of outcomes. With an appropriate generalization the existence of the maximal observable (in general, with an infinite Ω) can be deduced from compatibility of all observables of the model. Essentially, this is the message of the famous Kolmogorov extension theorem for a random process defined by system of compatible finite-dimensional distributions. A detailed study of the notion of stochastic compatibility, including the proof that the separated model, in which all observables are stochastically compatible, can be embedded within the Wald model, can be found in the paper [112].

A brief introduction to the basic notions of quantum theory targeted at quantum information science is given in the books of Nielsen and Chuang [179] and Hayashi [95]. The papers of Fuchs [75], Chiribella et al. [45], Masanes and Müller [175] and the book of D'Ariano et al. [54] elaborate on information-theoretical approaches to the foundations of quantum theory.

2. The generalized concept of a quantum observable presented here was developed by Ludwig [170], Davies and Lewis [56], and Holevo [122]. As concerns the convex structure of the set of observables, see Kraus [157]. In analysis and in signal theory, overcomplete systems are known under the name "(rigid) frames."

The spin of a quantum particle is intrinsically related to representations of the group of rotations of three-dimensional Euclidean space [245], [70], [171]. Results related to Theorem 2.21 are discussed in the paper of Davies [55].

3. The problem of discriminating the two pure quantum states was treated, in 1968, in the paper of Bakut and Shchurov [16]. Such problems arise naturally in connection with the detection of weak light sources, and in quantum optics [103]. A physical device that achieves the bound (2.43) for two coherent states of a radiation field (see Chapter 12), called Dolinar receiver, was described in [103]. It uses photon counting as a measurement, together with an ingenious feedback from the output of the photon detector to the input field of the counter.

General detection and estimation theory for quantum states was developed in the 1970s in works of Helstrom [102], Holevo [107], Yuen and Lax [260], Stratonovich [228], Belavkin [20], and other authors. Example 2.27, with the three equiangular states, was proposed in [110]. For further details and extensive references, see the monographs [103], [122]. The new interest in quantum estimation theory emerged in connection with the ideas of quantum computation. Any such computation is completed by measuring parameters of the final state of the quantum computer, which should be maximally precise. The achievements of modern quantum estimation theory, including asymptotic theory, are presented in the books of Hayashi [95] and Petz [190]. The Bayes problem is a convex programming problem (see [172], [194]), and Theorem 2.22 could be proved basing on the corresponding duality theorem. An interesting variation of this problem proposed by Peres [187] concerns the unambiguous discrimination between quantum states when an inconclusive result is allowed. For a survey of the recent status of the field see, e. g., Herzog [104].

10.3 3 Composite Systems and Entanglement

10.3.1 3.1 Composite Systems

10.3.2 3.1.1 Tensor Products

The new possibilities that are offered by quantum information are to a large extent due to the unusual features of composite quantum systems. Let $\mathcal{H}_j, j = 1, 2$, be the Hilbert spaces of two finite quantum systems with inner products $\langle \cdot \mid \cdot \rangle_j$. The combination of the two systems is described by the tensor product of the Hilbert spaces, which is defined as follows.

According to Section 1.1, the element $\psi \in \mathcal{H}$ defines the antilinear function $\psi(\phi) = \langle \phi \mid \psi \rangle$ of the argument $\phi \in \mathcal{H}$. For any two elements $\psi_j \in \mathcal{H}_j, j = 1, 2$, we denote by $\psi_1 \otimes \psi_2$ the bi-antilinear function of the arguments $\phi_1 \in \mathcal{H}_1, \phi_2 \in \mathcal{H}_2$, defined by the relation

$$(\psi_1 \otimes \psi_2)(\phi_1, \phi_2) = \langle \phi_1 \mid \psi_1 \rangle_1 \langle \phi_2 \mid \psi_2 \rangle_2 .$$

Consider the vector space $\mathcal{L}$ of finite linear combinations of such functions $\sum_j c_j \psi_1^j \otimes \psi_2^j$. Introduce the inner product in $\mathcal{L}$ by letting

$$\langle \varphi_1 \otimes \varphi_2 \mid \psi_1 \otimes \psi_2 \rangle = \langle \varphi_1 \mid \psi_1 \rangle_1 \langle \varphi_2 \mid \psi_2 \rangle_2$$

on the generating elements $|\psi_1 \otimes \psi_2\rangle \equiv |\psi_1\rangle \otimes |\psi_2\rangle$ and extending, by linearity, to $\mathcal{L}$.

Exercise 3.1 Show that such a linear extension is possible and that it is unique and satisfies all the properties of an inner product.

Definition 3.2. The space $\mathcal{L}$ with the inner product defined above is called the tensor product $\mathcal{H}_1 \otimes \mathcal{H}_2$ of the Hilbert spaces $\mathcal{H}_1, \mathcal{H}_2$.

Exercise 3.3 Prove the following statement. If $\{e_1^j\}, \{e_2^k\}$ are orthonormal bases in $\mathcal{H}_1, \mathcal{H}_2$, then $\{e_1^j \otimes e_2^k\}$ is an orthonormal basis in $\mathcal{H}_1 \otimes \mathcal{H}_2$ and $\dim \mathcal{H}_1 \otimes \mathcal{H}_2 = \dim \mathcal{H}_1 \times \dim \mathcal{H}_2$.

It follows that any vector $\psi \in \mathcal{H}_1 \otimes \mathcal{H}_2$ is uniquely represented in the form

$$|\psi\rangle = \sum_{j,k} c_{jk} \left|e_1^j\right\rangle \otimes \left|e_2^k\right\rangle,$$

where c_{jk} are complex numbers. Summing with respect to j and denoting $|\psi_k\rangle = \sum_{j=1}^{d_1} c_{jk} \left|e_1^j\right\rangle \in \mathcal{H}_1$, we obtain

$$|\psi\rangle = \sum_{k=1}^{d_2} |\psi_k\rangle \otimes \left|e_2^k\right\rangle,$$

which means that the space $\mathcal{H}_1 \otimes \mathcal{H}_2$ is isomorphic to the direct orthogonal sum $\mathcal{H}_1 \oplus \cdots \oplus \mathcal{H}_1$ of $d_2 = \dim \mathcal{H}_2$ copies of the space $\mathcal{H}_1$.

For the operators X_j in the spaces $\mathcal{H}_j$ we define the tensor product by putting

$$(X_1 \otimes X_2)(\psi_1 \otimes \psi_2) = X_1\psi_1 \otimes X_2\psi_2,$$

and extending by linearity. Let a basis in $\mathcal{H}_2$ be fixed, so that $\mathcal{H}_1 \otimes \mathcal{H}_2$ is realized as $\mathcal{H}_1 \oplus \cdots \oplus \mathcal{H}_1$. In this case, $X_1 \otimes X_2$ is realized as the block matrix $\left[X_1 x_2^{jk}\right]$, where $\left[x_2^{jk}\right]$ is the matrix of the operator X_2. Now, a general operator X in $\mathcal{H}_1 \otimes \mathcal{H}_2$ is given by a block matrix $[X_{jk}]$ whose entries are operators in $\mathcal{H}_1$.

Let us recall that in Section 1.4 we denoted by $\mathfrak{B}_h(\mathcal{H})$ the real linear space of all Hermitian operators (i. e., sharp real observables) in $\mathcal{H}$. From the result of Exercise 1.5, in the case of complex Hilbert spaces $\mathcal{H}_1\mathcal{H}_2$ we have

$$\dim \mathfrak{B}_h(\mathcal{H}_1 \otimes \mathcal{H}_2) = \dim \mathfrak{B}_h(\mathcal{H}_1) \cdot \dim \mathfrak{B}_h(\mathcal{H}_2)$$

while in the case of real Hilbert spaces $\mathcal{H}_1, \mathcal{H}_2$ the dimensionalities of spaces of symmetric operators are related by the inequality $>$. [1]

Exercise 3.4 Prove the following statement. If S_j are the density operators in $\mathcal{H}_j$, then $S_1 \otimes S_2$ is a density operator in $\mathcal{H}_1 \otimes \mathcal{H}_2$.

Definition 3.5. Let T be an operator in $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$. The partial trace of T (with respect to $\mathcal{H}_2$) is defined as an operator $\mathrm{Tr}_{\mathcal{H}_2} T$ in $\mathcal{H}_1$, satisfying

$$\langle\phi| (\mathrm{Tr}_{\mathcal{H}_2} T) |\psi\rangle = \sum_k \left\langle \phi \otimes e_2^k \right| T \left| \psi \otimes e_2^k \right\rangle, \quad \phi, \psi \in \mathcal{H}_1.$$

If S_{12} is a density operator corresponding to a state of the composite system, then $S_1 = \mathrm{Tr}_{\mathcal{H}_2} S_{12}$ and the similarly defined S_2 are called partial states of the first or second subsystem, respectively.

Partial states are the noncommutative analog of marginal probability distributions in probability theory.

Exercise 3.6 Show that this definition does not depend on the choice of the orthonormal basis $\left\{e_2^k\right\}$. If $T = T_1 \otimes T_2$, then $\mathrm{Tr}_{\mathcal{H}_2}(T_1 \otimes T_2) = (\mathrm{Tr}\, T_2)\, T_1$.

Let $\mathcal{H}_1 \otimes \mathcal{H}_2$ be realized as $\mathcal{H}_1 \oplus \cdots \oplus \mathcal{H}_1$, so that $T = [T_{jk}]$. Then $\mathrm{Tr}_{\mathcal{H}_2} T = \sum_{j=1}^{d_2} T_{jj}$ and $\mathrm{Tr}_{\mathcal{H}_1} T = [\mathrm{Tr}\, T_{jk}]$.

10.3.3 3.1.2 Naimark's Dilation

The fundamental relation between orthogonal and nonorthogonal resolutions of the identity is established by the following theorem.

[1] It is possible to consider quaternionic Hilbert spaces, in which case the inequality changes to $<$; see [8].

Theorem 3.7 (Naimark). Let $\{M_x\}$ be a resolution of the identity in $\mathcal{H}$ with m outcomes, $\dim \mathcal{H} = d$. Then there exist a Hilbert space $\mathcal{K}$ of dimensionality $\dim \mathcal{K} \leq md$, an isometry $V : \mathcal{H} \to \mathcal{K}$, and an orthogonal resolution of the identity $\{E_x\}$ in $\mathcal{K}$ such that

$$M_x = V^* E_x V, \quad x \in \mathcal{X}. \tag{3.1}$$

An isometry is a linear map that preserves the norms and hence the inner products of vectors in the Hilbert spaces. For arbitrary $|\phi\rangle, |\psi\rangle \in \mathcal{H}, \langle\phi|V^*V|\psi\rangle = \langle\phi \mid \psi\rangle$ holds, i. e., $V^*V = I$. The isometric embedding V allows us to identify $\mathcal{H}$ with the subspace $V\mathcal{H}$ of the space $\mathcal{K}$ and consider $\mathcal{H} \subset \mathcal{K}$. Then M_x can be considered as a restriction of E_χ onto $\mathcal{H}$, i.e.,

$$E_x = \begin{bmatrix} M_x & \dots \\ \dots & \dots \end{bmatrix}.$$

Proof. The construction of $\mathcal{K}$ is done in two steps. First, we define vectors $|\Psi\rangle \in \mathcal{H}_m$ with

$$|\Psi\rangle = \begin{bmatrix} |\psi_1\rangle \\ \vdots \\ |\psi_m\rangle \end{bmatrix}, \quad |\psi_x\rangle \in \mathcal{H}. \tag{3.2}$$

In addition, we define the pre-inner product, i.e., a form satisfying all the properties of the inner product except nondegeneracy, by the relation

$$\langle \Psi' \mid \Psi \rangle = \sum_x \langle \psi'_x | \, M_x \, |\psi_x\rangle \, . \tag{3.3}$$

The properties follow from the definition of the resolution of the identity.
In order to ensure that the norm induced by this pre-inner product is nondegenerate, one considers the quotient space $\mathcal{K} = \mathcal{H}_m/\mathcal{H}_0$, where

$$\mathcal{H}_0 = \{\Psi_0 \in \mathcal{H}_m : \langle \Psi_0 \mid \Psi_0 \rangle = 0\},$$

i. e., we identify the vectors whose difference has zero norm. Now, the map $V : \mathcal{H} \to \mathcal{H}_m$, defined as

$$V|\psi\rangle = \begin{bmatrix} |\psi\rangle \\ \vdots \\ |\psi\rangle \end{bmatrix}, \tag{3.4}$$

is an isometry because

$$\langle\psi|V^*V|\psi\rangle = \sum_{x=1}^{m} \langle\psi|M_x|\psi\rangle = \langle\psi \mid \psi\rangle. \tag{3.5}$$

For the orthogonal resolution of the identity $\{E_x\}$ in $\mathcal{K}$, we introduce $E_x|\Psi\rangle = [0, \dots, |\psi_x\rangle, \dots, 0]^\top$, where the only nonzero component is on the x th place. Hence,

$$\langle V\phi|E_x|V\psi\rangle = \langle\phi|M_x|\psi\rangle, \quad \phi, \psi \in \mathcal{H},$$

which concludes the proof. □

We now consider an important corollary of Naimark's dilation theorem, which provides us with a statistical interpretation of an arbitrary resolution of the identity and establishes that the generalized definition of a quantum observable is just an extension of the standard one.

Corollary 3.8. Let $\{M_x\}$ be an observable in $\mathcal{H}$. Then there exist a Hilbert space $\mathcal{H}_0$, a unit vector $\psi_0 \in \mathcal{H}_0$, and a sharp observable $\{E_x\}$ in $\mathcal{H} \otimes \mathcal{H}_0$, such that

$$M_x = \mathrm{Tr}_{\mathcal{H}_0} \left(I \otimes |\psi_0\rangle \langle\psi_0| \right) E_x. \tag{3.6}$$

Proof. According to Naimark's theorem, $M_x = V^* E_x V$, where $V : \mathcal{H} \to \mathcal{K}$ is an isometric embedding. Let us identify $\mathcal{H}$ with the subspace $V\mathcal{H} \subseteq \mathcal{K}$. By extending, if necessary, the space $\mathcal{K}$, we can take $\dim \mathcal{K} = \dim \mathcal{H} \cdot d_0$, and hence

$$\mathcal{K} \simeq \mathcal{H} \oplus \cdots \oplus \mathcal{H} \simeq \mathcal{H} \otimes \mathcal{H}_0,$$

where $\mathcal{H}_0 = \mathbb{C}^{d_0}$ is the coordinate complex Hilbert space of dimensionality d_0, and $\mathcal{H}$ is identified with the first term in the direct sum, or with the subspace $\mathcal{H} \otimes |\psi_0\rangle$, where $|\psi_0\rangle = [1, 0, \ldots, 0]^\top$. Then

$$\left(I \otimes |\psi_0\rangle \langle\psi_0| \right) E_x = \begin{bmatrix} M_x & \cdots \\ 0 & 0 \end{bmatrix},$$

so that (3.6) indeed holds. □

Thus, every observable can be realized as a sharp observable in the composite system by introducing an auxiliary system in a fixed state $S_0 = |\psi_0\rangle \langle\psi_0|$. Such a way of realization can be called quantum randomization.

In classical statistics, randomization, i. e., the introduction of a "roulette" can be a useful trick, but it can never increase the information about the state of the observed system. From the result of Section 2.4.2 it follows that in quantum statistics this is no longer true. Paradoxically, quantum randomization allows us to extract more information about the state of the observed system than is contained in the sharp observables when we are not using an auxiliary system.

10.3.4 3.1.3 Schmidt Decomposition and Purification

Consider a state S_{12} in the Hilbert space of the composite system $\mathcal{H}_1 \otimes \mathcal{H}_2$.

Definition 3.9. A pure state S_{12} is called entangled if it cannot be represented as a product state $S_1 \otimes S_2$.

Thus, any unit vector $\psi_{12} \in \mathcal{H}_1 \otimes \mathcal{H}_2$ that is a nontrivial superposition of product vectors generates a pure entangled state. An important example is the maximally entangled state, generated by the vector

$$|\psi_{12}\rangle = \frac{1}{\sqrt{d}} \sum_{j=1}^{d} \left| e_j^1 \right\rangle \otimes \left| e_j^2 \right\rangle \tag{3.7}$$

in the space $\mathcal{H}_1 \otimes \mathcal{H}_2$, where $d = \dim \mathcal{H}_1 = \dim \mathcal{H}_2$ and $\left\{ e_j^{1,2} \right\}$ are orthonormal bases in $\mathcal{H}_{1,2}$. The meaning of this name will be clarified in Section 7.5. Meanwhile, note that the partial states of the maximally entangled state are the chaotic states in $\mathcal{H}_1$ and $\mathcal{H}_2$:

$$\mathrm{Tr}_{\mathcal{H}_2} |\psi_{12}\rangle \langle\psi_{12}| = \frac{I_1}{d}$$

and similarly for $\mathcal{H}_2$.

We shall often make use of the following result.

Theorem 3.10 (Schmidt Decomposition). Let $S_{12} = |\psi\rangle\langle\psi|$ be a pure state in the Hilbert space $\mathcal{H}_1 \otimes \mathcal{H}_2$ and $S_1 = \mathrm{Tr}_{\mathcal{H}_2} S_{12}, S_2 = \mathrm{Tr}_{\mathcal{H}_1} S_{12}$ be its partial states. Then the density operators S_1, S_2 have the same nonzero eigenvalues λ_j. Furthermore,

$$|\psi\rangle = \sum_j \sqrt{\lambda_j} \left| e_j^1 \right\rangle \otimes \left| e_j^2 \right\rangle, \tag{3.8}$$

where $\left\{e_j^{1,2}\right\}$ are orthonormal eigenvectors of S_1, resp. of S_2.

Proof. Taking the orthonormal basis $\left\{e_j^1\right\}$ of eigenvectors in $\mathcal{H}_1$, we can write $|\psi\rangle$ as

$$|\psi\rangle = \sum_j \left|e_j^1\right\rangle \otimes \left|h_j^2\right\rangle, \tag{3.9}$$

with some vectors $\left|h_j^2\right\rangle \in \mathcal{H}_2$. Computation of the partial trace gives

$$\sum_{j,k} \left\langle h_j^2 \mid h_k^2\right\rangle \left|e_k^1\right\rangle \left\langle e_j^1\right| = \sum_j \lambda_j \left|e_j^1\right\rangle \left\langle e_j^1\right| \equiv S_1, \tag{3.10}$$

and therefore $\left\langle h_j^2 \mid h_k^2\right\rangle = \lambda_j \delta_{jk}$ (Kronecker's delta). Thus, we can put $\left|e_j^2\right\rangle = \frac{1}{\sqrt{\lambda_j}} \left|h_j^2\right\rangle$ for $\lambda_j > 0$ and complete this orthonormal system to a basis in $\mathcal{H}_2$, consisting of eigenvectors of the operator S_2. □

Conversely, an arbitrary mixed state of a quantum system can be "purified," i. e., extended to a pure state of a larger system.

Theorem 3.11 (Purification). Let S_1 be a state in $\mathcal{H}_1$. Then there exist a reference Hilbert space $\mathcal{H}_2$ of the same dimensionality as $\mathcal{H}_1$ and a pure state $|\psi\rangle\langle\psi|$ in $\mathcal{H}_1 \otimes \mathcal{H}_2$ such that $S_1 = \mathrm{Tr}_{\mathcal{H}_2} |\psi\rangle\langle\psi|$.

For any other pure state $|\psi'\rangle \langle\psi'|$ in $\mathcal{H}_1 \otimes \mathcal{H}_2$ that has this property, there is a unitary operator U_2 in $\mathcal{H}_2$ such that $|\psi'\rangle = (I_1 \otimes U_2) |\psi\rangle$.

Proof. Diagonalize S_1 and take $|\psi\rangle$ as in (3.8), with an arbitrary basis $\left\{e_j^2\right\}$ in a Hilbert space $\mathcal{H}_2$ isomorphic to $\mathcal{H}_1$. Any other $|\psi'\rangle$ has a decomposition (3.8) with a different basis in $\mathcal{H}_2$, and any two bases in the same space are related by a unitary transformation. □

Corollary 3.12. Let S_{12} be a state in $\mathcal{H}_1 \otimes \mathcal{H}_2$ such that the partial state S_1 is pure. In this case, $S_{12} = S_1 \otimes S_2$.

Proof. For a pure state S_{12} the statement obviously follows from Theorem 3.10. For an arbitrary state S_{12}, we can apply the same argument to its purification. □

From Theorem 3.10, it also follows that the purification is essentially unique. Any two purifications with reference spaces $\mathcal{H}_2, \mathcal{H}_2'$, such that $\dim \mathcal{H}_2 \leq \dim \mathcal{H}_2'$, are related by an isometric embedding of $\mathcal{H}_2$ into $\mathcal{H}_2'$.

Remarkably, there is one universal Hilbert space that contains purifications of all states in $\mathcal{H}$. Consider the Hilbert space $L^2(\mathcal{H})$ of all operators $X, Y, \ldots$ in $\mathcal{H}$, equipped with the inner product

$$(X, Y) = \mathrm{Tr}\, X^* Y.$$

Then the bilinear correspondence

$$|\psi\rangle\langle\varphi| \leftrightarrow |\psi\rangle \otimes \langle\varphi|, \tag{3.11}$$

where $\langle\varphi| \in \mathcal{H}^*$ (the dual space of linear functions on $\mathcal{H}$) is uniquely extended to the isometry between the Hilbert spaces $L^2(\mathcal{H})$ and $\mathcal{H} \otimes \mathcal{H}^*$. Denoting by L_A (resp. R_B) the operation of left multiplication by A (resp. of right multiplication by B), we have for $X = |\psi\rangle\langle\varphi|$

$$L_A R_B X \equiv AXB \leftrightarrow |A\psi\rangle \otimes \langle B^*\varphi| .$$

For an arbitrary density operator S in $\mathcal{H}$ consider the unit vector $\sqrt{S}W \in L^2(\mathcal{H})$, where W is arbitrary unitary in $\mathcal{H}$. Then

$$\left(\sqrt{S}W, L_A R_B \sqrt{S}W\right) = \mathrm{Tr}\, \sqrt{S} A \sqrt{S} W B W^*,$$

whence, letting $B = I$,

$$\operatorname{Tr} SA = \left(\sqrt{S}W, \left(A \otimes I_{\mathcal{H}^*}\right)\sqrt{S}W\right).$$

Therefore $\sqrt{S}W$ is a purification of S in $L^2(\mathcal{H})$ identified with $\mathcal{H}\otimes\mathcal{H}^*$ via the correspondence (3.11). Moreover, all purifications of S are obtained in this way.

Note that purification is a mathematical construct that does not correspond to any physical operation. Indeed, it would imply cloning the quantum state S_1.

Definition 3.13. A general mixed state $S_{12} \in \mathfrak{S}\left(\mathcal{H}_1 \otimes \mathcal{H}_2\right)$ is called separable (unentangled) if it belongs to the convex hull of the set of all product states, i. e., if it has the form of the convex combination

$$S_{12} = \sum_x \pi_x S_1^x \otimes S_2^x,$$

where $S_j^x \in \mathfrak{S}\left(\mathcal{H}_j\right), j = 1, 2$, and $\{\pi_x\}$ is a finite probability distribution. The states that are not separable are called entangled.

A simple necessary condition for separability is that the state S_{12} has a positive partial transpose (PPT). An arbitrary operator in $\mathcal{H}_1 \otimes \mathcal{H}_2$ can be represented as $A_{12} = \sum_j A_1^j \otimes A_2^j$. Its partial transpose with respect to the second system is correctly defined as

$$A_{12}^{\tau_2} = \sum_j A_1^j \otimes \left[A_2^j\right]^{\tau_2},$$

where ${}^{\top}{}_2$ is a transposition in the second system. In general, this condition is not sufficient, so there exist PPT entangled states.

10.3.5 3.2 Quantum Entanglement vs. "Local Realism"

10.3.6 3.2.1 Paradox of Einstein-Podolski-Rosen and Bell's Inequalities

Entanglement, along with complementarity, constitutes the principal structural difference between the classical and the quantum description of systems.

The pure state of a classical system is described by a point in the phase space (practically, this is a complete set of parameter values describing "inner properties" of the system). If the classical system under consideration consists of several subsystems, an arbitrary pure state is necessarily a product of the pure states of the subsystems. By fixing the values of the parameters of the system we ipso facto fix the values of the parameters of all its subsystems. In this case, there is no need to involve a statistical treatment.

For quantum systems the situation is different. As Corollary 3.12 shows, for any pure entangled state S_{12} of a composite system, the partial states $S_{1,2}$ are necessarily mixed, i. e., they require a statistical description.

Such behavior is quite unusual from a classical point of view and, as will be shown in this section, is entirely incompatible with the classical mode of description (which is often called "realism").

The key example of the unusual behavior of composite quantum systems was provided by Einstein, Podolski, and Rosen (EPR) in 1935. In the 1950s Bohm presented it in a clearer form, using spin degrees of freedom instead of spatial ones, and in the 1960s it was substantially clarified by J. S. Bell, who suggested a fundamental inequality, which holds for classical composite systems satisfying a natural requirement of "locality" (separability), but is violated in quantum systems and which, in principle, can be verified experimentally.

Consider two particles with spin 1/2, each of which is described by the Hilbert space $\mathcal{H}$ with $\dim \mathcal{H} = 2$. Initially, the particles interact, resulting in the common spin state described by the vector

$$|\psi\rangle = \frac{1}{\sqrt{2}}[|\uparrow\rangle \otimes |\downarrow\rangle - |\downarrow\rangle \otimes |\uparrow\rangle],$$

where the basis vectors

$$|\uparrow\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |\downarrow\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

describe the states of each particle, with the spin along the positive (resp. negative) direction of the z axis. Usually, one writes briefly

$$|\psi\rangle = \frac{1}{\sqrt{2}}[|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle]. \tag{3.12}$$

Every component denotes the state with the spins in opposite directions, while $|\psi\rangle$ is their superposition, which cannot be represented as a tensor product of state vectors related to different particles. This state is called "singlet" and is a canonical example of an entangled state of two quantum systems.

Suppose that the particles travel apart along the y axis at a macroscopic distance, while preserving the entangled state of their spins. Consider an experiment in which simultaneous measurements of spin observables $\sigma(\vec{a})$ for one particle and $\sigma(\vec{b})$ for another particle are made simultaneously in remote laboratories A and B. Operators $X = \sigma(\vec{a}) \otimes I, Y = I \otimes \sigma(\vec{b})$ commute. Hence, the corresponding observables are compatible and their covariance is given by expression (2.23).

Exercise 3.14 By using expressions for the matrix elements

$$\langle\uparrow |\sigma(\vec{a})| \uparrow\rangle = a_z, \quad \langle\downarrow |\sigma(\vec{a})| \uparrow\rangle = a_x + ia_y, \quad \langle\downarrow |\sigma(\vec{a})| \downarrow\rangle = -a_z, \tag{3.13}$$

which follows from (2.14), show that in the singlet state the mean value and the variance of the spin observable in any direction are given by

$$\mathrm{E}(\sigma(\vec{a}) \otimes I) = 0, \quad \mathrm{D}(\sigma(\vec{a}) \otimes I) = 1,$$

while the covariance between the spins is given by the formula

$$\langle\psi|\sigma(\vec{a}) \otimes \sigma(\vec{b})|\psi\rangle = -\vec{a} \cdot \vec{b} \tag{3.14}$$

It follows that for $\vec{b} = \vec{a}$, the correlation coefficient is equal to -1 . Hence, there is a deterministic relation $a = -b$ between the outcomes a, b of the measurements. The formulas (3.13) and the fact that $\sigma(\vec{a})^2 = I$ imply

$$\langle\psi|[\sigma(\vec{a}) \otimes I + I \otimes \sigma(\vec{a})]^2|\psi\rangle = 0,$$

whence

$$[\sigma(\vec{a}) \otimes I + I \otimes \sigma(\vec{a})]|\psi\rangle = 0. \tag{3.15}$$

If the spins were classical random variables, this would mean that measuring the spin of the first particle in some arbitrarily chosen direction $\vec{a}$ would "instantaneously" bring the spin of the second particle into the opposite direction.

Exercise 3.15 Prove the following statement. For any direction $\vec{a}$,

$$|\psi\rangle = \frac{\epsilon}{\sqrt{2}}[|\vec{a}\rangle \otimes |-\vec{a}\rangle - |-\vec{a}\rangle \otimes |\vec{a}\rangle], \tag{3.16}$$

where ϵ is inessential factor of modulus one.

Thus, one has to choose between the following alternatives.

(1) In quantum mechanics, like in the classical case, the (pure) state describes "real" inner properties of a system. However, in this case, in order to explain how the second particle "gets to know" the chosen spin direction of the first particle, one has to accept instantaneous action at a distance, contradicting the physical "locality principle."

(2) The state vector is only an expression of the information about the preparation procedure. In that case there is no contradiction with locality, but one has to abandon the complete mechanistic description of a system state as the totality of its "inner properties."

However, a thorough consideration of the EPR experiment led Bell to a much deeper conclusion: if one tries to describe the quantum correlations classically and simultaneously attempts to satisfy the principle of locality, one cannot achieve the level of correlation between systems A and B predicted by quantum theory. "Local realism" and the correlations (3.14) predicted by quantum theory are incompatible.

This is established with the help of the Clauser-Horne-Shimony-Holt inequality, which is a convenient modification of Bell's original inequality.

Let $X_j, Y_k (j, k = 1, 2)$ be arbitrary random variables on one probability space Ω, such that $|X_j| \leq 1, |Y_k| \leq 1$. In this case, for any probability distribution P on Ω, the correlations of these random variables satisfy

$$|\mathrm{E}X_1Y_1 + \mathrm{E}X_1Y_2 + \mathrm{E}X_2Y_1 - \mathrm{E}X_2Y_2| \leq 2, \tag{3.17}$$

where E is the expectation corresponding to the distribution P.

The proof is obtained by averaging the elementary inequality over the distribution P,

$$-2 \leq X_1Y_1 + X_1Y_2 + X_2Y_1 - X_2Y_2 \leq 2,$$

which in turn follows from

$$|X_1Y_1 + X_1Y_2 + X_2Y_1 - X_2Y_2| \leq |Y_1 + Y_2| + |Y_1 - Y_2| \leq 2\max\{|Y_1|, |Y_2|\}.$$

Let us go back to the system of two qubits and consider the four different experiments in which the spin observables $\sigma(\vec{a}_j)\,(j = 1, 2)$ are measured over the first qubit, and $\sigma\left(\vec{b}_k\right)\,(k = 1, 2)$ over the second, while the directions $\vec{a}_j, \vec{b}_k (j, k = 1, 2)$ will be chosen later. In all four experiments the system is prepared in the singlet state (3.12). Assume that there exists a "local" classical description reproducing the statistical results of all these four experiments. This means that there is a probability space Ω, a probability distribution on Ω describing the statistical ensemble in the singlet state, and the random variables $X_j, Y_k, j, k = 1, 2$, taking values ± 1, which classically describe the spin observables $\sigma(\vec{a}_j), \sigma\left(\vec{b}_k\right), j, k = 1, 2$. In this case, the quantum correlations (3.14) have to satisfy inequality (3.17). The requirement of "locality" (or, better to say, separability of the two subsystems) is expressed by the fact that the random variables that describe the spin of the first particle (X_1 in the first two correlations and X_2 in the other two cases) are assumed to be the same for the experiments with different directions of spin of the second particle (Y_1 or Y_2), and vice vers a for Y_1 and Y_2, which allows us to apply inequality (3.17). Omitting this requirement would mean that the given classical description allows the choice of a measurement on the second particle to influence the inner characteristics of the first particle (the term "locality" is used in connection with the fact that the two particles are supposed to be spatially separated).

Now, choose the spin directions as shown in Figure 3.1. Substituting the correlations given by formula (3.14) into the left-hand side of (3.17) gives the value $2\sqrt{2}$, which breaks the inequality. Thus, assuming the possibility of a classical "local" description is incorrect. The requirement of separability appears to be so natural that it is not so easy to perceive. However, it is this condition which forbids instantaneous influence of measurements in one subsystem on another. If this condition is abandoned, the four correlations in question can be arbitrary numbers in $[-1, 1]$, and the left-hand side of inequality (3.17) can be bounded only by the value 4, which does not contradict quantum theory.

Therefore, one has a dilemma: either quantum theory gives incorrect predictions for the correlations, or the composite system of two qubits has no classical local (separable) description. Several experiments were made, starting with Aspect's experiments in 1981-1982, the results of which essentially confirm the predictions of quantum theory.

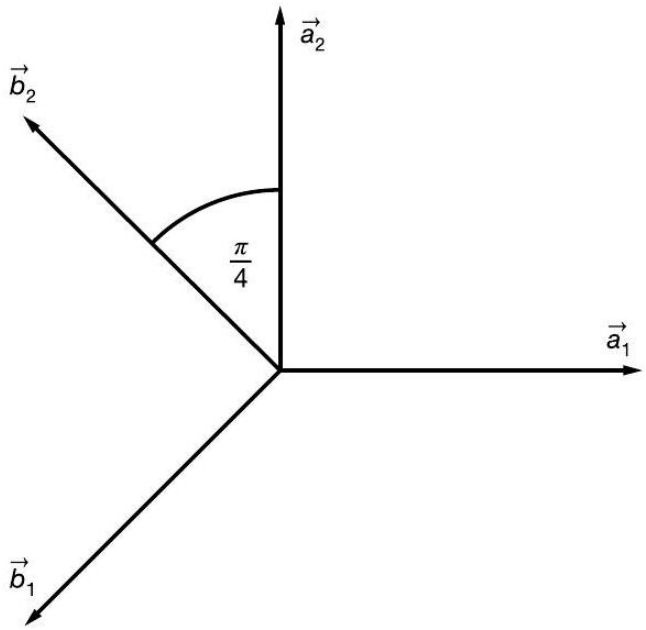


Figure 3.1: Choice of the vectors $\vec{a}_{j}$ and $\vec{b}_k$.

10.3.7 3.2.2 Mermin-Peres Game

The fact that quantum entanglement between parts of a composite system is profoundly different from any kind of classical connection, and in some situations can provide a real advantage over the latter, is demonstrated in a most spectacular, nearly grotesque, way by "quantum pseudotelepathy games." We will describe one of these, the Mermin-Peres magic square game, which uses nothing but the basic postulates of quantum theory.

In the following game, a team of two players, A (Alice) and B (Bob), tries to win against a croupier C. Imagine a 3×3-matrix in which C chooses a row and a column and announces the number i of the row to A and the number j of the column to B. A and B are allowed to agree on any joint strategy prior to this announcement, but cannot communicate after it has been made. Thus, A does not know the number of the column for B and viceversa. Then A must put $+1$ or -1 in each cell of her row, subject to the constraint that the product of elements must be 1 . Similarly B must put $+1$ or -1 in each cell of his row subject to the constraint that the product of elements must be -1 . They win if their choices coincide on the intersection ij of the row and the column chosen by the croupier.

In order to win, players A and B could agree a priori on some fixed 3×3-matrix with elements ± 1. However, it is easy to see that there is no matrix that satisfies the imposed constraints: from the constraint on A (resp. B) the product of all matrix elements should be equal to 1 (resp. -1). They could adopt a randomized strategy, but the probability of success will always be strictly less than 1 .

However, assuming that they are capable of producing and sharing an entangled quantum state before C makes his announcement and make pre-agreed quantum measurements on their respective parts of this state after the announcement, they will al-
ways be able to win! Of course, both the entangled state and the measurements are independent of the choices of C, as it should be. Hence, the rules of the game are perfectly respected and it is the use of advanced quantum information technology that produces a result that is unachievable by solely classical means. From the point of view of a purely classical observer it looks like there is some immaterial connection between A and B, hence the name "pseudotelepathy."

For a pair of qubits A and B, let us introduce the Bell state

$$|\Psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle),$$

which is similar to the singlet state (3.12).
The prepared entangled state is the tensor product of two Bell states of two pairs of qubits A_1B_1 and A_2B_2, i. e.,

$$|\Psi\rangle = |\Psi\rangle_{A_1B_1} \otimes |\Psi\rangle_{A_2B_2}.$$

Before C makes his announcement, qubits A_1 and A_2 are distributed to player A, while qubits B_1 and B_2 are given to B. Players A and B also agree in advance that, as soon as they receive the numbers of the row i and the column j, respectively, they will perform the spin measurements on their pairs of qubits, according to the table

$$\begin{bmatrix} \sigma_0 \otimes \sigma_z & \sigma_z \otimes \sigma_0 & \sigma_z \otimes \sigma_z \\ \sigma_x \otimes \sigma_0 & \sigma_0 \otimes \sigma_x & \sigma_x \otimes \sigma_x \\ -\sigma_x \otimes \sigma_z & -\sigma_z \otimes \sigma_x & \sigma_y \otimes \sigma_y \end{bmatrix},$$

and write the outcome of the measurement in the corresponding cell. At this point, we should expand on the special properties of this array of operators.

Denoting by X_{ij} the operator on the intersection of the i th row and the j th column, one has
i. $X_{ij} = X_{ij}^*$ and $X_{ij}^2 = \sigma_0 \otimes \sigma_0 \equiv I$, so that all X_{ij} are (sharp) real observables with eigenvalues ± 1;
ii. in any row i, the operators $X_{ij}, j = 1, 2, 3$, commute. Hence, the observables are compatible. Moreover, $X_{i1}X_{i2}X_{i3} = I$. Hence for any value $i = 1, 2, 3$ given by C, player A can make a joint measurement of the observables $X_{ij}, j = 1, 2, 3$, obtaining the outcomes $+1$ or -1 , which obey the constraint for A. Next, A writes these outcomes in row i. A similar description applies to player B and any column j.
iii. miraculously, the numbers written on the intersection of the i th row and the j th column by A and B always coincide. This follows from the identity

$$\left(X_{ij}^A \otimes X_{ij}^B\right)|\Psi\rangle = |\Psi\rangle, \quad i, j = 1, 2, 3,$$

where X_{ij}^A (resp. X_{ij}^B) is the operator X_{ij} in system $A = A_1A_2$ (resp. $B = B_1B_2$). Indeed, this identity means that, if the whole system $A_1A_2B_1B_2$ is prepared in the state $|\Psi\rangle$, the product of the outcomes of the (compatible) measurements of A and B, in any cell ij, will be equal to 1 , i.e., the outcomes coincide.

Exercise 3.16 Prove the properties i, ii by using the multiplication table (2.17) for the Pauli matrices. Prove the property iii by using the identities

$$(\sigma_{x,z} \otimes \sigma_0) |\Psi\rangle_{AB} = (\sigma_0 \otimes \sigma_{x,z}) |\Psi\rangle_{AB}$$
$$(\sigma_y \otimes \sigma_0) |\Psi\rangle_{AB} = -(\sigma_0 \otimes \sigma_y) |\Psi\rangle_{AB}$$

similar to (2.17).

10.3.8 3.3 Quantum Systems as Information Carriers

10.3.9 3.3.1 Transmission of Classical Information

If the information carrier is a classical system with a finite number of states d, the maximal number of binary digits, or bits, which can be recorded or transmitted by such a carrier is equal to $\log_2 d$. If the transmission is without errors, one speaks of an ideal communication channel. In general, a noisy classical channel is described by the conditional probabilities $p(y \mid x)$ for receiving the signal y at the output, if the value at the input was x. For the ideal channel $p(y \mid x) = \delta_{xy}$. The opposite case is the channel for which the probabilities $p(y \mid x) = p(y)$ do not depend on the transmitted signal x and hence the information is not transmitted at all. More detailed account of classical channels will be given in Chapter 4.

Let us now consider how classical information can be transmitted with a quantum carrier described by a Hilbert space $\mathcal{H}$. The carrier's state S is prepared with macroscopic devices. By changing the parameters of a device, one changes the parameters of the state, thus having a possibility to "record" classical information into the quantum state. Let there be n different signals and let S_x be the quantum state corresponding to the signal $x = 1, \ldots, n$. The mapping $x \to S_x$ describes the net result of a physical process that generates the state S_x. A detailed description of such a process is beyond the scope of information theory, for which only the resulting states S_x are relevant.

To extract the classical information contained in the output state of a channel, one has to perform a measurement. If one measures the observable $M = \{M_y\}$, the conditional probability of obtaining a signal y at the output given the input signal x is equal to

$$p_M(y \mid x) = \operatorname{Tr} S_x M_y \tag{3.18}$$

Thus, for a fixed quantum measurement, we have the usual classical channel. Assume that one manages to prepare states and perform a measurement in such a way that $S_x = |e_x\rangle \langle e_x|$, $M_y = |e_y\rangle \langle e_y|$. Then $P_M(y \mid x) = \delta_{xy}$, i. e., one has an ideal classical channel, capable of transmitting $\log_2 d$ bits, where $d = \dim \mathcal{H}$. Later, in Chapter 5, we will establish that this quantity is the upper bound for the amount of classical information that can in principle be transmitted with the given quantum carrier. This implies the following important consequences:
(1) The fact that Hilbert space contains infinitely many different state vectors does not aid us in transmitting an unlimited amount of information. The more states are used for transmission, the closer they are to each other and hence they become less and less distinguishable.
(2) The dimensionality of the Hilbert space is a measure of the ultimate information resource of the corresponding quantum system.

10.3.10 3.3.2 Entanglement and Local Operations

In this section, we will need elementary knowledge about quantum evolutions. Later, in Chapter 6, we will provide a detailed discussion of this question from the viewpoint of the general theory. Meanwhile, it is sufficient to know that reversible evolutions of a quantum system are

described by unitary operators U. The vector of the initial pure state ψ is transformed into $U\psi$. Correspondingly, a density operator S is transformed into USU^*.

Consider now the following question. The nonlocal, from a classical viewpoint, nature of the EPR correlations suggests to attempt using them for instantaneous information transmission. Let us show that this is not possible within the quantum mechanical framework, so that the EPR correlations do not contradict locality. Consider two quantum systems A and B, in the corresponding spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, which are in an entangled state S_{AB}. In the case of practical interest, the systems are sufficiently spatially separated, although this is not reflected by the formulas. The system A (transmitter) uses the classical messages x, which should be transmitted to B (receiver), in order to perform certain unitary operations U_x in the space $\mathcal{H}_A$ (such operations are called local, i.e., acting nontrivially only in one of the two systems). This brings the state of the system AB into $S_x = (U_x \otimes I_B)\, S_{AB}\, (U_x \otimes I_B)^*$, and in this way the classical information is written into the quantum state of the composite system. After that, observer B makes a local measurement of an observable in $\mathcal{H}_B$, corresponding to the resolution of the identity $M = \{I_A \otimes M_y\}$ in the space of the composite system $\mathcal{H}_A \otimes \mathcal{H}_B$. The resulting conditional probability (3.18) is

$$p_M(y \mid x) = \operatorname{Tr} (U_x \otimes I_B)\, S_{AB}\, (U_x \otimes I_B)^*\, (I_A \otimes M_y) = \operatorname{Tr} S_B M_y,$$

where $S_B = \operatorname{Tr}_A S_{AB}$ is the partial state of the system B, which does not depend on x. This means that local operations of observer A do not in any way influence the state of B, and hence, no information is transmitted.

Consider now the different scenario where observer A makes a local measurement of observable M_x^A and sends the outcome to observer B, who takes this into account by selecting the subensemble where this outcome x has appeared. In this case, the posterior state $S_B(x)$ of party B will depend on the outcome of the measurement x. To find the posterior state, assume that B performs his local measurement M_y^B, and consider the joint probability distribution of the two measurements

$$p_{x,y} = \operatorname{Tr} S_{AB} \left(M_x^A \otimes M_y^B\right).$$

By introducing the conditional probabilities $p(y \mid x) = p_{x,y}/p_x$ (assuming $p_x > 0$), we have

$$\begin{aligned} p_x &= \operatorname{Tr} S_{AB} \left(M_x^A \otimes I_B\right) = \operatorname{Tr} S_A M_x^A, \\ p(y \mid x) &= \operatorname{Tr} S_B(x) M_x^B, \end{aligned}$$

where

$$S_B(x) = p_x^{-1} \operatorname{Tr}_{\mathcal{H}_A} S_{AB} \left(M_x^A \otimes I_B\right)$$

are the posterior states.

The change of the state of observer B from S_B to $S_B(x)$ means a reduction of the full statistical ensemble of B to the subensemble characterized by the value x of the outcome of the measurement of observer A. If this outcome is not taken into account (for example, A does not send it to B, hence B makes no selection), then the state of B is not changed, i.e.,

$$S_B = \sum_x p_x S_B(x).$$

Exercise 3.17 Let $S_{AB} = |\psi\rangle\langle\psi|$ be a pure entangled state,

$$|\psi\rangle = \sum_x \left|e_x^A\right\rangle \otimes \left|\psi_x^B\right\rangle,$$

where e_x^A is an orthonormal basis in $\mathcal{H}_A, \sum_x \left\|\psi_x^B\right\|^2 = 1$. Assume that A measures the observable $M_x^A = \left|e_x^A\right\rangle \left\langle e_x^A\right|$ and sends the measurement outcome x to party B. Prove that $p_x = \left\|\psi_x^B\right\|^2$ and the posterior states of B are

$$S_B(x) = p_x^{-1} \left|\psi_x^B\right\rangle \left\langle \psi_x^B\right| . \tag{3.19}$$

Coming back to the EPR experiment, we obtain from the relation (3.16) that, in the case where A measures the spin observable $\sigma(\vec{a})$ and sends the outcome ± 1 to observer B, the posterior state of B (i. e., the state of the corresponding statistical subensemble) is $|\mp\vec{a}\rangle\langle\mp\vec{a}|$. On the other hand, if there is no communication between A and B, the state of B remains chaotic, independently of the measurement of A. Thus, quantum theory does not contradict the principle of locality.

10.3.11 3.3.3 Superdense Coding

Although EPR correlations cannot aid in transmitting information from A to B, it appears that using these correlations as additional resource allows one to double the
amount of classical information transmitted from A to B if they are connected by an ideal quantum channel enabling perfect transmission of a quantum state from A to B. Hence, EPR correlations appear as a "catalyst" for classical information transmission and from this viewpoint can be considered a unit of a specific information resource (sometime called an ebit).

Consider the two systems A and B, each of which is a qubit, connected by an ideal quantum channel. The maximum amount of classical information that can be transmitted from A to B is equal to 1 bit and is obtained by encoding this bit into two orthogonal vectors, say,

$$0 \to |0\rangle, 1 \to |1\rangle,$$

where $|0\rangle, |1\rangle$ is the canonical basis for one qubit.
The protocol of "superdense coding," which allows us to double the amount of transmitted classical information, is based on the following simple mathematical fact. All vectors of the Bell basis

$$|e_+\rangle = |00\rangle + |11\rangle, \quad |e_-\rangle = |00\rangle - |11\rangle, \quad |h_+\rangle = |10\rangle + |01\rangle, \quad |h_-\rangle = |10\rangle - |01\rangle$$

in the system of two qubits AB (we will systematically omit the normalizing factor $1/\sqrt{2}$) can be obtained from one of these vectors by the action of "local" unitary operators, i. e., operators acting nontrivially only on qubit A. Namely,

$$|e_-\rangle = (\sigma_z \otimes I) |e_+\rangle , \quad |h_+\rangle = (\sigma_x \otimes I) |e_+\rangle , \quad |h_-\rangle = -i (\sigma_y \otimes I) |e_+\rangle .$$

Thus, if AB is initially in the state $|e_+\rangle$, A can encode 2 bits of classical information into 4 states of the Bell basis by mere local operations $\sigma_y, y = 0, x, y, z$, and then (physically) send its qubit to B via the ideal quantum channel. Then, making the measurement in the Bell basis, B receives 2 bits of classical information.

10.3.12 3.3.4 Quantum Teleportation

So far, we considered transmission of classical information. This information can be "written" into a quantum state and transmitted through a physical channel. However, the quantum state itself is an information resource, since it carries statistical uncertainty. The information carried by an unknown quantum state is qualitatively different from the classical one and

deserves the special name quantum information. The most apparent distinction of quantum information is impossibility of copying (no cloning). While classical information can be reproduced in an arbitrary number of copies, there is no room for a physical device that could perform the same task for quantum information. Indeed, the cloning transformation

$$|\psi\rangle \to \underbrace{|\psi\rangle \otimes \cdots \otimes |\psi\rangle}_{n}$$

is nonlinear, and hence cannot be implemented by a unitary operator. Of course, any fixed state (or even a collection of orthogonal states) may be copied by a specific device, but there is no universal device which would do this for an arbitrary state.

Let us briefly discuss the question of how a quantum state can be transmitted. A straightforward way is to just send the quantum system itself. Much more interesting and nontrivial is teleportation of the state, where the system itself is not transmitted, but instead a certain classical message is sent. An essential additional resource are the EPR correlations between the input and the output, which again play the role of "catalyst." Note that teleportation of a quantum state cannot be accomplished by merely sending classical information without using the entanglement. Since the classical information can be copied, this would mean the possibility of cloning quantum information.

Let there be two quantum systems A and B, describing input and output of the communication channel, respectively. In the simplest and basic version, the systems A and B are just qubits.
i. Before the transmission, the system AB is prepared in the state $|00\rangle + |11\rangle$ (recall that we omit the normalizing factor $1/\sqrt{2}$).
ii. The third party C provides A with an arbitrary pure state

$$|\psi\rangle = a|0\rangle + b|1\rangle,$$

which should be transmitted to B. Now, the combination of the three systems CAB is in the state

$$(a|0\rangle + b|1\rangle) \otimes (|00\rangle + |11\rangle).$$

iii. Then observer A performs a certain reversible local transformation of the state of CA.
iv. Observer A performs a measurement in CA with 4 outcomes (comprising 2 bits of classical information) and transmits the outcome of its measurement to B by using the ideal classical communication channel. The transformation and the measurement will be described below.
v. Depending on the outcome received, observer B performs a certain transformation of its state, obtaining the required state vector $|\psi\rangle$.

The necessary transformations are examples of quantum "gates," used in quantum computations. In step iii the state of CA is transformed by the operation CNOT (controlled "not"), i. e.,

$$|00\rangle \to |00\rangle, \quad |01\rangle \to |01\rangle, \quad |10\rangle \to |11\rangle, \quad |11\rangle \to |10\rangle,$$

when the state of the first qubit is unchanged, whilst the state of the second qubit is changed to its opposite if and only if the state of the first qubit is $|1\rangle$. As this transformation turns one basis into another basis, it is a unitary operator in the four-dimensional
space of CA. Next, the qubit C is transformed by the Hadamard gate H, implemented by the unitary matrix

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

Then the basis is rotated by the angle $\pi/4$, i. e.,

$$|0\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |1\rangle \to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

The initial state of the total system CAB is

$$a|000\rangle + b|100\rangle + a|011\rangle + b|111\rangle.$$

The action of CNOT on CA results in

$$a|000\rangle + b|110\rangle + a|011\rangle + b|101\rangle.$$

Then the Hadamard gate H acts on C, and we obtain

$$a(|000\rangle + |100\rangle) + b(|010\rangle - |110\rangle) + a(|011\rangle + |111\rangle) + b(|001\rangle - |101\rangle).$$

Singling out the state of the subsystem CA we have

$$|00\rangle(a|0\rangle + b|1\rangle) + |01\rangle(a|1\rangle + b|0\rangle) + |10\rangle(a|0\rangle - b|1\rangle) + |11\rangle(a|1\rangle - b|0\rangle).$$

Now, in step iv, the measurement in the subsystem CA is performed, which projects onto one of four basis vectors $|00\rangle, |01\rangle, |10\rangle, |11\rangle$. According to formula (3.19), the posterior state of the system B, depending on the obtained measurement outcome, is described by one of the vectors

$$a|0\rangle + b|1\rangle, a|1\rangle + b|0\rangle, a|0\rangle - b|1\rangle, a|1\rangle - b|0\rangle.$$

The outcome of the measurement is sent to B through the ideal classical channel. In step v, depending on the outcome, B applies one of the unitary Pauli operators $\sigma_0 = I, \sigma_x, \sigma_z, \sigma_y$, in each case transforming the state of B into $a|0\rangle + b|1\rangle$. Thus, observer B is transformed to the state in which observer C was initially, while the state of C is irreversibly lost (otherwise cloning of the quantum information would be possible).

10.3.13 3.4 Notes and References

1. For more details about tensor products of Hilbert spaces, see Chapter II. 4 of the book [193], where one can also find solutions to the exercises in this section. For a general formulation of Naimark's dilation theorem, see [180], where it was proved for an arbitrary resolution of the identity (probability operator-valued measure, see Definition 11.29) in infinite-dimensional Hilbert space. The motivation was to obtain selfadjoint extensions of symmetric operators but it was later recognized that this was just the first discovery of the remarkable general phenomenon that the properties of various operator objects can be improved by extension to a wider underlying space. In quantum information theory this principle received the colorful name "the Church of Larger Hilbert Space." The purification of quantum states and the unitary dilation of irreversible quantum dynamics in Section 6.3 are two of its other manifestations.

An analog of the decomposition (3.8) in separable Hilbert space dates back to Schmidt's paper of 1907, which is devoted to integral equations. The "purification map" was introduced by Powers and Størmer [191] and studied by Woronowicz [259] in connection with the problem of the quasi-equivalence of states on a C^*-algebra. The trick of purifying mixed states, which is widely used in quantum information theory, also appeared in the paper of Lindblad [167].

The observation that the PPT condition is necessary for separability is due to Peres [188] and Horodeckis [136], while the latter has shown that this condition is also sufficient for separability of states in 2×2 - and 2×3-dimensional composite systems. In higher dimensions there exist PPT states that are not separable, but their entanglement (called bound entanglement) is "weak," since it does not allow for distillation, i. e., transformation to maximally entangled Bell states by using local operations and classical communication (LOCC) (P. Horodecki [137], Horodeckis [140]).

2. The term "entanglement" (German "Verschränktheit") was introduced by Schrödinger, who was the first to note the unusual properties of entangled states. The careful logical analysis of the EPR experiment is due to Bell [21], who in particular established an inequality related to (3.17) and applied it to analyze the EPR paradox. "Loophole-free" experimental tests of the CHSH inequality were reported recently by Zeilinger et al. [262], Shalm et al. [205], Hanson et al. [91]. In the discussion of the Mermin-Peres game, we followed Aravind [9], where one can find further references. Experimental demonstrations of the quantum gain were also reported; see Zu et al. [261].

3. The protocol of superdense coding was proposed by Bennett and Wiesner [30]. The protocol of quantum teleportation was proposed in the famous publication of Bennett, Brassard, Crépeau, Jozsa, Peres, and Wootters [22]. The possibility of teleportation of the polarization state of a photon was experimentally demonstrated by the group of Zeilinger in 1997. Since then, a number of further successful experiments were performed, both on photons and on atoms.

10.4 4 Classical Entropy and Information

10.4.1 4.1 Entropy of a Random Variable and Data Compression

Let X be a random variable with values in a finite set $\mathcal{X}$ and let $P = \{p_x, x \in \mathcal{X}\}$ be its probability distribution. The entropy $H(X) = H(P)$ is defined as

$$H(X) = \sum_{x \in \mathcal{X}} \eta\left(p_x\right), \tag{4.1}$$

where

$$\eta(t) = \begin{cases} -t \log t, & t > 0, \\ 0, & t = 0. \end{cases} \tag{4.2}$$

Here and in what follows $\log = \log_2$ denotes the binary logarithm. The entropy $H(X)$ is a measure of uncertainty, of variability, or of the information content in the random variable X, as we shall see below. Without loss of generality we will assume in what follows that $p_x > 0$ for all x.

Let d be the number of elements in the set $\mathcal{X}$. One has

$$0 \leq H(P) \leq \log d \tag{4.3}$$

with the minimum value attained on degenerate distributions $\{1, 0, \ldots, 0\}, \ldots, \{0, \ldots, 0, 1\}$ and the maximum value on the uniform distribution $\left\{\frac{1}{d}, \ldots, \frac{1}{d}\right\}$. The first inequality follows from the nonnegativity of the function $\eta(t)$ in the domain $[0, 1]$, and the second follows from the concavity of the function $t \to \log t$, i.e.,

$$H(P) = \sum_{x=1}^{d} p_x \log \frac{1}{p_x} \leq \log \sum_{x=1}^{d} p_x \frac{1}{p_x} = \log d.$$

Let us now explain the operational interpretation of the entropy $H(X)$ as a measure of the information content in the random variable X. Consider a "random source" which produces independent, identically distributed (i.i.d.) random variables with distribution P. A sequence $w = (x_1, \ldots, x_n)$ of n letters from the alphabet $\mathcal{X}$ is called a word of length n. The total number of such words is $|\mathcal{X}|^n = 2^{n \log |\mathcal{X}|}$. Hence it is possible to encode all these words using binary strings of length $n \log |\mathcal{X}|$, i. e., $n \log |\mathcal{X}|$ bits. [1] However, by using the fact that the probability distribution P of X is in general nonuniform, one can in general achieve a much better encoding. The possibility of the data compression is closely connected with the asymptotic equipartition property.

Theorem 4.1. If $X_1, \ldots, X_n$ are i. i. d. random variables with distribution P, then

$$-\frac{1}{n} \sum_{i=1}^{n} \log p_{X_i} \longrightarrow H(X) \quad \text{in probability.} \tag{4.4}$$

This means that for any $\delta, \epsilon > 0$ there exists an n_0, such that for all $n \geq n_0$ we have

$$\mathrm{P}\left\{ \left| -\frac{1}{n} \sum_{i=1}^{n} \log p_{X_i} - H(X) \right| < \delta \right\} > 1 - \epsilon. \tag{4.5}$$

This is a direct consequence of the law of large numbers applied to the i.i.d. random variables $-\log p_{X_i}, i = 1, \ldots, n$, taking into account that $\mathrm{E}\,(-\log p_{X_i}) = H(X)$.

Noting that the probability of the occurrence of a word $w = (x_1, \ldots, x_n)$ is

$$p_w = p_{x_1} \cdots p_{x_n} = 2^{-n\left(-\frac{1}{n}\sum_{i=1}^{n} \log p_{x_i}\right)}, \tag{4.6}$$

we can now use relation (4.5) to introduce a basic notion of the typical word.

Definition 4.2. A word w, having probability p_w, is called δ-typical if

$$2^{-n(H(X)+\delta)} < p_w < 2^{-n(H(X)-\delta)} \tag{4.7}$$

in other words, if it satisfies the event in formula (4.5).

The collection of all δ-typical words of length n will be denoted by $T^{n,\delta}$. By using (4.5), (4.7), it is straightforward to see that δ-typical words have the following properties (where δ, ϵ are fixed positive numbers).

Exercise 4.3 Prove the following statements:

i. There are at most $2^{n(H(X)+\delta)}$ typical words, i. e., $\left|T^{n,\delta}\right| \leq 2^{n(H(X)+\delta)}$.

ii. For sufficiently large n, the set of all nontypical words has a probability $\mathrm{P}\left(\overline{T^{n,\bar{\delta}}}\right) \leq \epsilon$.

iii. For sufficiently large n, there are at least $(1-\epsilon)2^{n(H(X)-\delta)}$ typical words.

Now, one can do efficient data compression by using all binary sequences of length $n(H(X)+\delta)$ to encode all δ-typical words and all nontypical words into one additional (idle) symbol. Then the error probability of such a coding scheme will be less than or equal to ϵ.

Conversely, any code that uses only binary sequences of length $n(H(X)-\delta)$ has an asymptotically nonvanishing error probability, which in fact can be made arbitrarily close to 1 for n large enough. Indeed, let C be the collection of words that are used for the encoding into $n(H(X)-\delta)$ binary strings, while all other words are encoded into
the idle symbol. In this case, the error probability is $1 - \mathrm{P}(C)$, where

[1] To avoid inessential complications, we shall systematically neglect the fact that this number is not necessarily an integer.

$$\mathrm{P}(C) = \mathrm{P}\left(C \cap T^{n,\delta/2}\right) + \mathrm{P}\left(C \cap \overline{T^{n,\delta/2}}\right) \tag{4.8}$$

$$\leq |C| 2^{-n(H(X)-\delta/2)} + \mathrm{P}\left(\overline{T^{n,\delta/2}}\right) \tag{4.9}$$

$$\leq 2^{-n\delta/2} + \epsilon, \tag{4.10}$$

which can be made arbitrarily small for n large enough.
Since we need asymptotically $N \sim 2^{nH(X)}$ codewords for efficient encoding, $H(X)$ can be interpreted as a measure of the information content of the source in bits per letter. It is also clear that if we start with a uniform distribution $p_x = \frac{1}{|\mathcal{X}|}$, then $H(X) = \log|\mathcal{X}|$ and no data compression is possible.

Exercise 4.4 Let $\mathcal{X}$ be a finite subset of $\mathbb{R}$ and let $X_1, \ldots, X_n, \ldots$ be i. i. d. random variables with values in $\mathcal{X}$. Assuming the conditions of Theorem 4.1, prove the following large deviations inequality:

$$\mathrm{P}\left\{\frac{1}{n}\sum_{i=1}^{n}(X_i - \mathrm{E}X) \geq \delta\right\} \leq \exp\left\{-n \sup_{s>0}[s\delta - \mu(s)]\right\}, \tag{4.11}$$

where

$$\mu(s) = \ln Ee^{s(X-EX)} = o(s) \quad \text{for } s \to 0$$

This implies the law of large numbers with exponential decay of tails, since $s\delta - \mu(s) > 0$ for small $s > 0$.

Hint: prove and apply the following version of the Markov inequality:

$$\mathrm{P}\{X \geq x\} = \mathrm{P}\left\{\mathrm{e}^{\mathrm{s}X} \geq \mathrm{e}^{\mathrm{s}X}\right\} \leq \exp(-sx)\mathrm{E}\mathrm{e}^{\mathrm{s}X}$$

for any $x \in \mathbb{R}$ and $s > 0$.

10.4.2 4.2 Conditional Entropy and the Shannon Information

Let X, Y be random variables on one probability space with joint probability distribution $\{p_{x,y}\}$. In this case, one can define their joint entropy $H(XY)$ similar to relation (4.1). The conditional entropy $H(Y \mid X)$ is defined as

$$\begin{aligned} H(Y \mid X) &= \sum_x p_x H(Y \mid X = x) \\ &= -\sum_x p_x \sum_y p(y \mid x) \log p(y \mid x) \\ &= -\sum_{x,y} p_{x,y} \log p_{x,y} + \sum_x p_x \log p_x \\ &= H(XY) - H(X) \end{aligned} \tag{4.12}$$

There is a useful general rule stating that any linear relation for (conditional) entropies continues to hold if, in every term, a condition is supplemented with one and the same extra condition. For example, (4.12) implies

$$H(XY \mid Z) = H(X \mid Z) + H(Y \mid XZ). \tag{4.13}$$

A noisy communication channel is described by the transition probability $p(y \mid x)$ from the input alphabet $\mathcal{X}$ to the output alphabet $\mathcal{Y}$, i.e., a collection of conditional probabilities that a letter $y \in \mathcal{Y}$ is received when a letter $x \in \mathcal{X}$ is sent. An input probability distribution $P = \{p_x\}$ is transformed by the channel to the output probability distribution $P' = \{p'_y\}$, where $p'_y = \sum_x p(y \mid x)p_x$. The Shannon information (about the random variable X contained in Y) is defined as

$$I(X;Y) = H(Y) - H(Y \mid X), \tag{4.14}$$

where the entropy $H(Y)$ can be interpreted as the information content of the output, while the conditional entropy $H(Y \mid X)$ is interpreted as its useless component that arises from the noise in the channel. Substituting (4.12) into this expression for the Shannon information, we see that it is symmetric in X and Y, and hence it can also be called the mutual information

$$I(X;Y) = H(X) + H(Y) - H(XY). \tag{4.15}$$

Furthermore, $I(X;Y) = H(X) - H(X \mid Y)$, where $H(X)$ can now be interpreted as the information content of the input, and $H(X \mid Y)$ is sometimes referred to as loss. An explicit expression for the Shannon information via the input distribution and the channel transition probabilities is given by

$$I(X;Y) = \sum_{xy} p_x p(y \mid x) \log \left(\frac{p(y \mid x)}{\sum_{x'} p\left(y \mid x'\right) p_{x'}} \right). \tag{4.16}$$

A very useful quantity from classical statistics is the relative entropy of two probability distributions $P = \{p_x\}, Q = \{q_x\}$ (the Kullback-Leibler-Sanov entropy):

$$H(P;Q) = \begin{cases} \sum_{x:p_x>0} p_x \log \frac{p_x}{q_x}, & \text{if } \{x : p_x > 0\} \subseteq \{x : q_x > 0\}, \\ +\infty, & \text{otherwise .} \end{cases}$$

By using the inequality $\ln t \leq t - 1$, we obtain

$$H(P;Q) \geq -\log \mathrm{e} \sum_{x:p_x>0} p_x \left(\frac{q_x}{p_x} - 1 \right) \geq 0, \tag{4.17}$$

with equality if and only if $P = Q$.
The quantity $H(P;Q)$ plays an important role as an "asymmetric distance" between the probability distributions. It has the following monotonicity property. Consider the channel $r(y \mid x)$ and two input probability distributions $P = \{p_x\}, Q = \{q_x\}$, which are transformed to the output distributions $P' = \left\{p'_y\right\}, Q' = \left\{q'_y\right\}$,

$$p'_y = \sum_x r(y \mid x)p_x, \quad q'_y = \sum_x r(y \mid x)q_x.$$

In this case,

$$H\left(P';Q'\right) \leq H(P;Q). \tag{4.18}$$

In fact,

$$
\begin{aligned}
H(P;Q) &= \sum_{xy} p_x r(y \mid x) \log \frac{r(y \mid x) p_x}{r(y \mid x) q_x} \\
&= \sum_{xy} p_{x,y} \left(\log \frac{p'_y}{q'_y} + \log \frac{p(x \mid y)}{q(x \mid y)} \right) \\
&= H\left(P';Q'\right) + \sum_y p'_y H(p(x \mid y); q(x \mid y)) \\
&\geq H\left(P';Q'\right)
\end{aligned}
$$

Exercise 4.5 Prove that $I(X;Y) = H\left(p_{x,y}; p_x \cdot p_y\right)$. Hence, due to (4.17), $I(X;Y) \geq 0$, while $I(X;Y) = 0$ if and only if X and Y are independent random variables, i. e., $p_{x,y} = p_x \cdot p_y$.

This also implies monotonicity of the conditional entropy,

$$
0 \leq H(Y \mid X) \leq H(Y),
$$

and subadditivity of the entropy,

$$
H(XY) \leq H(X) + H(Y). \tag{4.19}
$$

Exercise 4.6 Consider the concatenation of two channels $p(y \mid x)$ and $q(z \mid y)$, defined as $r(z \mid x) = \sum_y q(z \mid y) p(y \mid x)$. Let X be a random variable at the input of the channel $p(y \mid x)$ having the probability distribution $\{p(x)\}$, and denote by Y and Z the output of the channel $p(y \mid x)$ and $r(z \mid x)$, resp., so that $X \to Y \to Z$ is a Markov chain. In this case, the data-processing inequalities hold,

$$
I(X;Z) \leq \min\{I(X;Y), I(Y;Z)\}. \tag{4.20}
$$

Hint: $I(X;Z) \leq I(X;YZ) = I(X;Y)$ follows from $H(X \mid Z) \geq H(X \mid YZ) = H(X \mid Y)$ and analogously for the second quantity.

The Shannon information has the following expression, in terms of the relative entropy:

$$
I(X;Y) = \sum_x p_x H\left(P'_x; P'\right), \tag{4.21}
$$

where $P'_x = \{p(y \mid x)\}$ for fixed $x \in \mathcal{X}$, and $P' = \sum_x p_x P'_x$ is the distribution of Y.

10.4.3 4.3 The Shannon Capacity of the Classical Noisy Channel

Consider the classical channel $X \to Y$ determined by the transition probability $p(y \mid x)$. The most important characteristic of the channel is the Shannon capacity

$$
C_{\text{Shan}} = \max_X I(X;Y), \tag{4.22}
$$

where the maximum is taken over all possible distributions $P = \{p_x\}$ of the input X. It will later be identified as the operationally defined information transmission capacity of the channel.

As an example, let us consider the binary symmetric channel. Assume that $\mathcal{X}$ and $\mathcal{Y}$ consist of two letters 0,1 , which are transmitted with probability p and flipped with probability $1-p$. Introducing the binary entropy

$$
h_2(p) = -p \log p - (1-p) \log(1-p), \tag{4.23}
$$

the mutual information can be written as $I(X;Y) = H(Y) - H(Y \mid X) = H(Y) - h_2(p)$, and is thus bounded by the quantity

$$C_{\text{Shan}} = 1 - h_2(p), \tag{4.24}$$

which is achieved for the uniform input distribution: $p_0 = p_1 = \frac{1}{2}$.
In general, $I(X;Y)$ is a concave function of the input probability distribution $P = \{p_x\}$. Hence, the Kuhn-Tucker conditions from convex analysis (see, e. g., [47]) can be applied to characterize the optimal input distribution P that maximizes $I(X;Y)$.

Exercise 4.7 Show that the entropy $H(P)$ is a concave function of the probability distribution P. Hint: use concavity of the function $t \to \eta(t)$. Therefore, the output entropy $H(Y) = H(P')$ is also concave, while the conditional entropy $H(Y \mid X)$ is affine. Use formula (4.14) to conclude that $I(X;Y)$ is concave.

Exercise 4.8 (Kuhn-Tucker Conditions) Let $F(P)$ be a concave function of probability distribution P, continuously differentiable at the interior of the simplex of all probability distributions on $\mathcal{X}$, and having possibly infinite limits of the partial derivatives at its boundary. Prove the following statement: a necessary and sufficient condition for the point P^0 to be the maximizer for $F(P)$ is that there exists a λ such that

$$\frac{\partial F(P^0)}{\partial p_x} \begin{cases} = \lambda, & \text{if } p_x^0 > 0, \\ \leq \lambda, & \text{if } p_x^0 = 0. \end{cases}$$

In the case of Shannon information (4.21), we find

$$\frac{\partial I}{\partial p_x} = H(P'_x; P') - \log \mathrm{e},$$

which leads to the following "maximal distance" characterization of the optimal input distribution $P^0 = \{p_x^0\}$: there exists a μ such that

$$H\left(P'_x; \left(P^0\right)'\right) \begin{cases} = \mu, & \text{if } p_x^0 > 0, \\ \leq \mu, & \text{if } p_x^0 = 0, \end{cases} \tag{4.25}$$

in which case, necessarily $\mu = C_{\text{Shan}}$.
Assume that two channels $\{p_j(y_j \mid x_j)\}, j = 1, 2$, are given, and consider the composite parallel channel consisting of the independent use of these two channels, described by the transition probability $\{p_1(y_1 \mid x_1)\, p_2(y_2 \mid x_2)\}$.

Proposition 4.9. The Shannon capacity of the composite channel is

$$(C_{\text{Shan}})_{12} = (C_{\text{Shan}})_1 + (C_{\text{Shan}})_2 . \tag{4.26}$$

Thus the Shannon capacity is additive for the parallel channels.
Proof. Let P^j be the optimal input probability distributions for the j th channel. Then they satisfy the condition (4.25) with constants $\mu_j = (C_{\text{Shan}})_j$. Using the fact that in general

$$H\left(P^1 \times P^2; Q^1 \times Q^2\right) = H\left(P^1; Q^1\right) + H\left(P^2; Q^2\right),$$

we obtain that the probability distribution $P = P^1 \times P^2$ satisfies the condition (4.25) for the composite channel, with the constant $\mu = (C_{\text{Shan}})_1 + (C_{\text{Shan}})_2$. □

10.4.4 4.4 The Channel Coding Theorem

Given the channel $p(y \mid x)$, one can consider the composite memoryless channel

$$p\left(y^n \mid x^n\right) = p\left(y_1 \mid x_1\right) \cdots p\left(y_n \mid x_n\right), \tag{4.27}$$

which transmits words of length n, by using the initial channel n times, with each use being independent of the others,

$$x^n \left\{ \begin{array}{ccc} x_1 & \longrightarrow & y_1 \\ x_2 & \longrightarrow & y_2 \\ \vdots & & \vdots \\ x_n & \longrightarrow & y_n \end{array} \right\} y^n.$$

By X^n, Y^n, we denote the random variables at the input and the output of the composite channel.

Following (4.22), consider the quantity

$$C_n = \max_{X^n} I\left(X^n; Y^n\right)$$

for the composite channel. Inductively applying property (4.26), we find that the sequence $\{C_n\}$ is additive for memoryless channels, whence

$$C_n = nC_{\text{Shan}}\,. \tag{4.28}$$

To reduce the effect of noise, one uses encoding of the messages at the input and, correspondingly, decoding at the output. The whole process of information transmission is given by the following diagram:

$$i \xrightarrow{\text{encoding}} x^n \xrightarrow{\text{channel}} y^n \xrightarrow{\text{decoding}} j, \tag{4.29}$$

where i (resp. j) denotes transmitted (resp. received) messages. One can simply assume that $i, j \in \{1, \ldots, N\}$ are the indices of the messages, since only the quantity N of the transmitted messages is of importance.

The aim is to choose an encoding and decoding that maximizes the transmission rate $R = \frac{\log N}{n}$, equal to the number of bits per transmitted symbol, while keeping the error probability small. Let us proceed to the exact formulation.

Definition 4.10. A code (W, V) of size N for the classical memoryless channel consists of a codebook W, which is a collection of N codewords $w^{(1)}, \ldots, w^{(N)}$ of length n, and a decision rule that is a decomposition of $\mathcal{Y}^n$ into $N+1$ nonintersecting subsets $V = \left\{V^{(0)}, V^{(1)}, \ldots, V^{(N)}\right\}$. The subsets $V^{(1)}, \ldots, V^{(N)}$ can be interpreted as decision domains. Whenever $y^n \in V^{(j)}$ is received, we decide that the word $w^{(j)}$ was transmitted. If $y^n \in V^{(0)} = \overline{\bigcup_{j=1}^N V^{(j)}}$, no definite decision is made.

Thus, the maximal error probability of such a code is

$$P_e(W, V) = \max_{1 \le j \le N} \left(1 - p\left(V^{(j)} \mid w^{(j)}\right)\right), \tag{4.30}$$

where $p\left(V^{(j)} \mid w^{(j)}\right) = \mathrm{P}\left(Y^n \in V^{(j)} \mid X^n = w^{(j)}\right)$ are the probabilities of correct decisions. The mean error probability is equal to

$$\bar{P}_e(W, V) = \frac{1}{N} \sum_{j=1}^{N} \left(1 - p\left(V^{(j)} w^{(j)}\right)\right) \le P_e(W, V). \tag{4.31}$$

The following useful statement implies that criteria for information transmission based on the average error probability $\bar{P}_e(W,V)$ and on the maximal error probability $P_e(W,V)$ are asymptotically the same.

Lemma 4.11. For any code (W,V) of size $2N$ with average error probability $\bar{P}_e(W,V)$ there exists a subcode $(\tilde{W},\tilde{V})$ of size N which has a maximal error probability $P_e(\tilde{W},\tilde{V}) \le 2\bar{P}_e(W,V)$.

Proof. Put $\epsilon = \bar{P}_e(W,V)$ and assume that there are at least $N+1$ codewords with error probability $p\left(V^{(j)} \mid w^{(j)}\right) \ge 2\epsilon$, so that it would not be possible to construct the required N-code. In this case, the average error probability of the $2N$-code would be bounded from below, since

$$\bar{P}_e(W,V) > \frac{1}{2N} 2\epsilon(N+1) > \epsilon$$

which contradicts the assumption. □

Denote by $p_e(n,N)$ (resp. by $\bar{p}_e(n,N)$) the maximal (resp. average) error probability minimized over all codes of length n and size N. Then

$$\frac{1}{2} p_e(n,N) \le \bar{p}_e(n,2N) \le p_e(n,2N) \tag{4.32}$$

Definition 4.12. The number $R \ge 0$ is called the achievable transmission rate if

$$\lim_{n\to\infty} p_e\left(n, 2^{nR}\right) = 0$$

The supremum of all achievable rates is called the information capacity C of the channel $p(y \mid x)$.

Theorem 4.13 (Shannon's channel coding theorem). For a memoryless channel,

$$C = C_{\text{Shan}} .$$

Thus, the operationally (and asymptotically) defined transmission capacity is equal to the "one-letter" characteristic of the channel as defined by (4.22). The inequality $C \ge C_{\text{Shan}}$ will follow from the statement

$$\lim_{n\to\infty} p_e\left(n, 2^{nR}\right) = 0, \quad \text{if } R < C_{\text{Shan}} ,$$

which is called the direct statement of the coding theorem, while the weak converse amounts to

$$\liminf_{n\to\infty} p_e\left(n, 2^{nR}\right) > 0, \quad \text{if } R > C_{\text{Shan}} , \tag{4.33}$$

which implies $C \le C_{\text{Shan}}$. In fact, one can prove a stronger result, i.e.,

$$\lim_{n\to\infty} p_e\left(n, 2^{nR}\right) = 1, \quad \text{if } R > C_{\text{Shan}}$$

Proof. The weak converse. Due to inequality (4.32), it is sufficient to prove the analog of the statement (4.33) for the average error probability $\bar{p}_e(n,N)$.

Lemma 4.14 (Fano's Inequality). Let X, Y be two random variables and $\hat{X} = \hat{X}(Y)$ be an estimator of X with error probability $p_e = \mathrm{P}(\hat{X}(Y) \ne X)$. In this case,

$$H(X \mid Y) \le h_2(p_e) + p_e \log(|\mathcal{X}| - 1) \le 1 + p_e \log|\mathcal{X}|. \tag{4.34}$$

Proof. Let E denote an indicator of the estimation error,

$$E = \begin{cases} 0, & \text{if } \hat{X}(Y) = X, \\ 1, & \text{otherwise} . \end{cases} \tag{4.35}$$

Since E is a function of $(X, \hat{X})$ and thus is fixed for a given value of X, Y, we have $H(X \mid Y) = H(E, X \mid Y)$. But (4.13) implies

$$H(EX \mid Y) = H(E \mid Y) + H(X \mid EY) \tag{4.36}$$

Here $H(E \mid Y) \leq H(E) = h_2(p_e)$ and

$$H(X \mid EY) = (1 - p_e) H(X \mid E = 0, Y) + p_e H(X \mid E = 1, Y) \leq p_e \log(|\mathcal{X}| - 1),$$

where we have used the notion that $H(X \mid E = 0, Y) = 0$, since $E = 0$ means that, given Y, we know X exactly. The condition $E = 1$ is the same as $X \neq \hat{X}(Y)$, which leaves the possibility for $|\mathcal{X}| - 1$ values of X. Hence, the maximal possible value of the entropy is $\log(|\mathcal{X}| - 1)$. $\square$

Consider an arbitrary code (W, V) of size N, with codewords $w^{(1)}, \ldots, w^{(N)}$ of length n and a decomposition of $\mathcal{Y}^n$ into $N + 1$ decision domains

$$V^{(0)}, V^{(1)}, \ldots, V^{(N)} \subset \mathcal{Y}^n.$$

Denote by X^n a random variable taking the values $w^{(1)}, \ldots, w^{(N)}$ with equal probabilities $\frac{1}{N}$ and let $\hat{X}^n = \hat{X}(Y^n)$ be an estimate for X^n such that $\hat{X}^n = w^{(j)}$ if $Y^n \in V^{(j)}$. In this case,

$$\begin{aligned} C_n &\geq I(X^n; Y^n) = H(X^n) - H(X^n \mid Y^n) \\ &\geq \log N \left(1 - \mathrm{P}\left\{\hat{X}^n \neq X^n\right\}\right) - 1, \end{aligned} \tag{4.37}$$

by Fano's inequality, where $\mathrm{P}\left\{\hat{X}^n \neq X^n\right\} = \bar{P}_e(W, V)$. Substituting $N = 2^{nR}$ and dividing by nR leads to

$$\bar{P}_e(W, V) \geq 1 - \frac{C_n}{nR} - \frac{1}{nR}. \tag{4.38}$$

Taking the minimum of all possible codes, and using the additivity (4.28), we have in the limit $n \to \infty$

$$\liminf_{n \to \infty} \bar{p}_e\left(n, 2^{nR}\right) \geq 1 - \frac{C_{\text{Shan}}}{R} > 0$$

for $R > C_{\text{Shan}}$.

Proof of the direct statement. The main idea, due to Shannon, is to use random coding. Take N independent codewords $w^{(1)}, \ldots, w^{(N)}$ with the same probability distribution

$$\mathrm{P}\left\{w^{(i)} = (x_1, \ldots, x_n)\right\} = p_{x_1} \cdots p_{x_n}, \tag{4.39}$$

where the input distribution $P = \{p_x\}$ is chosen such that it maximizes $I(X; Y)$. Note that we have $2^{nH(X)}$ $\left(2^{nH(Y)}\right)$ typical codewords for the input (output) and on average $2^{nH(Y|X)}$ typical outputs for every input codeword w. In order for the error in the discrimination between different words at the output to tend to zero, it is necessary that the sets of typical output words corresponding to different input words do not intersect asymptotically. Hence, the size of the code is

$$N \approx \frac{2^{nH(Y)}}{2^{nH(Y|X)}} = 2^{n(H(Y) - H(Y|X))} = 2^{nI(X;Y)} = 2^{nC_{\text{Shan}}} \tag{4.40}$$

To make this argument precise, let us call an output word y^n conditionally typical for the input word $w = x^n$ if

$$2^{-n(H(Y|X)+\delta)} < p\left(y^n \mid w\right) < 2^{-n(H(Y|X)-\delta)}. \tag{4.41}$$

Denote by $T_w^{n,\delta} \subset \mathcal{Y}^n$ the subset of all conditionally typical words for the given input word w.

Exercise 4.15 Assuming that w is random, with distribution (4.39), show, by using the law of large numbers, that $\mathrm{P}\left\{Y^n \in \overline{T_w^{n,\bar{\delta}}}\right\} \le \varepsilon$ for arbitrary $\varepsilon > 0$ and sufficiently large n.

For a given encoding $W = \left\{w^{(1)}, \ldots, w^{(N)}\right\}$, we construct a special suboptimal decoding. The subsets $T_{w^{(j)}}^{n,\delta}$ may be intersecting for different j. Hence, to obtain nonintersecting decision domains we put

$$V^{(j)} = T_{w^{(j)}}^{n,\delta} \cap \overline{\left(\bigcup_{k:k\neq j} T_{w^{(k)}}^{n,\delta}\right)}. \tag{4.42}$$

Now, if, e. g., the word $w^{(1)}$ was transmitted, the error occurs if and only if

$$y^n \in \overline{V^{(1)}} = \overline{T_{w^{(1)}}^{n,\delta}} \cup \left(\bigcup_{k=2}^{N} T_{w^{(k)}}^{n,\delta}\right). \tag{4.43}$$

We now assume that the codewords $w^{(1)}, \ldots, w^{(N)}$ are selected randomly, as described above, i. e., independently, each with distribution (4.39), and let us evaluate the expectation of the mean error probability $\bar{P}_e(W, V)$. This will give us the required estimate, since obviously

$$\bar{p}_e(n, N) \le \mathrm{E}\bar{P}_e(W, V).$$

Denote by $\mathrm{P}_w\{B\}$ the probability $\mathrm{P}\left\{Y^n \in B \mid X^n = w\right\}$, where B is some, possibly random, subset of $\mathcal{Y}^n$. Due to the complete symmetry between the codewords,

$$\begin{aligned} \mathrm{E}\bar{P}_e(W, V) &= \mathrm{EP}_{w^{(1)}}\left\{\overline{V^{(1)}}\right\} \\ &= \mathrm{EP}_{w^{(1)}}\left\{\overline{V^{(1)}} \cap T^{n,\delta}(Y)\right\} + \mathrm{EP}_{w^{(1)}}\left\{\overline{V^{(1)}} \cap \overline{T^{n,\delta}(Y)}\right\} \end{aligned} \tag{4.44}$$

where $T^{n,\delta}(Y)$ is the set of the output δ-typical sequences y^n, defined similarly to Definition 4.2 with the replacement of $H(X)$ by $H(Y)$. Then, taking into account (4.43),

$$\mathrm{E}\bar{P}_e(W, V) \le \mathrm{P}\left\{Y^n \in \overline{T_{w^{(1)}}^{n,\delta}}\right\} + \sum_{k=2}^{N} \mathrm{EP}_{w^{(1)}}\left\{T_{w^{(k)}}^{n,\delta} \cap T^{n,\delta}(Y)\right\} + \mathrm{P}\left\{\overline{T^{n,\delta}(Y)}\right\}. \tag{4.45}$$

The first and third terms are $\le \varepsilon$ for sufficiently large n by the corresponding properties of the (conditionally) nontypical words. Each term in the second sum is evaluated as

$$\begin{aligned} &\sum_{w^{(1)}} \sum_{w^{(k)}} \sum_{y^n \in T_{w^{(k)}}^{n,\delta} \cap T^{n,\delta}(Y)} p\left(y^n \mid w^{(1)}\right) p_{w^{(1)}} p_{w^{(k)}} \\ &\quad \le 2^{n(H(Y|X)+\delta)} \sum_{w^{(1)}} \sum_{w^{(k)}} \sum_{y^n \in T^{n,\delta}(Y)} p\left(y^n \mid w^{(1)}\right) p_{w^{(1)}} p\left(y^n \mid w^{(k)}\right) p_{w^{(k)}} \\ &\quad = 2^{n(H(Y|X)+\delta)} \sum_{y^n \in T^{n,\delta}(Y)} (p_{y^n})^2 \le 2^{n(H(Y|X)-H(Y)+2\delta)}. \end{aligned}$$

Here, the first inequality is obtained by introducing the factor

$$2^{n(H(Y|X)+\delta)} p\left(y^n \mid w^{(k)}\right) > 1$$

on the set $T^{n,\delta}_{w^{(k)}}$, while the last one follows from the second inequality in the definition of a typical word y^n and the fact that $\mathrm{P}\left\{T^{n,\delta}(Y)\right\} \leq 1$. Finally,

$$E\bar{P}_e(W,V) \leq 2\varepsilon + (N-1)2^{n(H(Y|X)-H(Y)+2\delta)} \leq 2\varepsilon + N2^{-n(C_{\text{Shan}}-2\delta)},$$

which can be made less than 3ε if $N = 2^{nR}$, with $R < C_{\text{Shan}}$ and δ sufficiently small. □

It should be noted that the method of random encoding that allows us to prove the existence of asymptotically optimal codes and which discloses their nature is unfortunately not very suitable for practical applications. Its realization even for moderate values of n requires a huge (exponentially growing) amount of computation for the decoding. The development of practically acceptable methods of encoding and decoding is the subject of a special topic in information theory - coding theory - which makes ample use of the methods of modern algebra and combinatorics.

10.4.5 4.5 Wiretap Channel

Another important issue in modern information theory is the study of multiple user systems - networks - such as the internet. A specific example of a system with a malicious party is the wiretap channel, which we will briefly discuss here, since it will be used in Chapter 10, which is devoted to quantum information transmission.

Let $\mathcal{X}, \mathcal{Y}, \mathcal{Z}$ be finite alphabets, where alphabet $\mathcal{X}$ is associated with the transmitter, $\mathcal{Y}$ with the receiver, and $\mathcal{Z}$ with an eavesdropper. A wiretap channel is determined by a pair of channels $p(y \mid x), q(z \mid x)$, one from transmitter to receiver and another from transmitter to eavesdropper. The transmitter sends the words $w = (x_1, \ldots, x_n)$ of length n through the channels $p\left(y^n \mid x^n\right), q\left(z^n \mid x^n\right)$, and the goal is to achieve asymptotically exact transmission of a maximal amount of information to the receiver, subject to the condition that the eavesdropper receives an asymptotically negligible amount of information.

Definition 4.16. For a composite wiretap channel, the code $(\mathcal{M}, r, V)$ of size N consists of a collection of messages $\mathcal{M} = \{1, \ldots, N\}$, the transition probability $r\left(x^n \mid m\right)$ from $\mathcal{M}$ to $\mathcal{X}^n$, defining the randomized encoding of the messages $m \in \mathcal{M}$ into words x^n, and a decoding V for the receiver, given by a decomposition of the set $\mathcal{Y}^n$ into $N+1$ pairwise nonintersecting subsets $V^{(0)}, V^{(1)}, \ldots, V^{(N)} \subset \mathcal{Y}^n$.

The maximal error probability of such a code is equal to

$$P_e(\mathcal{M}, r, V) = \max_{1 \leq m \leq N} \left(1 - p\left(V^{(m)} \mid m\right)\right), \tag{4.46}$$

where $p\left(V^{(m)} \mid m\right) = \sum_{x^n} \mathrm{P}\left(Y^n \in V^{(m)} \mid x^n\right) r\left(x^n \mid m\right)$ is the probability of a correct decision for the receiver. We call R achievable rate for the wiretap channel if there exists a sequence of codes $\left(\mathcal{M}^{(n)}, r^{(n)}, V^{(n)}\right)$ of sizes $N = 2^{nR}$ such that

$$\lim_{n\to\infty} P_e\left(\mathcal{M}^{(n)}, r^{(n)}, V^{(n)}\right) = 0$$

and

$$\lim_{n\to\infty} I\left(M^n; Z^n\right) = 0,$$

where M^n is a random variable, uniformly distributed over the set of messages $\mathcal{M}^{(n)}$. The last condition expresses the requirement that the eavesdropper's information about the transmitted messages should tend to zero. The supremum of the achievable rates is called the private capacity C_p of the wiretap channel.

The coding theorem for the wiretap channel provides the following expression:

$$C_p = \max[I(M;Y) - I(M;Z)], \tag{4.47}$$

where the maximum is taken over all possible triples of random variables M, Y, Z, such that the sequence $M, X, (Y, Z)$ is a Markov chain, while the couples X, Y and X, Z are related correspondingly via channels $p(y \mid x)$ and $q(z \mid x)$.

The proof is based on the following idea. Let us fix $\delta, \varepsilon > 0$ and a distribution for X and let $T^{n,\delta}$ be the set of δ-typical words of length n. Consider the "pruned" random encoding $W^{(n)}$ which uses N independent words, each uniformly distributed over the set $T^{n,\delta}$. Let $V^{(n)}$ be the suboptimal decoding for Y constructed as in (4.42). A modification of the proof of Theorem 4.13 allows us to prove that for $N = 2^{n[I(X;Y)-\delta]}$ the inequality

$$\bar{P}_e\left(W^{(n)}, V^{(n)}\right) \leq \varepsilon \tag{4.48}$$

holds with a high probability.

To make the code secret, the transmitter has to sacrifice $n[I(X;Z) + \delta/2]$ bits of information by additional randomization of the messages. Assuming $I(X;Y) - I(X;Z) > 0$, let

$$N_{\mathcal{Z}} = 2^{n[I(X;Z)+\delta/2]}, \quad N_{\mathcal{Y}} = 2^{n[I(X;Y)-I(X;Z)-3\delta/2]},$$

so that $N_{\mathcal{Z}} N_{\mathcal{Y}} = N$. Let us arrange the array of all codewords $W^{(n)}$ as a matrix with $N_{\mathcal{Y}}$ rows and $N_{\mathcal{Z}}$ columns. In this case,

$$W^{(n)} = \left\{w^{mj}; m = 1, \ldots, N_{\mathcal{Y}}; j = 1, \ldots, N_{\mathcal{Z}}\right\}.$$

Next, let for any message m the transmitter choose the values j randomly, with equal probabilities. It can be shown that such a randomization makes almost all transmitted information hidden for the eavesdropper. For every m the collection of codewords

$$\left\{w^{mj}; j = 1, \ldots, N_{\mathcal{Z}}\right\} \tag{4.49}$$

with high probability contains almost maximal possible information $I(X;Z)$, subject to the condition that the eavesdropper uses optimal decoding. In other words, for every value of m, the sets of conditionally typical words corresponding to (4.49) cover almost the whole set of typical words for Z. The mutual information between the collections of codewords with different values of m is close to zero, so that randomization inside each collection erases almost all information going to the eavesdropper. This argument, together with relation (4.48), shows that the rate $I(X;Y) - I(X;Z) - \delta$ should be achievable, while randomization is equivalent to using an additional channel $M \to X$. A modification of a similar argument for any triple M, X, YZ satisfying the conditions of the coding theorem allows us to show that $I(M;Y) - I(M;Z) - \delta$ is also an achievable rate.

10.4.6 4.6 Gaussian Channel

Consider the continuous analog of the memoryless channel (4.27), with the real line $\mathbb{R}$ as the input and output alphabets. The channel is defined by the transition probability density

$$p\left(y_i \mid x_i\right) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left[-\frac{\left(y_i - x_i\right)^2}{2\sigma^2}\right], \quad i = 1, \ldots, n.$$

Equivalently, one obtains the output random variables Y_i by addition of the noise given by i.d.d. Gaussian random variables Z_i to the input signal x_i, with $\mathrm{E}Z_i = 0$ and $\mathrm{E}Z_i^2 = \sigma^2$, i.e.,

$$Y_i = x_i + Z_i, \quad i = 1, \ldots, n$$

Clearly, the naturally defined information capacity of such a channel is infinite if one does not introduce constraints on the signal. Usually, the quadratic constraint is considered, i. e.,

$$\sum_{i=1}^{n} x_i^2 \le ns^2 \tag{4.50}$$

motivated by the finiteness of the signal power. Under this constraint the channel capacity is computed as

$$C = \frac{1}{2} \log \left(1 + \frac{s^2}{\sigma^2} \right) \tag{4.51}$$

This formula also belongs to Shannon and it also has a simple heuristic explanation. The inequalities

$$\frac{1}{n} \sum_{i=1}^{n} Z_i^2 \le \sigma^2 + \varepsilon, \quad \frac{1}{n} \sum_{i=1}^{n} Y_i^2 \le s^2 + \sigma^2 + \varepsilon$$

hold with high probability for arbitrary $\varepsilon > 0$ and sufficiently large n.

Exercise 4.17 Prove this statement by using the Markov inequality $\mathrm{P}\{X \ge \varepsilon\} \le \mathrm{E}X/\varepsilon$ for a nonnegative random variable X and the relation (4.50).

The first of these inequalities means that, for any input word $w = (x_1, \ldots, x_n)$, the output vector $Y^n = (Y_1, \ldots, Y_n)$ lies in an n-dimensional ball with radius $\sqrt{n\,(\sigma^2 + \varepsilon)}$ and center w, while the second tells us that the output vectors for arbitrary inputs that satisfy constraint (4.50) lie in an n-dimensional ball of radius $\sqrt{n\,(s^2 + \sigma^2 + \varepsilon)}$, with its center at the origin. The ratio of the volumes of these balls gives an approximate value for the quantity of balls of the first type within the big ball,

$$N = \left[\frac{\sqrt{n\,(s^2 + \sigma^2 + \varepsilon)}}{\sqrt{n\,(\sigma^2 + \varepsilon)}} \right]^n = 2^{nR}$$

where $R = \frac{1}{2} \log \left(1 + \frac{s^2}{\sigma^2 + \varepsilon} \right)$, which can be made arbitrarily close to (4.51).

10.4.7 4.7 Notes and References

1. The ideas of reliable data transmission have been promoted since the 1930s and even earlier (see Verdú [236] for a detailed historical survey). Remarkably, Kotelnikov, the Russian pioneer in the field, maintained a deep interest in the foundations of quantum mechanics throughout his life. The mathematical tradition in information theory goes back to the 1950s, when Khinchin and Kolmogorov gave insights into Shannon's discoveries from the viewpoint of advanced probability theory. Nowadays, there are many excellent texts on information theory. Here, we mainly follow the book of Cover and Thomas [47], which provides an enlightening, nontechnical introduction to the subject. The method of types was systematically developed by Cziszar and Körner [50].

2. The idea of using the exponential function in the Markov inequality with subsequent large deviation estimates goes back to Bernstein, followed by Cramér. Its importance to information theory and statistics was emphasized in the work of Chernoff, see, e. g., [47], Lemma 12.9.1, and also [78].

3. For a complete proof of Exercise 4.8 and its application to the additivity of the Shannon capacity, see Gallager [78], Theorems 4.4.1, 4.5.1.

4. The heuristic argument for the direct coding theorem was already present in Shannon's pioneering paper [206]. Our proof differs from the one given in the book [47] in that it uses conditional rather than joint typicality. It is this approach that allows for the noncommutative extension; see Section 5.6.

5. Theory of multiuser systems is presented in the books of Cziszar and Körner [50] and Cover and Thomas [47]. The proof of the coding theorem for the wiretap channel is given in [50].

6. For a rigorous proof of formula (4.51), see, e. g., [47]. The quantum analog of the channel with additive Gaussian noise is considered in Section 12.1.4.

10.5 5 The Classical-Quantum Channel

10.5.1 5.1 Codes and Achievable Rates

As was explained in Section 3.3.1, a simple mathematical model of a quantum communication channel is given by a map $x \to S_x$ that transforms the letters x of a (finite) input alphabet $\mathcal{X}$ into the quantum states at the channel output. We will call such a model a classical-quantum (c-q) channel. If an observable $M = \{M_y\}$ is measured at the output of such a channel, the conditional probability to obtain the outcome y, under the condition that the signal x was sent, is given by the formula

$$p(y \mid x) = \operatorname{Tr} S_x M_y. \tag{5.1}$$

Thus, for a fixed quantum measurement we have a usual classical channel. This leads to the question as to the maximum amount of classical information that can be transmitted through the quantum communication channel with asymptotically vanishing error, i.e., its "classical capacity." This question will be considered in detail in the present chapter.

Consider the composite c-q channel which maps a word $w = (x_1, \dots, x_n)$ into the product state $S_w = S_{x_1} \otimes \cdots \otimes S_{x_n}$ in the space $\mathcal{H}^{\otimes n}$. The process of transmission of classical information is described by the diagram

$$i \xrightarrow{\text{encoding}} w \xrightarrow{\text{channel}} S_w \xrightarrow{\text{decoding}} j. \tag{5.2}$$

The assumption that a word w is mapped into the tensor product of states S_{x_j} corresponds to the definition of a memoryless channel in the classical case. At the channel output, there is a receiver which performs a measurement of an observable $M = \left\{ M_j^{(n)} \right\}$ in the space $\mathcal{H}^{\otimes n}$ (the outcome j means that the receiver decides that the signal j was sent). Thus, the resolution of the identity in the space $\mathcal{H}^{\otimes n}$ describes the overall statistics of the decision procedure, including both the physical measurement and the subsequent classical information processing. The choice of the observable M is formally similar to the choice of the decision rule in the classical case, but here it plays a much more significant role, as we shall see.

Definition 5.1. A code (W, M) of size N consists of a classical codebook $W = \left\{ w^{(i)}; i = 1, \dots, N \right\}$, which is a collection of N codewords of length n, and a quantum decision rule given by an observable $M = \{M_j; j = 0, 1, \dots, N\}$ in $\mathcal{H}^{\otimes n}$. An outcome $j = 1, \dots, N$ corresponds to the decision that the word w^j was sent, while $j = 0$ means no definite decision.

The probability of decoding the signal i as j is equal to

$$p_{WM}(j \mid i) = \operatorname{Tr} S_{w^{(i)}} M_j, \quad j = 0, 1, \ldots, N. \tag{5.3}$$

Then the probability of a correct decision is $p_{WM}(i \mid i) = \operatorname{Tr} S_{w^{(i)}} M_i$, while the maximal error probability of the code $(\ W, M\ )$ is equal to

$$P_e(W, M) = \max_{1 \le j \le N} \left[1 - p_{WM}(j \mid j)\right]. \tag{5.4}$$

The average error probability is

$$\bar{P}_e(W, M) = \frac{1}{N} \sum_{j=1}^{N} \left[1 - p_{WM}(j \mid j)\right]. \tag{5.5}$$

In what follows we denote by

$$p_e(n, N) = \min_{W,M} P_e(W, M), \quad \bar{p}_e(n, N) = \min_{W,M} \bar{P}_e(W, M) \tag{5.6}$$

the maximal and the average error, respectively, minimized over all codes $(\ W, M\ )$ of size N, using words of length n.

Definition 5.2. The classical capacity C of the c−q channel $x \to S_x$ is equal to the supremum of the transmission rates R that are achievable, in the sense that $\lim_{n\to\infty} p_e\left(n, 2^{nR}\right) = 0$ or, equivalently (by inequalities (4.32)), that $\lim_{n\to\infty} \bar{p}_e(n,\ 2^{nR}) = 0$.

10.5.2 5.2 Formulation of the Coding Theorem

The notion of the entropy of a quantum state is a natural extension of the entropy of a probability distribution. Let S be a density operator in d-dimensional Hilbert space $\mathcal{H}$, and let

$$S = \sum_{j=1}^{d} s_j \left|e_j\right\rangle \left\langle e_j\right|$$

be its spectral decomposition. Its eigenvalues s_j form a probability distribution. The von Neumann entropy of the density operator S is defined as

$$H(S) = -\sum_{j=1}^{d} s_j \log s_j = \operatorname{Tr} \eta(S) \tag{5.7}$$

where the function $\eta(\cdot)$ is given by (4.2), and is equal to the Shannon entropy of the probability distribution $\{s_j\}$. In what follows we use a more spectacular expression $H(S) = -\operatorname{Tr} S \log S$, although the logarithm is not defined for degenerate density operators. As in the case of distributions, this will not lead to ambiguities. From (4.3) it follows that

$$0 \le H(S) \le \log d$$

with the minimum achieved on pure states, and the maximum on the chaotic state $\bar{S} = \frac{1}{d} I$. As in the classical case, the entropy is a measure of the uncertainty and also of the information content of the state (this last statement will be substantiated in Section 5.5).

The following properties of the quantum entropy are easy to check.

Exercise 5.3

i. Unitary invariance: $H(VSV^*) = H(S)$, where V is a unitary operator. Moreover, this equality holds for any operator V, isometric on the support of S.
ii. Additivity: $H(S_1 \otimes S_2) = H(S_1) + H(S_2)$.

In earlier works on quantum communications, the quantity

$$\chi(\{\pi_\chi\}; \{S_\chi\}) = H\left(\sum_x \pi_\chi S_x\right) - \sum_x \pi_x H(S_x), \tag{5.8}$$

with $\pi = \{\pi_x\}$ a probability distribution on $\mathcal{X}$, was used to evaluate the capacity of the c -q channel $x \to S_x$ on heuristic grounds. The quantity (5.8) can be considered a formal quantum analog of the Shannon information, where the first term plays the role of the output entropy, and the second that of the conditional entropy of the output with respect to the input. Remarkably, this quantity appears to be strictly related to the classical capacity of the $c - q$ channel as defined in the previous section. When the states $\{S_x\}$ are fixed and there is no risk of confusion, we shall abbreviate the notation (5.8) as $\chi(\pi)$ and put

$$C_\chi = \max_\pi \chi(\pi). \tag{5.9}$$

The main goal of the next sections will be the proof of the following coding theorem.

Theorem 5.4 (Holevo [113]; Schumacher and Westmoreland [200]). The classical capacity C of the $c - q$ channel $x \to S_x$, defined as in Definition 5.2, is equal to C_x.

Note that the quantum entropy is continuous on the compact set of quantum states, hence χ is continuous in π and the maximum in the above formula is indeed achieved. Let us introduce the notation

$$\bar{S}_\pi = \sum_x \pi_x S_x \tag{5.10}$$

for the average output state. In general,

$$\chi(\pi) \le H\left(\bar{S}_\pi\right),$$

with equality in the case of the pure-state channel $S_x = |\psi_x\rangle\langle\psi_x|$. Since the maximum possible value of the entropy is $\log \dim \mathcal{H}$, this theorem implies an absolute upper bound on the classical capacity, i.e.,

$$C \le \log \dim \mathcal{H}. \tag{5.11}$$

Thus, in spite of the fact that in a Hilbert space there are infinitely many different pure states, the finite-dimensional quantum carrier cannot be used to transmit an unlimited amount of classical information. The upper bound (5.11) is achieved for the channel with orthogonal pure states $S_x = |e_x\rangle\langle e_x|, x = 1, \ldots, d$, where $\{e_x\}$ is an orthonormal basis in $\mathcal{H}, d = \dim \mathcal{H}$, and for the uniform distribution $\pi_x \equiv 1/d$. Note that such states, as a rule, cannot be obtained at the output of a realistic communication channel. It is remarkable, however, that orthogonality of the output states is not necessary in order to attain the capacity of the ideal quantum channel.

Example 5.5. Consider the trine channel with the three equiangular pure states ψ_0, ψ_1, ψ_2 in a two-dimensional Hilbert space as in Example 2.27. Taking the equal probabilities $\pi_x = \frac{1}{3}$, we obtain the chaotic average output state

$$\bar{S}_\pi = \sum_{x=0}^{2} \pi_x |\psi_x\rangle\langle\psi_x| = \frac{1}{2} I, \tag{5.12}$$

implying $C_\chi = \log 2 = 1$ bit, i. e., the capacity of the ideal channel.
More generally, if $\{\psi_x\}$ is an arbitrary overcomplete system in a Hilbert space $\mathcal{H}$, the pure state channel $x \to \frac{|\psi_x\rangle\langle\psi_x|}{\langle\psi_x|\psi_x\rangle}$ has the maximum possible capacity $\log d$, and the maximum is attained on the distribution $\pi_x = \langle\psi_x \mid \psi_x\rangle / d$.

Example 5.6. Consider a binary channel with two pure states with unit vectors ψ_0, ψ_1 as in Example 2.25. In this case,

$$C_\chi = h_2\left(\frac{1+\epsilon}{2}\right), \tag{5.13}$$

where $\epsilon = |\langle\psi_0 \mid \psi_1\rangle|$. Indeed, the entropy $H\left(\bar{S}_\pi\right)$ is maximized by the uniform distribution $\pi_0 = \pi_1 = \frac{1}{2}$ since, by concavity of the quantum entropy (see Corollary 7.17 in Chapter 7),

$$H\left(\frac{1}{2}|\psi_0\rangle\langle\psi_0| + \frac{1}{2}|\psi_1\rangle\langle\psi_1|\right) = H\left(\frac{S+S'}{2}\right) \geq \frac{1}{2}\left(H(S) + H\left(S'\right)\right),$$

where

$$S = \pi_0|\psi_0\rangle\langle\psi_0| + \pi_1|\psi_1\rangle\langle\psi_1|, \quad S' = \pi_1|\psi_0\rangle\langle\psi_0| + \pi_0|\psi_1\rangle\langle\psi_1|,$$

and $H\left(S'\right) = H(S)$ due to the reflection symmetry with respect to the bisector of the angle between the two vectors. Similar to the solution of Exercise 2.26, the eigenvalues of the density operator $\frac{1}{2}|\psi_0\rangle\langle\psi_0| + \frac{1}{2}|\psi_1\rangle\langle\psi_1|$ are equal to $\frac{1\pm\epsilon}{2}$, whence (5.13) follows.

10.5.3 5.3 The Upper Bound

Consider an arbitrary c-q channel $x \to S_x$ and an observable $M = \{M_y\}$ at its output. Note that the alphabets $\mathcal{X}$ and $\mathcal{Y}$ need not coincide. The variables x and y are related by the classical channel $p_M(y \mid x) = \operatorname{Tr} S_x M_y$. Denote by

$$\mathcal{I}_1(\pi, M) = \sum_{xy} \pi_x p_M(y \mid x) \log\left(\frac{p_M(y \mid x)}{\sum_{x'} p_M\left(y \mid x'\right)\pi_{x'}}\right) \tag{5.14}$$

the Shannon information between the variables x and y corresponding to some input distribution $\pi = \{\pi_x\}$.

> Exercise 5.7 Prove that for given π and $\mathcal{Y}$ the information quantity $\mathcal{I}_1(\pi, M)$ is a continuous and convex function of the transition probability $p_M(y \mid x)$, and hence of M. Hint: use the corresponding property of the Shannon information $I(X;Y)$.

For given distribution π on the input alphabet, consider the accessible information

$$A(\pi) = \sup_M \mathcal{I}_1(\pi, M),$$

where the supremum is taken over all possible observables at the output of the channel $x \to S_x$.

Proposition 5.8 (Davies [55]). The supremum of the information quantity $\mathcal{I}_1(\pi, M)$ is attained by the observable M^0 of the form

$$M^0_y = |\phi_y\rangle\langle\phi_y|, \quad y = 1, \ldots, m, \tag{5.15}$$

where $m \leq d^2$ in the case of complex $\mathcal{H}$ $\left(m \leq \frac{d(d+1)}{2}\right.$ in the case of real $\left.\mathcal{H}\right)$.
Proof. For any $k = 2, 3, \ldots$ the set $\mathfrak{M}_k$ of observables with k outcomes is compact, and the

continuous convex functional $\mathcal{I}_1(\pi, M)$ attains its maximum on the set $\mathfrak{M}_k$. Assume that $\hat{M}^0$ maximizes $\mathcal{I}_1(\pi, M)$ on $\mathfrak{M}_k$. By throwing off, if necessary, zero components, we obtain the observable $\tilde{M}^0 \in \mathfrak{M}_l, l \leq k$, for which $\mathcal{I}_1\left(\pi, \tilde{M}^0\right) = \mathcal{I}_1\left(\pi, \hat{M}^0\right)$. By making the spectral decomposition of the components of the observable $\tilde{M}^0$ into rank one operators, we can construct the new observable M^0 of the form (5.15), with $m \geq l$, for which $\tilde{M}^0$ is a coarse-graining,

$$\underbrace{M_1, M_2, \ldots}_{=\tilde{M}_1}, \underbrace{i_1}_{=\tilde{M}_2} \cdots, \underbrace{\ldots, M_m}_{=\tilde{M}_l}.$$

Then $\mathcal{I}_1(\pi, M^0) \geq \mathcal{I}_1\left(\pi, \tilde{M}^0\right)$. In fact, this is a statement about the classical Shannon information, $I(X; f(Y)) \leq I(X; Y)$ or, equivalently, $H(X \mid f(Y)) \geq H(X \mid Y)$, which follows from the monotonicity of the classical conditional entropy, since $H(X \mid Y) = H(X \mid f(Y), Y)$.

The function $M \to \mathcal{I}(\pi, M)$ is convex. Therefore, we can assume that the maximizing observable $M^0 = \left\{M_y^0\right\}$ is an extreme point of the set $\mathfrak{M}_m$. Then, according to Theorem 2.21, the operators M_y^0 are linearly independent and Exercise 1.5 implies the estimate $m \leq d^2$. Since k was arbitrary, it follows that $\sup_M \mathcal{I}_1(\pi, M)$ is attained on an observable from the compact convex set $\mathfrak{M}_{d^2}$. □

Theorem 5.9 (Holevo [111]). For an arbitrary distribution π

$$A(\pi) \equiv \max_M \mathcal{I}_1(\pi, M) \leq \chi(\pi), \tag{5.16}$$

with equality attained if and only if the operators $\pi_x S_x, x \in \mathcal{X}$ all commute.

In Chapter 7, we will obtain the information bound (5.16) as a corollary of the rather general monotonicity property of the quantum relative entropy. Here we give instead an outline of the original proof, based on the comparison of the convexity of the classical and quantum entropies. This proof reveals a connection between the quantum entropy and the noncommutative analog of the Fisher information, and moreover allows us to obtain a necessary and sufficient condition for equality. The latter condition will be used in the next section, in order to establish the nonclassical property of superadditivity of the Shannon information for the c-q channel.

Proof. Without loss of generality, we assume all $\pi_x > 0$. In this case, the condition for equality amounts to the commutativity of all operators S_x. Now, equality in (5.16) is apparently achieved by the common spectral measure M of the operators S_x.

To prove the inequality let us first consider the case of two states S_0, S_1. Denote

$$\chi(t) = H\left((1-t)S_0 + tS_1\right) - (1-t)H\left(S_0\right) - tH\left(S_1\right), \quad t \in [0, 1]. \tag{5.17}$$

Also set $S_t = (1-t)S_0 + tS_1, D = S_1 - S_0$ and let $S_t = \sum_k s_k E_k$ be the spectral decomposition of the operator S_t. Here and in what follows, s_k will denote strictly positive eigenvalues.

By using Cauchy's integral formula, we have

$$S_t \log S_t = \frac{1}{2\pi i} \oint (Iz - S_t)^{-1} z \log z dz,$$

where $z \log z$ is the branch of the function, analytic in the right halfplane, and the integral is taken over a closed contour embracing the segment $[\varepsilon, 1], \varepsilon > 0$, which contains all positive eigenvalues of S_t. Differentiating twice with respect to t,

$$[S_t \log S_t]'' = \frac{1}{2\pi i} \oint \left[(Iz - S_t)^{-1}\right]'' z \log z dz,$$

where, using the resolvent expansion and taking into account that $S_t' = D$,

$$\left[(Iz - S_t)^{-1}\right]'' = 2\left(Iz - S_t\right)^{-1} D \left(Iz - S_t\right)^{-1} D \left(Iz - S_t\right)^{-1}.$$

By using the fact that $\operatorname{Tr} E_k D E_j D = \operatorname{Tr} E_j D E_k D$ due to (1.11), we have

$$\begin{aligned}\chi''(t) &= -\frac{1}{\pi i}\oint \operatorname{Tr}\left(Iz - S_t\right)^{-2} D \left(Iz - S_t\right)^{-1} D z \log z dz \\ &= -\frac{1}{\pi i}\oint \sum_{k,j} \frac{\operatorname{Tr} E_k D E_j D}{\left(z - s_k\right)^2 \left(z - s_j\right)} z \log z dz \\ &= -\sum_{k,j} \left(\operatorname{Tr} E_k D E_j D\right) f\left(s_k, s_j\right) \end{aligned} \tag{5.18}$$

where

$$\begin{aligned} f(a,b) &= \frac{1}{2\pi i}\oint \left[\frac{1}{(z-a)^2(z-b)} + \frac{1}{(z-b)^2(z-a)}\right] z \log z dz \\ &= \frac{\log a - \log b}{a-b}, \quad a \neq b, f(a,a) = a^{-1} \end{aligned} \tag{5.19}$$

Note that $\operatorname{Tr} E_k D E_j D = \operatorname{Tr} E_k D E_j D E_k \geq 0$. By using the inequality

$$f(a,b) \geq \frac{2}{a+b}, \quad 0 < a, 0 < b \tag{5.20}$$

in which equality is obtained if and only if $a = b$, we have

$$\chi''(t) \leq -\sum_{k,j} \operatorname{Tr} E_k D E_j D \frac{2}{s_k + s_j}, \tag{5.21}$$

with equality attained if and only if $\operatorname{Tr} E_k D E_j D = 0$ for all $k \neq j$. The latter condition is equivalent to $[D, S_t] = 0$, i. e., $[S_0, S_1] = 0$, because of the identity

$$\operatorname{Tr}\left[D, S_t\right]^* \left[D, S_t\right] = \sum_{k,j} \left(s_k - s_j\right)^2 \operatorname{Tr} E_k D E_j D$$

Exercise 5.10 Prove relation (5.19) and inequality (5.20).
Exercise 5.11 Show that the operator

$$L_t = \sum_{k,j} E_k D E_j \frac{2}{s_k + s_j}$$

is a solution of the equation

$$S_t \circ L_t \equiv \frac{1}{2}\left[S_t L_t + L_t S_t\right] = D$$

Moreover, show that

$$\sum_{k,j} \operatorname{Tr} E_k D E_j D \frac{2}{s_k + s_j} = \operatorname{Tr} D L_t = \operatorname{Tr} S_t L_t^2. \tag{5.22}$$

The operator L_t is a noncommutative (symmetric) analog of the logarithmic derivative of the operator-valued function S_t, while (5.22) is an analog of the Fisher information quantity in mathematical statistics. From (5.21), (5.22) it follows that

$$\chi''(t) \leq -\operatorname{Tr} D L_t = -\operatorname{Tr} S_t L_t^2, \quad 0 < t < 1; \tag{5.23}$$

in particular, $\chi''(t) \leq 0$, so that $\chi(t)$ is concave on the segment [0,1] with $\chi(0) = \chi(1) = 0$. Moreover, equality in (5.23) is achieved if and only if $[S_0, S_1] = 0$.

Now let $M = \{M_y\}$ be an arbitrary observable, let $P_t(y) = \operatorname{Tr} S_t M_y = (1-t)P_0(y) + tP_1(y)$ be its distribution in the state S_t, and $J_M(t) = \mathcal{I}_1(\pi, M)$, where $\pi = \{1-t, t\}$. In other words,

$$J_M(t) = H\left((1-t)P_0 + tP_1\right) - (1-t)H\left(P_0\right) - tH\left(P_1\right),$$

where $H(P)$ is the Shannon entropy of the probability distribution P. Also denote $D(y) = P_1(y) - P_0(y)$. Applying the previous argument to the diagonal matrix $\operatorname{diag}[P_t(y)]$ instead of the state S_t, we obtain

$$J''_M(t) = -\sum_y \frac{D(y)^2}{P_t(y)} = -\operatorname{Tr} D\Lambda_t, \tag{5.24}$$

where

$$\Lambda_t = \sum_y M_y \frac{D(y)}{P_t(y)}.$$

The first equality in (5.24) diagonal matrices. The right-hand side of (5.24) is equal to minus the classical Fisher information for the family of measurement probability distributions. We have $J''_M(t) \leq 0$, so that the function $J_M(t)$ is concave on $[0, 1]$, and $J_M(0) = J_M(1) = 0$.

Finally, let us prove that

$$J''_M(t) \geq \chi''(t), \tag{5.25}$$

and hence

$$J_M(t) \leq \chi(t), \quad 0 < t < 1, \tag{5.26}$$

with the sharp inequality if $[S_0, S_1] \neq 0$.

Proof of inequality (5.25). First note that

$$\operatorname{Tr} DM_y = \operatorname{Tr}\left(S_t \circ L_t\right) M_y = \operatorname{Re} \operatorname{Tr} S_t L_t M_y,$$

hence by using the noncommutative Cauchy-Schwarz inequality

$$\left(\operatorname{Tr} DM_y\right)^2 \leq \left|\operatorname{Tr} S_t \left(L_t \sqrt{M_y}\right) \sqrt{M_y}\right|^2 \leq \left(\operatorname{Tr} S_t L_t M_y L_t\right) \cdot \left(\operatorname{Tr} S_t M_y\right).$$

By using (5.24),

$$-J''_M(t) \leq \sum_y \operatorname{Tr} S_t L_t M_y L_t = \operatorname{Tr} S_t L_t^2 \leq -\chi''(t)$$

where in the last inequality (which is sharp if $[S_0, S_1] \neq 0$) we invoked (5.23). This implies (5.25) and hence (5.26).

This completes the proof of Theorem 5.9 in the case of two states. The case of several states $S_x, x = 0, 1, \ldots, k$, with distribution $\pi = \{\pi_x; x = 0, 1, \ldots, k\}$ is reduced to the case of two states with the help of the following recurrent formula.

Exercise 5.12 Prove that

$$X(\pi) = \sum_{m=1}^{k} \left(\pi_0 + \cdots + \pi_m\right) X_m\left(t_m\right),$$

where

$$X_m(t) = H\left((1-t)S_0^m + tS_m\right) - (1-t)H\left(S_0^m\right) - tH\left(S_m\right),$$
$$t_m = \frac{\pi_m}{\pi_0 + \cdots + \pi_m},$$
$$S_0^m = \sum_{j=0}^{m-1} \frac{\pi_j S_j}{\pi_0 + \cdots + \pi_{m-1}}.$$

Similarly,

$$\mathcal{I}_1(\pi, M) = \sum_{m=1}^{k} \left(\pi_0 + \cdots + \pi_m\right) J_M^m\left(t_m\right)$$

where $J_M^m\left(t_m\right)$ are defined in the same way as $\chi_m\left(t_m\right)$, via the Shannon entropies of the measurement probability distributions. From the proven result for two states, $J_M^m\left(t_m\right) \leq \chi_m\left(t_m\right)$. Hence, inequality (5.16) follows. If there is at least a pair of noncommuting states, we can take them as S_0, S_1, and the sharp inequality follows.

10.5.4 5.4 Proof of the Weak Converse

The bound (5.16) is the main tool for proving the weak converse of the quantum coding theorem, which implies $C \leq C_\chi$.

Theorem 5.13 (Weak Converse). If $R > C_\chi$, then

$$\liminf_{n\to\infty} \bar{p}_e\left(n, 2^{nR}\right) > 0. \tag{5.27}$$

Proof. Consider the composite, memoryless c-q channel $w \to S_w$, where $w = x^{(n)}$ denote words of length n. Let $\mathcal{I}_n\left(\pi^{(n)}, M^{(n)}\right)$ be the Shannon information defined for this composite channel similarly to $\mathcal{I}_1(\pi, M)$, where $\pi^{(n)} = \{\pi_w\}$ is a probability distribution of codewords of length n and $M^{(n)}$ is an observable in $\mathcal{H}^{\otimes n}$. Then (5.16) implies

$$\mathcal{I}_n\left(\pi^{(n)}, M^{(n)}\right) \leq C_\chi^{(n)}, \tag{5.28}$$

where

$$C_\chi^{(n)} = \max_{\pi^{(n)}} \chi\left(\{\pi_w\}; \{S_w\}\right) = \max_{\pi^{(n)}} \left[H\left(\sum_w \pi_w S_w\right) - \sum_w \pi_w H\left(S_w\right)\right]. \tag{5.29}$$

Lemma 5.14. The sequence $C_\chi^{(n)}$ is additive, i.e., $C_\chi^{(n)} = nC_\chi$.

Proof. The inequality $C_\chi^{(n)} \geq nC_\chi$ follows from the additivity of the entropy by using the product input probability distributions $\pi^{(n)}$. The proof of the converse inequality $C_\chi^{(n)} \leq nC_\chi$ follows from subadditivity of the von Neumann entropy with respect to the tensor products (see Corollary 7.4), which implies

$$\chi_n\left(\pi^{(n)}\right) \leq \sum_{k=1}^{n} \chi\left(\pi^{(n,k)}\right) \tag{5.30}$$

where $\pi^{(n,k)}$ is the k th marginal distribution of π on $\mathcal{X}$. □

Defining

$$C_n = \max_{\pi^{(n)}, M^{(n)}} \mathcal{I}_n\left(\pi^{(n)}, M^{(n)}\right), \tag{5.31}$$

we thus have $C_n \leq nC_\chi$ and, applying the classical Fano inequality (4.34), we obtain, similar to (4.38),

$$\bar{P}_e(W, M) \geq 1 - \frac{C_n}{nR} - \frac{1}{nR} \geq 1 - \frac{C_\chi}{R} - \frac{1}{nR}, \tag{5.32}$$

and hence, (5.27) follows. □

The quantity C_n is the maximal Shannon information accessible through n uses of the c-q channel when arbitrary decodings are allowed on the quantum output $\mathcal{H}^{\otimes n}$. The following result clarifies its relation to the classical capacity.

Proposition 5.15. The classical capacity C of the channel $x \to S_x$ is equal to

$$\sup_n \frac{1}{n} C_n = \lim_n \frac{1}{n} C_n. \tag{5.33}$$

Proof. The equality in (5.33) follows from superadditivity of the sequence $\{C_n\}$.

Exercise 5.16 Show that the sequence C_n is superadditive, i. e., $C_{n+m} \geq C_n + C_m$, by taking product probability distributions $\pi^{(n+m)} = \pi^{(n)} \times \pi^{(m)}$.

The inequality $C \leq \sup_n \frac{1}{n} C_n$ follows from the first relation in (5.32). The opposite inequality $C \geq \sup_n \frac{1}{n} C_n$ follows from the direct statement of Shannon's coding theorem 4.13 applied to composite channels. Indeed, let us show that any $R < \sup_n \frac{1}{n} C_n$ is an achievable rate. We have $n_0 R < C_{n_0}$ for some n_0. Hence, we can choose an observable $M^{(n_0)}$ in $\mathcal{H}^{\otimes n_0}$ such that

$$n_0 R < \max_{\pi^{(n_0)}} \mathcal{I}_n \left(\pi^{(n_0)}, M^{(n_0)} \right) \equiv C \left(M^{(n_0)} \right).$$

The quantity $C\left(M^{(n_0)}\right)$ is the Shannon capacity of the classical channel

$$p_M^{(n_0)} \left(j \mid x^{n_0} \right) = \operatorname{Tr} S_{x^{n_0}} M_j^{(n_0)}. \tag{5.34}$$

Therefore, the minimal error probability for this channel satisfies $\tilde{p}_e\left(n, 2^{n(n_0 R)}\right) \to 0$ as $n \to \infty$. Apparently, $\bar{p}_e\left(nn_0, 2^{n(n_0 R)}\right) \leq \tilde{p}_e\left(n, 2^{n(n_0 R)}\right)$, since the channel (5.34) corresponds to a certain block decoding for the initial c-q channel. Thus, $\bar{p}_e\left(nn_0, 2^{n(n_0 R)}\right) \to 0$ as $n \to \infty$. For arbitrary n', one can find n such that $nn_0 \leq n' \leq (n+1)n_0$. Then

$$\bar{p}_e\left(n', 2^{n' R}\right) \leq \bar{p}_e\left(nn_0, 2^{(n+1)n_0 R}\right) \leq \bar{p}_e\left(nn_0, 2^{n(n_0 R')}\right) \to 0, \tag{5.35}$$

if R' is chosen such that $R(1 + 1/n) \leq R' < \sup_n \frac{1}{n} C_n$ for sufficiently large n. □

The quantity

$$C_1 = \max_{\pi, M} \mathcal{I}_1(\pi, M),$$

which we call the Shannon capacity of the c-q channel $x \to S_x$, is of special interest. Similar to the proof of Proposition 5.15, it can be shown to be equal to the capacity of the c-q channel $x \to S_x$, with the additional restriction that only product observables $\left\{M_{y_1}^1 \otimes \cdots \otimes M_{y_n}^n\right\}$ are allowed at the output of the composite channel. More generally, we call the decoding $M^{(n)} = \left\{M_j^{(n)}\right\}$ in $\mathcal{H}^{\otimes n}$ unentangled if

$$M_j^{(n)} = \sum_{y^n} p\left(j \mid y^n\right) M_{y_1}^1 \otimes \cdots \otimes M_{y_n}^n, \tag{5.36}$$

where $\left\{M_{y_k}^k\right\}$ is a quantum observable for the k th copy of the space $\mathcal{H}$, and $p\left(j \mid y^n\right)$ is a conditional probability describing the classical (stochastic) transformation of the measurement outcomes of a product observable

$$\left\{M_{y_1}^1 \otimes \cdots \otimes M_{y_n}^n\right\} \tag{5.37}$$

at the output.

Exercise 5.17 Denoting by C_{ud} the supremum of achievable rates for the codes (W, M), with the additional constraint (5.36) on the decoding M, show that $C_{ud} = C_1$. Hint: the effect of the decoding (5.36) can be described by concatenation of the classical composite channel corresponding to the product observable (5.37) and the channel $p(j \mid y^n)$. Use the data-processing inequality (4.20) and the analog of the first inequality in (5.32) to prove that $C_{ud} \leq C_1$. For the proof of the converse inequality, use the direct statement of the classical coding theorem for the channel $p_M(y \mid x) = \operatorname{Tr} S_x M_y$ to prove that any rate $R < \max_\pi \mathcal{I}_1(\pi, M)$ is achievable. Since the decoding M in $\mathcal{H}$ is arbitrary, it follows that any rate $R < C_1$ is achievable. Hence, $C_1 \leq C_{ud}$.

So far, we have shown that

$$C_1 \leq C \leq C_\chi.$$

The direct statement of the coding theorem, which will be proven below, implies $C = C_\chi$. The following result means that $C_1 < C$ for channels with essentially quantum output. Thus, for the memoryless c-q channels the capacity can be increased by using entangled decodings. It follows that, while $C_n = nC_1$ for a classical memoryless channel (see Proposition 4.9), in the quantum case strict superadditivity of the classical information $C_n > nC_1$ is possible, the reason being the existence of entangled observables at the output of the composite quantum channel. One can say that this is a dual manifestation of the EPR correlations. The latter arise when the state of a composite quantum system is entangled, while the measurements are local, i. e., unentangled. Here, the strict superadditivity of the information appears for the product states and entangled measurements.

Proposition 5.18. The equality $C_1 = C$ holds if and only if the operators $\pi_x^0 S_x$ commute for a probability distribution π^0 that maximizes $\chi(\pi)$.

Proof. The sufficiency of the condition is obvious. Conversely, let $C_1 = C$. In this case, by using Proposition 5.8, compactness of the set of probability distributions $\{\pi\}$, and continuity of the Shannon information $\mathcal{I}_1(\pi^1, M^1)$, we have $C_1 = \mathcal{I}_1(\pi^1, M^1)$ for some distribution π^1 and observable M^1. Hence, $\mathcal{I}_1(\pi^1, M^1) = \chi(\pi^0)$. It follows that $\chi(\pi^1) = \chi(\pi^0)$; otherwise, by using inequality (5.16), we would have

$$\mathcal{I}_1\left(\pi^1, M^1\right) \leq \chi\left(\pi^1\right) < \chi\left(\pi^0\right).$$

Thus, we can replace π^0 with $\pi^1, \mathcal{I}_1(\pi^1, M^1) = \chi(\pi^1)$, and necessity follows from the second statement of Theorem 5.9. □

The following examples (more detailed references and discussion are given in Section 5.8) illustrate the inequality $C_1 < C$.

Example 5.19. For the trine channel,

$$C_1 = 1 - h_2\left(\frac{1 + \sqrt{3}/2}{2}\right) \approx 0.645\text{bit}, \tag{5.38}$$

which is obtained for the nonuniform distribution $\pi = [1/2, 1/2, 0]$ and for the optimal measurement for the two equiprobable states ψ_0, ψ_1, see Sasaki et al. [199]. Thus, $C_1 < C$ and the sequence $\{C_n\}$ is strictly superadditive. Note that taking the uniform distribution $\pi = [1/3, 1/3, 1/3]$ and the information optimal observable results in the smaller quantity $\log(3/2) \approx 0.585$ bit.

Example 5.20. The Shannon capacity of the c − q channel with two pure states is given by

$$C_1 = \max_{\pi, M} \mathcal{I}(\pi, M) = 1 - h_2\left(\frac{1+\sqrt{1-\epsilon^2}}{2}\right), \tag{5.39}$$

where the maximum is achieved for the uniform distribution ($\pi_0 = \pi_1 = \frac{1}{2}$) and for the sharp observable M given by the orthonormal basis situated symmetrically with respect to the vectors $|\psi_0\rangle, |\psi_1\rangle$; see Levitin [162]. Here, $\epsilon = |\langle\psi_0 \mid \psi_1\rangle| = \cos\alpha$, where α is the angle between the vectors. Note that in this case the optimal observable is the same as the one obtained by the maximum likelihood criterion (Example 2.26), while C_1 is just the capacity (4.24) of the classical binary symmetric channel, with error probability

$$p = \sin^2(\pi/4 - \alpha/2) = \frac{1-\sin\alpha}{2}$$

The plot of the quantities C_1, C as functions of ϵ is given in Figure 5.1.

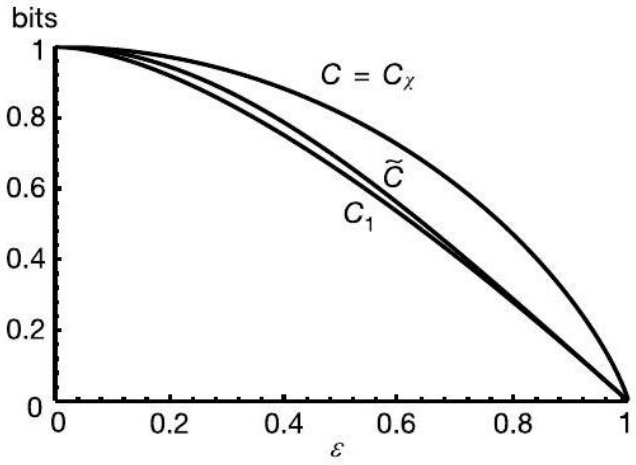


Figure 5.1: The capacity of the binary pure-state channel.

10.5.5 5.5 Typical Projectors

Before proving the direct statement of the coding theorem for the quantity C_χ, we shall consider the important notion of the typical subspace due to Schumacher and Jozsa [146].

Consider the tensor degree of a density operator

$$S^{\otimes n} = S \otimes \cdots \otimes S$$

in the space $\mathcal{H}^{\otimes n}$. Let

$$S = \sum_j \lambda_j |e_j\rangle \langle e_j|$$

be the spectral decomposition of the operator S, where $\{e_j\}$ is an orthonormal basis of eigenvectors and λ_j are the corresponding eigenvalues. Note that λ_j form a probability distribution with entropy

$$\sum_j \eta(\lambda_j) = H(S).$$

Then the spectral decomposition of the product state

$$S^{\otimes n} = S \otimes \cdots \otimes S$$

can be written as

$$S^{\otimes n} = \sum_J \lambda_J \left|e_J\right\rangle \left\langle e_J\right|,$$

where $J = (j_1, \ldots, j_n)$, with eigenvectors $|e_J\rangle = |e_{j_1}\rangle \otimes \cdots \otimes |e_{j_n}\rangle$ and eigenvalues $\lambda_J = \lambda_{j_1} \cdots \lambda_{j_n}$, describing a probability distribution of i.i.d. classical random variables. In accordance with Definition 4.2, the eigenvector $|e_j\rangle$ will be called δ-typical if

$$2^{-n(H(S)+\delta)} < \lambda_J < 2^{-n(H(S)-\delta)}$$

From the spectral decomposition of $S^{\otimes n}$ we can now construct the projector $P^{n,\delta}$ onto the typical subspace $\mathcal{H}^{n,\delta} = P^{n,\delta}\mathcal{H}^{\otimes n}$ by the relation

$$P^{n,\delta} = \sum_{J \in T^{n,\delta}} \left|e_J\right\rangle \left\langle e_J\right|.$$

We also call $P^{n,\delta}$ the typical projector.
The properties of the typical subspace $\mathcal{H}^{n,\delta}$ are analogous to the properties of the set $T^{n,\delta}$ of typical words (see Section 4.1) and easily follow from the latter.
i. The dimensionality $\dim \mathcal{H}^{n,\delta} = \operatorname{Tr} P^{n,\delta} = \left|T^{n,\delta}\right|$ satisfies the inequality

$$\dim \mathcal{H}^{n,\delta} \leq 2^{n(H(S)+\delta)}.$$

ii. The contribution of the non- δ-typical eigenvectors to the operator $S^{\otimes n}$ can be made arbitrarily small, i. e., for given $\delta, \varepsilon > 0$ and large enough n

$$\operatorname{Tr} S^{\otimes n} \left(I - P^{n,\delta}\right) < \varepsilon \tag{5.40}$$

To see this, we evaluate the trace in the basis of the eigenvectors of the operator $S^{\otimes n}$, and we find that it is equal to

$$\begin{aligned} \sum_{J \in \overline{T^{n,\delta}}} \lambda_J &= \mathrm{P}\left\{\left|-\frac{1}{n}\log \lambda_J - H(S)\right| \geq \delta\right\} \\ &= \mathrm{P}\left\{\left|-\frac{1}{n}\sum_{k=1}^{n} \log \lambda_{j_k} - H(S)\right| \geq \delta\right\}, \end{aligned} \tag{5.41}$$

where P corresponds to the probability distribution $\{\lambda_J\}$ and, by the law of large numbers, the last probability can be made arbitrarily small for n large.
iii. For sufficiently large n

$$(1-\varepsilon)2^{n(H(S)-\delta)} \leq \dim \mathcal{H}^{n,\delta}.$$

Now, we can formulate the noncommutative version of the asymptotic equipartition property: for large n the state $S^{\otimes n}$ approaches the chaotic state in the subspace $\mathcal{H}^{n,\delta}$ of dimensionality $\approx 2^{nH(S)}$.

An immediate application of this property is the quantum analog of data compression. As we have seen, the dimensionality of the underlying Hilbert space reflects the potential classical information resource of the quantum system. On the other hand, e. g., in quantum computation, the logarithm of the dimensionality measures the size of the memory, i.e., the

number of qubits in the register, which is the most important characteristic that one would like to minimize. Consider the problem of encoding quantum states into other states in a Hilbert space of the smallest possible dimensionality without essential loss of the "quantum information" carried by the states. To this end, we consider a quantum source that produces the pure states $S_x = |\psi_x\rangle \langle\psi_x|$ with probabilities p_x. The words $w = (x_1, \ldots, x_n)$ generate the product states $S_w = |\psi_w\rangle \langle\psi_w|$, where $|\psi_w\rangle = |\psi_{x_1}\rangle \otimes \cdots \otimes |\psi_{x_n}\rangle \in \mathcal{H}^{\otimes n}$, which are then encoded in some other states S'_w in a subspace $\mathcal{H}_d \subset \mathcal{H}^{\otimes n}$, the dimensionality of which $d = \dim \mathcal{H}_d$ should be as small as possible. The fidelity of the encoding is measured by the quantities $\langle\psi_w| S'_w |\psi_w\rangle$. The closer they are to 1 , the better the encoding. We require that the average fidelity

$$F_n = \sum_w \pi_w \langle\psi_w| S'_w |\psi_w\rangle$$

converges to 1 as $n \to \infty$.
Let

$$\bar{S}_\pi = \sum_{x=1}^{d} \pi_x |\psi_x\rangle \langle\psi_x|$$

be the average state of the source.
The following is called the quantum data compression theorem.

Theorem 5.21 (Schumacher and Jozsa [146]).
i. For all small enough $\varepsilon, \delta > 0$ there exist a Hilbert space $\mathcal{H}_d \subset \mathcal{H}^{\otimes n}$ of dimensionality $d = 2^{n\left(H\left(\bar{S}_\pi\right)+\delta\right)}$ and density operators S'_w in $\mathcal{H}_d$, such that the fidelity $F_n > 1 - \varepsilon$ for n large enough.
ii. For any choice of the subspace $\mathcal{H}_d \subset \mathcal{H}^{\otimes n}$ with $d = 2^{n\left(H\left(\bar{S}_\pi\right)-\delta\right)}$ and of the density operators S'_w in $\mathcal{H}_d$ we have $F_n < \varepsilon$ for n large enough.

Proof.
i. Consider the source state $|\psi_w\rangle = |\psi_{x_1}\rangle \otimes \cdots \otimes |\psi_{x_n}\rangle$. We now define the "compressed" state as

$$S'_w = \frac{P^{n,\delta} |\psi_w\rangle \langle\psi_w| P^{n,\delta}}{\langle\psi_w \mid P^{n,\delta}\psi_w\rangle}, \tag{5.42}$$

where $P^{n,\delta}$ is the typical projector of the state $\bar{S}_\pi^{\otimes n}$. The operator S'_w acts in the typical subspace $\mathcal{H}^{n,\delta}$, which has a dimensionality of at most $d = 2^{n\left(H\left(\bar{S}_\pi\right)+\delta\right)}$. For the average fidelity we obtain

$$\begin{aligned} F_n &= \sum_w \pi_w \langle\psi_w \mid S'_w \psi_w\rangle \\ &= \sum \pi_w \left\langle\psi_w \mid P^{n,\delta}\psi_w\right\rangle = \operatorname{Tr} \bar{S}_\pi^{\otimes n} P^{n,\delta} \end{aligned}$$

because $\bar{S}_\pi^{\otimes n} = \sum \pi_w |\psi_w\rangle \langle\psi_w|$. Due to the second property of $P^{n,\delta}$, we can bound this quantity from below by $1 - \varepsilon$.
ii. Taking into account the fact that the inequality $S'_w \leq P_d$ holds for all S'_w in $\mathcal{H}_d = P_d \mathcal{H}^{\otimes n}$, we have

$$\begin{aligned} F_n &= \sum \pi_w \langle\psi_w \mid S'_w \psi_w\rangle \leq \operatorname{Tr} \bar{S}_\pi^{\otimes n} P_d \\ &= \operatorname{Tr} \bar{S}_\pi^{\otimes n} P^{\frac{\delta}{2},n} P_d + \operatorname{Tr} \bar{S}_\pi^{\otimes n} \left(I - P^{\frac{\delta}{2},n}\right) P_d \\ &\leq \left\| \bar{S}_\pi^{\otimes n} P^{\frac{\delta}{2},n} \right\| \cdot \operatorname{Tr} P_d + \operatorname{Tr} \bar{S}_\pi^{\otimes n} \left(I - P^{\frac{\delta}{2},n}\right). \end{aligned}$$

Here we also used the following general property of the trace: if $T, X \geq 0, \operatorname{Tr} TX \leq \operatorname{Tr} T\|X\|$, which follows from (1.18). By the definition of typical eigenvectors, the corresponding eigenvalues are upper-bounded by

$$\left\|\bar{S}_{\pi}^{\otimes n} P^{n,\delta}\right\| < 2^{-n(H(S)-\delta)}. \tag{5.43}$$

By using this inequality and property ii of the typical projector, we obtain that for n large enough the quantity F_n does not exceed

$$2^{-n\left(H\left(\bar{S}_{\pi}\right)-\delta/2\right)} d + \varepsilon.$$

Thus, if we take $d = 2^{n\left(H\left(\bar{S}_{\pi}\right)-\delta\right)}$, then $F_n \leq 2^{-n\delta/2} + \varepsilon \leq 2\varepsilon$ for n large enough. $\square$

For the proof of the direct statement of the coding theorem in the next section, we will also need the notion of a conditionally typical projector. Consider the product states $S_w = S_{x_1} \otimes \cdots \otimes S_{x_n}$, where S_x is now an arbitrary (not necessarily pure) state and $w = (x_1, \ldots, x_n)$ is a word in the input alphabet. Denote by

$$\bar{H}_{\pi}\left(S_{(\cdot)}\right) = \sum_x \pi_x H\left(S_x\right)$$

the quantum analog of the conditional entropy of the output with respect to the input. Let $P_w = P_w^{n,\delta}$ be the spectral projector of S_w corresponding to the eigenvalues in the interval $\left(2^{-n\left[\bar{H}_{\pi}\left(S_{(\cdot)}\right)+\delta\right]}, 2^{-n\left[\bar{H}_{\pi}\left(S_{(\cdot)}\right)-\delta\right]}\right)$. In more detail, consider the spectral decomposition

$$S_x = \sum_j \lambda_j^x \left|e_j^x\right\rangle \left\langle e_j^x\right|.$$

Then the spectral decomposition of the operator S_w has the form

$$S_w = \sum_J \lambda_J^w \left|e_J^w\right\rangle \left\langle e_J^w\right|$$

where $\lambda_J^w = \lambda_{j_1}^{x_1} \cdots \lambda_{j_n}^{x_n}$ are the eigenvalues and $\left|e_J^w\right\rangle = \left|e_{j_1}^{x_1}\right\rangle \otimes \cdots \otimes \left|e_{j_n}^{x_n}\right\rangle$ are the corresponding eigenvectors. The conditionally typical projector is defined as

$$P_w = \sum_{J \in T_w^{n,\delta}} \left|e_J^w\right\rangle \left\langle e_J^w\right|$$

where

$$T_w^{n,\delta} = \left\{J : 2^{-n\left[\bar{H}_{\pi}\left(S_{(\cdot)}\right)+\delta\right]} < \lambda_J^w < 2^{-n\left[\bar{H}_{\pi}\left(S_{(\cdot)}\right)-\delta\right]}\right\}.$$

The essential properties of the projector P_w are:

i. from the definition,

$$P_w \leq S_w 2^{n\left[\bar{H}_{\pi}\left(S_{(\cdot)}\right)+\delta\right]} \tag{5.44}$$

ii. for $\varepsilon > 0$ and sufficiently large n

$$\mathrm{E} \operatorname{Tr} S_w \left(I - P_w\right) \leq \varepsilon \tag{5.45}$$

where E is the expectation corresponding to the probability distribution

$$\mathrm{P}\left\{w = (x_1, \ldots, x_n)\right\} = \pi_{x_1} \cdots \pi_{x_n}. \tag{5.46}$$

To prove the second property, consider the sequence of independent trials with outcomes $(x_l, j_l), l = 1, \ldots, n$, where the probability of an outcome (x, j) is, in each trial, equal to $\pi_x \lambda_j^x$. In this case,

$$\mathrm{E}\,\mathrm{Tr}\, S_w (I - P_w) = \mathrm{P}\left\{J \in \overline{T_w^{n,\delta}}\right\} \tag{5.47}$$

which tends to 0 as $n \to \infty$, according to the law of large numbers; see Exercise 4.15.

10.5.6 5.6 Proof of the Direct Coding Theorem

According to Definition 5.2, it is sufficient to show that the minimal average error probability $\bar{p}_e\left(n, 2^{nR}\right)$ tends to zero, as $n \to \infty$, provided $R < C_\chi$.

Consider the average state

$$\bar{S}_\pi = \sum_x \pi_x S_x$$

and the typical projector $P = P^{n,\delta}$ of the state $\bar{S}_\pi^{\otimes n}$, defined in the previous section. For a given codebook $W = \left\{w^{(1)}, \ldots, w^{(N)}\right\}$, we can also define the conditionally typical projectors $P_{w^{(}}, j = 1, \ldots, N$. We now introduce the special suboptimal observable M. The classical Shannon coding theorem, Theorem 4.13, corresponds to the case of diagonal density operators S_x with conditional probabilities $p(y \mid x)$ on the diagonal. The projector P is a quantum analog of the indicator of the subset of all δ-typical output words, while $P_{w^{(j)}}$ is the same for the subset of all conditionally typical words, given the input word $w^{(j)}$. However, in the quantum case these projectors need not commute, which makes a straightforward generalization of the decision domains (4.43) and the corresponding measure-theoretic argument impossible. Therefore, we introduce the following observable M in $\mathcal{H}^{\otimes n}$ by letting

$$M_j = \left(\sum_{l=1}^N P P_{w^{(l)}} P\right)^{-1/2} P P_{w^{(j)}} P \left(\sum_{l=1}^N P P_{w^{(l)}} P\right)^{-1/2}, \quad j = 1, \ldots, N. \tag{5.48}$$

The normalization with the square root is necessary, because the sum of the operators $P P_{w^{(j)}} P$ may not be equal to the unit operator, and the replacement of $P_{w^{(j)}}$ by $P P_{w^{(j)}} P$ plays the role of intersection with the set of all typical words in formula (4.44). The operator $\left(\sum_{l=1}^N P P_{w^l} P\right)^{-1/2}$ is to be understood as the generalized inverse of $\left(\sum_{l=1}^N P P_{w^l} P\right)^{1/2}$, equal to 0 on the null subspace of that operator, which contains the range of the projector $I - P$. Denoting by $\hat{P}$ the projector onto the support of $\sum_{l=1}^N P P_{w^l} P$, we have

$$P P_{w^{(l)}} P \le \hat{P} \le P, \quad l = 1, \ldots, N. \tag{5.49}$$

To avoid cumbersome notations, we shall further enumerate words by the variable w, omitting the indices j, l. By denoting

$$A_w = P_w P \left(\sum_{w'=1}^N P P_{w'} P\right)^{-1/2}$$

and using the Cauchy-Schwarz inequality (2.24),

$$\left|\mathrm{Tr}\, S_w A_w\right|^2 \le \mathrm{Tr}\, S_w A_w{}^* A_w,$$

we obtain

$$\bar{P}_e(W,M) \le \frac{1}{N}\sum_{w=1}^{N}\left[1-|\operatorname{Tr} S_w A_w|^2\right] \le \frac{2}{N}\sum_{w=1}^{N}\left[1-\operatorname{Tr} S_w A_w\right]$$

where $\operatorname{Tr} S_w A_w = \operatorname{Tr} P S_w P_w P \left(\sum_{w'=1}^{N} P P_{w'} P\right)^{-1/2}$ is a real number between 0 and 1 (note that $S_w P_w = P_w S_w \ge 0$). Applying the inequality

$$-2x^{-1/2} \le -3 + x, \quad x > 0, \tag{5.50}$$

we obtain by (5.49)

$$-2\left(\sum_{w'=1}^{N} P P_{w'} P\right)^{-1/2} \le -3\hat{P} + \sum_{w'=1}^{N} P P_{w'} P \le -3 P P_w P + \sum_{w'=1}^{N} P P_{w'} P.$$

Therefore, by using inequality (1.13),

$$\begin{aligned}\bar{P}_e(W,M) &\le \frac{1}{N}\sum_{w=1}^{N}\left[2\operatorname{Tr} S_w - 3\operatorname{Tr} S_w P_w P P_w P + \sum_{w'=1}^{N}\operatorname{Tr} S_w P_w P P_{w'} P\right] \\ &= \frac{1}{N}\sum_{w=1}^{N}\left[2\operatorname{Tr} S_w\left(I - P_w P P_w P\right) + \sum_{w':w'\ne w}\operatorname{Tr} S_w P_w P P_{w'} P\right]\end{aligned}$$

Taking into account that

$$\begin{aligned}\operatorname{Tr} S_w\left(I - P_w P P_w P\right) =& \operatorname{Tr} S_w\left(I - P_w\right) P P_w P + \operatorname{Tr} S_w (I-P) P_w \\ &- \operatorname{Tr} S_w (I-P) P_w (I-P) + \operatorname{Tr} S_w\left(I - P_w\right) P \\ &+ \operatorname{Tr} S_w (I-P) \\ \le& 2\left[\operatorname{Tr} S_w\left(I - P_w\right) + \operatorname{Tr} S_w (I-P)\right]\end{aligned}$$

where we used (1.13), we can write

$$\bar{P}_e(W,M) \le \frac{1}{N}\sum_{w=1}^{N}\left[4\operatorname{Tr} S_w (I-P) + 4\operatorname{Tr} S_w\left(I - P_w\right) + \sum_{w':w'\ne w}\operatorname{Tr} P S_w P P_{w'}\right] \tag{5.51}$$

which is our final basic estimate, similar to (4.45) in the classical case.
We now again apply Shannon's random coding scheme, assuming that the words $w^{(1)}, \dots, w^{(N)}$ are chosen at random, independently, and with the probability distribution (5.46) for each word, where π is the optimal distribution for which

$$H\left(\bar{S}_\pi\right) - \bar{H}_\pi\left(S_{(\cdot)}\right) = C_\chi.$$

Then

$$E S_w = \sum_{x_1 \cdots x_n} \pi_{x_1} \cdots \pi_{x_n} S_{x_1} \otimes \cdots \otimes S_{x_n} = \bar{S}_\pi^{\otimes n}$$

Taking the expectations in (5.51) and using the independence of random operators $S_w, P_{w'}$, we obtain

$$\begin{aligned}\mathrm{E}\bar{P}_e(W,M) \le& 4\operatorname{Tr}\bar{S}_\pi^{\otimes n}(I-P) + 4\mathrm{E}\operatorname{Tr} S_w\left(I - P_w\right) \\ &+ (N-1)\operatorname{Tr}\bar{S}_\pi^{\otimes n} P E P_{w'}.\end{aligned} \tag{5.52}$$

By inequalities (5.40), (5.45), expressing typicality of the projectors P, P_w, and by inequality (1.18) we have

$$E\bar{P}_e(W,M) \le 8\epsilon + (N-1)\left\|\bar{S}_\pi^{\otimes n}P\right\| \operatorname{Tr} EP_{w'},$$

for $n \ge n(\pi,\epsilon,\delta)$. By the property (5.43) of the projector P,

$$\left\|\bar{S}_\pi^{\otimes n}P\right\| \le 2^{-n\left[H\left(\bar{S}_\pi\right)-\delta\right]}$$

and by property i of the projector P_w,

$$\operatorname{Tr} \mathrm{E}P_{w'} = \mathrm{E}\operatorname{Tr} P_{w'} \le \mathrm{E}\operatorname{Tr} S_{w'} \cdot 2^{n\left[\bar{H}_\pi\left(S_{(\cdot)}\right)+\delta\right]} = 2^{n\left[\bar{H}_\pi\left(S_{(\cdot)}\right)+\delta\right]}$$

Recalling that $H\left(\bar{S}_\pi\right) - \bar{H}_\pi\left(S_{(\cdot)}\right) = C_\chi$, we obtain

$$\bar{p}_e(n,N) \le \mathrm{E}\bar{P}_e(W,M) \le 8\epsilon + N2^{-n[C_x-2\delta]}$$

Thus, if $R \le C_\chi - 3\delta$,

$$\bar{p}_e\left(n,2^{nR}\right) \le 8\epsilon + 2^{-n\delta}$$

hence, the direct coding theorem follows.

A slight modification of this argument shows exponential decay of the average error probability. Namely, there exists a $\beta > 0$, such that

$$\mathrm{E}\bar{P}_e(W,M) \le 2^{-n\beta} \tag{5.53}$$

Indeed, we already have such an estimate for the last term in (5.52), provided $N \le 2^{n[C_x-3\delta]}$, so we have to establish it for the first two terms. But this follows by application of inequality (4.11) to the probabilities of large deviations (5.41), (5.47) (Exercise).

10.5.7 5.7 The Reliability Function for Pure-State Channel

In the classical case, pure signal states correspond to degenerate distributions, and the coding theorem trivially implies the maximal value of the channel capacity $\log|\mathcal{X}|$. However, for pure quantum nonorthogonal states, the coding theorem remains nontrivial, although the situation is simplified, allowing us to obtain a stronger result. Here, we give a different proof of the direct statement of the coding theorem in the case of pure states $S_x = |\psi_x\rangle\langle\psi_x|$, which does not use the notion of typicality but, due to a more sophisticated analysis, gives the estimate for the exponential speed of decay of the error probability.

Theorem 5.22 (Burnashev and Holevo [37]). For $R < C_\chi$, the following inequality holds:

$$\bar{p}_e\left(n,2^{nR}\right) \le 2\cdot 2^{-nE(R)},$$

where

$$E(R) = \max_{0\le r\le 1}\left[-Rr + \max_\pi\left(-\log\operatorname{Tr}\bar{S}_\pi^{1+r}\right)\right] > 0. \tag{5.54}$$

The function $E(R)$ gives a lower bound for the so-called reliability function of the channel, characterizing the exponential speed of decay of the error probability $\bar{p}_e\left(n,2^{nR}\right)$ as $n\to\infty$.

Proof. Consider the subspace of the space $\mathcal{H}^{\otimes n}$, spanned by the code vectors $\psi_{w^{(1)}},\ldots,$ $\psi_{w^{(N)}}$. As shown in Section 2.3.4, we can use the Gram operator $G = \sum_j |\psi_{w^{(j)}}\rangle\langle\psi_{w^{(j)}}|$ to construct the overcomplete system

$$\left|\hat{\psi}_j\right\rangle = G^{-\frac{1}{2}}\left|\psi_{w^{(j)}}\right\rangle, \quad j=1,\ldots,N,$$

and hence the observable M with the components

$$M_j = \left|\hat{\psi}_j\right\rangle \left\langle\hat{\psi}_j\right|, \quad j = 1, \ldots, N, \tag{5.55}$$

which can be extended to the whole space $\mathcal{H}^{\otimes n}$ by adjoining the projector M_0 onto the orthogonal complement to $\psi_{w^{(1)}}, \ldots, \psi_{w^{(N)}}$. This will be our suboptimal decoding for the composite channel. Note that it differs from (5.48), in that it does not contain the typical projector P (while the conditionally typical projectors in the case of pure states are $P_w = |\psi_w\rangle \langle\psi_w|$). In this way, we obtain the upper bound for the average error probability expressed via the Gram operator of the code vectors, i.e.,

$$\begin{aligned}
\bar{P}_e(W, M) &= \frac{1}{N} \sum_{j=1}^{N} \left(1 - \left\langle\hat{\psi}_j\right| G^{\frac{1}{2}} \left|\hat{\psi}_j\right\rangle^2\right) \\
&\leq \frac{2}{N} \sum_{j=1}^{N} \left(1 - \left\langle\hat{\psi}_j\right| G^{\frac{1}{2}} \left|\hat{\psi}_j\right\rangle\right) \\
&= \frac{2}{N} \left(N - \operatorname{Tr} G^{\frac{1}{2}}\right)
\end{aligned} \tag{5.56}$$

Assuming that the codewords $\left\{w^{(j)}\right\}$ are randomly chosen, independently of each other, with the distribution (5.46), we obtain

$$\mathrm{E}\bar{P}_e(W, M) \leq \frac{2}{N} \left(N - \mathrm{E} \operatorname{Tr} G^{\frac{1}{2}}\right). \tag{5.57}$$

By using the inequality

$$-2x^{\frac{1}{2}} \leq x^2 - 3x, \quad x \geq 0,$$

which follows from (5.50), in combination with the obvious one $-2x^{\frac{1}{2}} \leq 0$, we have

$$-2G^{\frac{1}{2}} \leq \begin{cases} G^2 - 3G, \\ 0. \end{cases} \tag{5.58}$$

The expectation of the Gram operator is equal to

$$\begin{aligned}
\mathrm{E}G &= \mathrm{E} \sum_{j=1}^{N} |\psi_{w^{(j)}}\rangle \langle\psi_{w^{(j)}}| = N\mathrm{E} |\psi_{w^{(j)}}\rangle \langle\psi_{w^{(j)}}| \\
&= N \sum_{x_1 \ldots x_n} \pi_{x_1} \ldots \pi_{x_n} \left(|\psi_{x_1}\rangle \otimes \cdots \otimes |\psi_{x_n}\rangle\right) \left(\langle\psi_{x_1}| \otimes \cdots \otimes \langle\psi_{x_n}|\right) \\
&= N \left[\sum_x \pi_x |\psi_x\rangle \langle\psi_x|\right]^{\otimes n} = N \bar{S}_\pi^{\otimes n}
\end{aligned} \tag{5.59}$$

Similarly

$$\begin{aligned}\mathrm{E}\left(G^2-G\right)=&\mathrm{E}\left(\sum_{j,k=1}^{N}|\psi_{w^{(j)}}\rangle\langle\psi_{w^{(j)}}\mid\psi_{w^{(k)}}\rangle\langle\psi_{w^{(k)}}|\right.\\&\left.-\sum_{j=1}^{N}|\psi_{w^{(j)}}\rangle\langle\psi_{w^{(j)}}|\right)\\=&\mathrm{E}\left(\sum_{j\neq k}|\psi_{w^{(j)}}\rangle\langle\psi_{w^{(j)}}\mid\psi_{w^{(k)}}\rangle\langle\psi_{w^{(k)}}|\right)\\=&N(N-1)\left(\bar{S}_{\pi}^{\otimes n}\right)^2,\end{aligned}\tag{5.60}$$

so that in combination with (5.58) we obtain

$$-2\mathrm{E}G^{\frac{1}{2}}\leq\begin{cases}N(N-1)\left(\bar{S}_{\pi}^{\otimes n}\right)^2-2N\bar{S}_{\pi}^{\otimes n}\\0\end{cases}\tag{5.61}$$

Let $\{|e_J\rangle\}$ be the orthonormal basis of eigenvectors and $\{\lambda_J\}$ the corresponding eigenvalues of the operator $\bar{S}_{\pi}^{\otimes n}$. Then

$$-2\langle e_J|\,\mathrm{E}G^{\frac{1}{2}}\,|e_J\rangle\leq\begin{cases}N(N-1)\lambda_J^2-2N\lambda_J,\\0,\end{cases}\tag{5.62}$$

hence, using the inequalities $\min(a,b)\leq a^r b^{1-r}$ and $2^{1-r}\leq 2$ for $0\leq r\leq 1$, we obtain

$$N\lambda_J\min\left[(N-1)\lambda_J,2\right]-2N\lambda_J\leq 2N(N-1)^r\lambda_J^{1+r}-2N\lambda_J,\tag{5.63}$$

whence

$$-2\mathrm{E}\,\mathrm{Tr}\,G^{\frac{1}{2}}\leq-2N+2N(N-1)^r\,\mathrm{Tr}\left(\bar{S}_{\pi}^{\otimes n}\right)^{1+r}.$$

Coming back to (5.57), we can evaluate the average error probability minimized over all codes as

$$\bar{p}_e(n,N)\leq 2N^r\left(\mathrm{Tr}\,\bar{S}_{\pi}^{1+r}\right)^n$$

for any $0\leq r\leq 1$. Putting $N=2^{nR}$, we obtain

$$\bar{p}_e\left(n,2^{nR}\right)\leq 2\cdot 2^{n\left(Rr+\log\mathrm{Tr}\,\bar{S}_{\pi}^{1+r}\right)}\tag{5.64}$$

Now, we can use the freedom in the choice of the parameters r and π. Note that $-\log\mathrm{Tr}\,\bar{S}_{\pi}^{1+r}$ is a concave function of r, which can be established by showing that the second derivative is negative (Exercise). Also,

$$\frac{d}{dr}\left(-\log\mathrm{Tr}\,\bar{S}_{\pi}^{1+r}\right)\Big|_{r=0}=-\,\mathrm{Tr}\,\bar{S}_{\pi}\log\bar{S}_{\pi}=H\left(\bar{S}_{\pi}\right)\tag{5.65}$$

Take for π the optimal distribution, for which $H\left(\bar{S}_{\pi}\right)=C_{\chi}$. Then, for $R<C_{\chi}$ we have $\bar{p}_e\left(n,2^{nR}\right)\leq 2\cdot 2^{-nE(R)}$, where $E(R)$ is given by expression (5.54).

10.5.8 5.8 Notes and References

1. The issue of the information capacity of quantum communication channels arose in the 1960s in the papers of Gordon [85], [86], Forney [72], Lebedev and Levitin [160], and Stratonovich [227] and goes back to even earlier, classical works of Gabor and Brillouin, that ask for fundamental physical limits on the rate and quality of information transmission (for detailed reference, see the surveys [43], [114] and the books [103], [122]). These works laid a physical foundation and raised the question of consistent quantum information treatment of the problem.

2. The proof of Theorem 5.9, including the criterion for the equality, based on comparison of the convexity of the quantities in (5.16), was given in [111]. The symmetric logarithmic derivative of a family of quantum states and the corresponding quantum Fisher information were introduced by Helstrom in the context of quantum estimation theory [103]. The information inequality (5.16) has a number of applications: from evaluation of eavesdropper information in quantum cryptography to entropic Heisenberg limits and uncertainty relations (Hall [90]).

3. A detailed comparison of the capacities C_1, C_χ for different channels was made in the paper of Hirota et al. [148].

The strong converse

$$\lim_{n\to\infty} \bar{p}_e\left(n, 2^{nR}\right) = 1 \quad \text{for } R \geq C_\chi$$

was obtained by Winter [253] and Ogawa and Nagaoka [181]; see also the book [95]. Exact strong converse exponent was obtained by Mosonyi and Ogawa [177]. It is expressed in terms of "sandwiched" Rényi divergence (Wilde, Winter and Yang [251]).

Formula (5.39) follows from the work of Levitin [162], who showed that for two pure states and arbitrary π the maximum $\max_M \mathcal{I}(\pi, M)$ over the two-valued sharp observables in the plane is attained by the observable that maximizes the average probability of correct decision, and from the work of Shor [217], who proved that the twovalued sharp observables are sufficient in this case, and the maximum $\max_M \mathcal{I}(\pi, M)$ is a concave symmetric function of π, implying that the optimal distribution is uniform.

The trine channel was introduced by Holevo [110], who proved that for the uniform distribution π, the maximum $\max_M \mathcal{I}(\pi, M)$ over all observables is strictly greater than the maximum over sharp observables ($\log\left(\sqrt{3}/\sqrt[3]{2}\right) \approx 0.459$). It is interesting that the information-optimal observable in this problem differs from the maximal likelihood observable (see Section 2.4.2) by rotation by the angle $\pi/2$, the latter being the least informative observable. A complete treatment of $\max_M \mathcal{I}(\pi, M)$ for an arbitrary symmetric family of pure states in two-dimensional Hilbert space was given by Sasaki, Barnett, Jozsa, Osaki, and Hirota [199], who also discussed experimental implementation of the optimal measuring procedures. Conjecture (5.38) was confirmed numerically in [147], and an additional argument was given in [217]. A remarkable study of the "lifted trine" channel, i. e., the channel with three linearly independent, equiangular state vectors in three-dimensional Hilbert space, was given by Shor [217]. It was shown, in particular, that the information-optimal observable in this case has in general 6 outcomes, i. e., the maximal value admitted by Proposition 5.8 in the case $d = 3$ (although the gain, as compared to 3 outcomes, is tiny).

4. The idea of quantum data compression, originally due to Schumacher, is one of the central ones in quantum information theory. Theorem 5.21 is proved by Jozsa and Schumacher [146]. For a survey of more recent results, from different authors, on the much more complicated problem of data compression for sources with mixed states, see the book of Hayashi [95], papers of

Winter [254] and Wilde et al. [249]. The topic of reverse Shannon theorem, both for classical and quantum channels was elaborated in the work of Bennett et al. [23].
5. The proof of the coding theorem for a general c − q channel was given by Holevo [113] and by Schumacher and Westmoreland [200]. See Winter [253] for a different proof in the spirit of Cziszar and Körner's approach [50] to the classical coding theorem. This was preceded by the consideration of the pure-state channel in the work of Hausladen, Josza, Schumacher, Westmoreland, and Wootters [94], who used the technique of typical subspaces discussed in Section 5.5. It should be noted that Shannon's method of random coding for the channel with pure, almost orthogonal states was first applied by Stratonovich and Vancian [229], who used the first term in the minimal error probability in the asymptotics $\varepsilon \to 1$ (almost orthogonal states) to conclude that this method allows us to obtain the so-called cut-off rate

$$\tilde{C} = -\log \min_{\pi} \operatorname{Tr} \bar{\rho}_{\pi}^{2} < C. \tag{5.66}$$

As shown by Burnashev and Holevo [37], the properly used method of random coding allows us to obtain not only the classical capacity C, but also the exponential estimate for the error probability, in the spirit of the classical results in Gallager [78]. Dalai [51], [52] was able to extend the classical sphere packing bound of Fano, Shannon, Gallager, and Berlecamp to the pure-state c-q channel, to obtain the upper bound on the reliability function, which coincides, at high rates, with the lower bound $E(R)$ of [37]. The paper [37] also contains a formulation of the hypothesis concerning the reliability function for an arbitrary mixed-state channel. In this case, like in the others, a mixed-state problem is much more complex than its pure-state analog. Among further variations and refinements of the coding theorem we mention here nonasymptotic approach of Wang and Renner [239] and second order asymptotic results by Tomamichel and Tan [231].

10.6 6 Quantum Evolutions and Channels

10.6.1 6.1 Quantum Evolutions

In this section, the notion of quantum communication channel will be considered from a general point of view. As we have seen in Chapter 4, a classical communication channel is completely characterized by the transition probability matrix

$$\mathcal{X} \xrightarrow{p(y|x)} \mathcal{Y}.$$

Such a channel describes an affine transformation $p_x \to p'_y = \sum_x p(y \mid x) p_x$ of classical states (probability distributions) $p = \{p_x\}$ on the input alphabet $\mathcal{X}$, into the classical states $p' = \{p'_y\}$ on the output alphabet $\mathcal{Y}$.

To have a proper quantum analog of a channel we will therefore first look for maps taking density operators into density operators, which respect convex combinations, i. e., affine maps $\Phi : \mathfrak{S}(\mathcal{H}) \to \mathfrak{S}(\mathcal{H})$,

$$\Phi\left[\sum_j p_j S_j\right] = \sum_j p_j \Phi\left[S_j\right], \quad p_j \geq 0, \quad \sum_j p_j = 1, \quad S_j \in \mathfrak{S}(\mathcal{H}).$$

Exercise 6.1 Prove the following statement: an affine map Φ of $\mathfrak{S}(\mathcal{H})$ into itself can be uniquely extended to a map of the linear space $\mathfrak{T}(\mathcal{H})$ with the following properties:
i. Φ is linear: $\Phi\left[\sum_j c_j S_j\right] = \sum_j c_j \Phi\left[S_j\right], c_j \in \mathbb{C}, S_j \in \mathfrak{T}(\mathcal{H})$;
ii. Φ is positive: $S \in \mathfrak{T}(\mathcal{H}), S \geq 0 \Rightarrow \Phi[S] \geq 0$;
iii. Φ is trace-preserving: $\operatorname{Tr} \Phi[S] = \operatorname{Tr} S, S \in \mathfrak{T}(\mathcal{H})$.

Hint: follow the proof of Theorem 2.6 to obtain the linear extension of Φ to $\mathfrak{T}(\mathcal{H})$. Properties ii, iii then are straightforward.

Definition 6.2. For every map $\Phi : \mathfrak{T}(\mathcal{H}) \to \mathfrak{T}(\mathcal{H})$, satisfying properties i-iii, the dual map $\Phi^* : \mathfrak{B}(\mathcal{H}) \to \mathfrak{B}(\mathcal{H})$ is defined by the formula

$$\operatorname{Tr} \Phi[S]X = \operatorname{Tr} S\Phi^*[X], \quad S \in \mathfrak{T}(\mathcal{H}), X \in \mathfrak{B}(\mathcal{H}). \tag{6.1}$$

Exercise 6.3 Prove the following statement: the properties of the map Φ from Exercise 6.1 are equivalent to the following:

i. Φ^* is linear;

ii. Φ^* is positive: $X \geq 0 \Rightarrow \Phi^*[X] \geq 0$;

iii. Φ^* is unital: $\Phi^*[I] = I$.

The map Φ describes an evolution of the quantum system in terms of states (the Schrödinger picture), while the map Φ^* does this in terms of observables (the Heisenberg picture). Note that positive linear maps transform Hermitian operators into Hermitian operators. In the case of a finite-dimensional $\mathcal{H}$ that we are considering, the linear space $\mathfrak{T}(\mathcal{H})$ and the algebra $\mathfrak{B}(\mathcal{H})$ coincide with the space of all linear operators in $\mathcal{H}$, but we use different notations to stress that $\mathfrak{T}(\mathcal{H})$ is the arena for the states and the Schrödinger picture, while $\mathfrak{B}(\mathcal{H})$ is that of the observables and the Heisenberg picture. This distinction becomes quite substantial in the infinite-dimensional case considered in Chapters 11, 12.

Example 6.4. Let U be a unitary operator. In this case, $\Phi[S] = USU^*$ is an affine, one-to-one mapping of the set of quantum states $\mathfrak{S}(\mathcal{H})$ onto itself (i.e., affine bijection), describing reversible evolution in the Schrödinger picture. In the Heisenberg picture $\Phi^*[X] = U^*XU$.

The following result, going back to the famous Wigner theorem, characterizes all reversible evolutions.

Theorem 6.5. Let Φ be an affine bijection of the convex set $\mathfrak{S}(\mathcal{H})$. Then

$$\Phi[S] = USU^*, \quad \text{or} \quad \Phi[S] = US^\top U^*, \tag{6.2}$$

where U is a unitary operator and $S^\top$ is the matrix transposition in some basis. Equivalently, $\Phi[S] = USU^*$, where U is a unitary or antiunitary operator.

An antiunitary operator U is characterized by the following properties:

i. $\|U\psi\| = \|\psi\|, \psi \in \mathcal{H}$;

ii. $U\left(\sum c_j\psi_j\right) = \sum \bar{c}_j U\psi_j$.

Such an operator can always be represented in the form $U = \tilde{U}\Lambda$, where $\tilde{U}$ is a unitary operator and $\Lambda = \Lambda^*$ is the antiunitary operator of the complex conjugation, in a fixed basis. The corresponding evolution of states is given by the matrix transposition in this basis

$$S^\top = \Lambda S \Lambda^*.$$

In physics, transposition and complex conjugation are associated with time inversion.

Proof. We rely on the case of the qubit ($\dim \mathcal{H} = 2$), for which the proof will be given in Section 6.8. Let ψ_1, ψ_2 be some linearly independent vectors in $\mathcal{H}$. Since an affine bijection of a convex set maps extreme points into extreme points, we have

$$\Phi\left[|\psi_j\rangle\langle\psi_j|\right] = |\phi_j\rangle\langle\phi_j|, \quad j = 1, 2. \tag{6.3}$$

Denote by $\mathcal{H}_2$ the two-dimensional subspace generated by ψ_1, ψ_2. Then for any $|\psi\rangle \in \mathcal{H}_2$ we have

$$|\psi\rangle\langle\psi| \leq c\left(|\psi_1\rangle\langle\psi_1| + |\psi_2\rangle\langle\psi_2|\right).$$

On the other hand, similar to (6.3),

$$\Phi[|\psi\rangle\langle\psi|] = |\phi\rangle\langle\phi|.$$

Because of the positivity of Φ

$$|\phi\rangle\langle\phi| \leq c\left(|\phi_1\rangle\langle\phi_1| + |\phi_2\rangle\langle\phi_2|\right),$$

i. e., $|\phi\rangle$ belongs to a two-dimensional subspace that contains the vectors ϕ_1, ϕ_2. By an additional unitary transformation, we can make this subspace coincide with $\mathcal{H}_2$. Hence, we can apply the aforementioned result for the qubit to the restriction of Φ onto the subset of states supported by the two-dimensional subspace $\mathcal{H}_2 \subset \mathcal{H}$ to conclude that this restriction is given by formula (6.2), where U may, however, depend on that subspace.

The proof in the general case is obtained by performing appropriate transformations of the subspace $\mathcal{H}_2$ to show that this dependence reduces to an inessential phase factor. Let $\{e_j; j = 1, \ldots, d\}$ be an orthonormal basis in $\mathcal{H}$. Then

$$\Phi\left[|e_j\rangle\langle e_j|\right] = |h_j\rangle\langle h_j|.$$

By applying the aforementioned result for $\mathcal{H}_2$ generated by the vectors e_j, e_k, we obtain that $\{h_j\}$ is an orthonormal basis. Moreover,

$$\Phi\left[|e_j\rangle\langle e_k|\right] = z_{jk}|h_j\rangle\langle h_k| \quad \text{or} \quad z_{kj}|h_k\rangle\langle h_j|, \tag{6.4}$$

where $|z_{jk}| = 1$. If $\Phi\left[|e_1\rangle\langle e_2|\right] = z_{12}|h_1\rangle\langle h_2|$ but $\Phi\left[|e_1\rangle\langle e_3|\right] = z_{31}|h_3\rangle\langle h_1|$, then

$$\Phi\left[|e_1\rangle\langle e_2 + e_3|\right] = z_{12}|h_1\rangle\langle h_2| + z_{31}|h_3\rangle\langle h_1|$$

is an operator of rank two, which contradicts (6.4). Repeating this argument, we obtain that in relation (6.4) one and the same alternative takes place for all j, k.

Consider the first alternative, when

$$\Phi\left[|e_j\rangle\langle e_k|\right] = z_{jk}|h_j\rangle\langle h_k|.$$

Now, putting $\psi = e_1 + \cdots + e_d$, we obtain that the operator

$$\Phi[|\psi\rangle\langle\psi|] = \sum_{j,k=1}^{d} z_{jk}|h_j\rangle\langle h_k|$$

has rank one, hence $z_{jk} = a_j\bar{a}_k$, where $|a_j| = 1$ for all j. Denoting by U the unitary operator for which $U|e_j\rangle = a_j|h_j\rangle$, we obtain $\Phi[S] = USU^*$. Similarly, in the case of the second alternative we obtain $\Phi[S] = US^\top U^*$, where $^\top$ is a transposition in the basis $\{e_j\}$. □

10.6.2 6.2 Completely Positive Maps

Generalizing the previous considerations, we shall consider a linear map Φ, acting from $\mathfrak{T}(\mathcal{H}_A)$ to $\mathfrak{T}(\mathcal{H}_B)$, where $\mathcal{H}_A, \mathcal{H}_B$ are, in general, different spaces. In this case, the dual map Φ^* acts from $\mathfrak{B}(\mathcal{H}_B)$ to $\mathfrak{B}(\mathcal{H}_A)$.

Definition 6.6. The map $\Phi^*(\Phi)$ is called completely positive (CP) if one of the two equivalent conditions holds:

i. $\Phi^* \otimes \mathrm{Id}_n$ is positive for all $n = 1, 2, \ldots$, where Id_n denotes the identity map of the algebra of all $n \times n$-matrices $\mathfrak{B}(\mathbb{C}^n)$;

ii. for arbitrary finite sets of vectors $\{\varphi_j\} \subset \mathcal{H}_B, \{\psi_j\} \subset \mathcal{H}_A$ the following inequality holds:

$$\sum_{j,k} \langle\varphi_j \mid \Phi\left[|\psi_j\rangle\langle\psi_k|\right]\varphi_k\rangle \geq 0.$$

To see the equivalence of the above conditions, let us introduce the spaces $\mathcal{H}_i^{(n)}$, which are direct orthogonal sums of n copies of $\mathcal{H}_i, i = A, B$, where n is the size of given sets of vectors $\{\varphi_j\}, \{\psi_j\}$. As we have seen in Section 3.1.1, $\mathcal{H}_i^{(n)}$ can be identified with $\mathcal{H}_i \otimes \mathbb{C}^n$. In this case, denoting

$$\varphi^{(n)} = \sum_{j=1}^{n} \oplus \varphi_j, \quad \psi^{(n)} = \sum_{j=1}^{n} \oplus \psi_j$$

we have

$$\sum_{j,k} \langle \varphi_j \mid \Phi\left[|\psi_j\rangle \langle \psi_k|\right] \varphi_k \rangle = \left\langle \psi^{(n)} \right| \left(\Phi^* \otimes \mathrm{Id}_n\right) \left[\left|\varphi^{(n)}\right\rangle \left\langle \varphi^{(n)}\right|\right] \left|\psi^{(n)}\right\rangle,$$

from which the implication i $\Rightarrow$ ii follows. Conversely, any positive operator $X^{(n)}$ in $\mathcal{H}_B^{(n)} \simeq \mathcal{H}_B \otimes \mathbb{C}^n$ can be represented as a sum of positive rank one operators of the form $\left|\varphi^{(n)}\right\rangle \left\langle \varphi^{(n)}\right|$. Hence, condition ii, which means positivity of $\Phi^* \otimes \mathrm{Id}_n$ on such operators, implies i.

Exercise 6.7 Prove the following statement: if the map Φ^* satisfies condition i for $n = 2$, the Kadison inequality holds,

$$\Phi^*[X]^* \Phi^*[X] \leq \|\Phi^*[I]\| \, \Phi^*\left[X^* X\right] \tag{6.5}$$

for arbitrary operator X.

Exercise 6.8 Show that for the transposition map $S \to S^\top$ in some basis, condition i already breaks for $n = 2$. Hint: consider condition ii where $\{\psi_j\}$ is the orthonormal basis in which the transposition is made.

The notion of complete positivity was introduced by Stinespring [226], who proved an important result, generalizing Naimark's theorem. We shall give the proof of Stinespring's dilation theorem in the special finite-dimensional case.

Theorem 6.9. For every completely positive map $\Phi^* : \mathfrak{B}(\mathcal{H}_B) \to \mathfrak{B}(\mathcal{H}_A)$ there exist a Hilbert space $\mathcal{H}_E$ and an operator $V : \mathcal{H}_A \to \mathcal{H}_B \otimes \mathcal{H}_E$ such that

$$\Phi^*[X] = V^* (X \otimes I_E) V, \quad X \in \mathfrak{B}(\mathcal{H}_B). \tag{6.6}$$

Dually,

$$\Phi[S] = \mathrm{Tr}_E \, V S V^*, \quad S \in \mathfrak{T}(\mathcal{H}_A).$$

The map Φ^* is unital, i.e., $\Phi^*[I_B] = I_A$ (the map Φ preserves the trace) if and only if the operator V is isometric.

In relation (6.7) and in what follows we use the abbreviated notation for the partial trace: $\mathrm{Tr}_E = \mathrm{Tr}_{\mathcal{H}_E}$, etc.

Proof. Consider the algebraic tensor product $\mathcal{L} = \mathcal{H}_A \otimes \mathfrak{B}(\mathcal{H}_B)$, generated by the elements $\Psi = \psi \otimes X, \psi \in \mathcal{H}_A, X \in \mathfrak{B}(\mathcal{H}_B)$. Let us introduce a pre-inner product in $\mathcal{L}$ with the corresponding square of the norm

$$\left\| \sum_j \psi_j \otimes X_j \right\|^2 = \sum_{j,k} \langle \psi_j | \, \Phi^*\left[X_j^* X_k\right] |\psi_k\rangle$$

This quantity is nonnegative because the block operator $X^{(n)} = \left[X_j^* X_k\right]_{j,k=\overline{1,n}}$ in $\mathcal{H}_B^{(n)}$ is positive and the map Φ is CP . Taking the quotient with respect to the subspace $\mathcal{L}_0$ of zero norm, we obtain the Hilbert space $\mathcal{K} = \mathcal{L}/\mathcal{L}_0$. Define V and π by the relations $V\psi = \psi \otimes I$ and $\pi[Y]\Psi = \pi[Y](\psi \otimes X) = \psi \otimes YX$. It is easy to check that these definitions agree with

taking the quotient. Then π is a *-homomorphism of the algebra $\mathfrak{B}(\mathcal{H}_B)$ into $\mathfrak{B}(\mathcal{K})$, i. e., a linear map that preserves the algebraic operations and the involution, i.e.,

$$\pi[XY] = \pi[X]\pi[Y], \pi[X^*] = \pi[X]^*.$$

The map π is unital. Moreover,

$$\langle\varphi|\Phi^*[X]|\psi\rangle = \langle\varphi\otimes I \mid \psi\otimes X\rangle = \langle\varphi|V^*\pi[X]V|\psi\rangle, \quad X\in\mathfrak{B}(\mathcal{H}_B),$$

that is,

$$\Phi^*[X] = V^*\pi[X]V. \tag{6.8}$$

However, by Lemma 6.10 proved below any *-homomorphism of the algebra $\mathfrak{B}(\mathcal{H}_B)$ is unitary equivalent to the ampliation $\pi[X] = X\otimes I_E$, where I_E is the unit
operator in a Hilbert space $\mathcal{H}_E$, i. e., we can take $\mathcal{K} = \mathcal{H}_B\otimes\mathcal{H}_E$, and the Stinespring representation (6.8) takes the form (6.6).

The dual representation (6.7) follows from (6.6) and from the definition of the dual map (6.1). □

In this construction, the dimensionality of the space $\mathcal{H}_E$ satisfies

$$\dim\mathcal{H}_E \le d_A d_B, \tag{6.9}$$

where $d_A = \dim\mathcal{H}_A, d_B = \dim\mathcal{H}_B$. Indeed, $\dim\mathcal{H}_E = \dim\mathcal{K}/d_B \le \dim\mathcal{L}/d_B$ and $\dim\mathcal{L} = d_A d_B^2$. However, there is no a priori restriction and any map of the form (6.6) is completely positive as concatenation of ampliation $X\to X\otimes I$ and conjugation $X\to V^*XV$, the complete positivity of which follows from Definition 6.6.

Lemma 6.10. Let π be a unital *-homomorphism of the algebra $\mathfrak{B}(\mathcal{H})$ into the algebra $\mathfrak{B}(\mathcal{K})$. Then there exist a Hilbert space $\mathcal{H}_E$ and an isometric map U of the space $\mathcal{K}$ onto $\mathcal{H}\otimes\mathcal{H}_E$ such that

$$\pi[X] = U^*(X\otimes I_E)U, \quad X\in\mathfrak{B}(\mathcal{H}). \tag{6.10}$$

Proof. Choose an orthonormal basis $\{e_j; j = 1,\dots,d\}$ in $\mathcal{H}$, and consider the matrix units $|e_j\rangle\langle e_k|$ and their images

$$V_{jk} = \pi[|e_j\rangle\langle e_k|]\in\mathfrak{B}(\mathcal{K}).$$

Since π is *-homomorphism, the operators V_{jk} satisfy the same algebraic relations as the matrix units

$$V_{jk}V_{lm} = \delta_{kl}V_{jm}, \quad V_{jk}^* = V_{kj}. \tag{6.11}$$

Consider the subspace $\mathcal{H}_E = V_{11}\mathcal{K}\subseteq\mathcal{K}$ and define $U:\mathcal{K}\to\mathcal{H}\otimes\mathcal{H}_E$ by the relation

$$U\psi = \sum_j |e_j\rangle\otimes V_{1j}\psi$$

(note that $V_{1j}\psi = V_{11}V_{1j}\psi\in\mathcal{H}_E$). Then

$$\langle U\psi_1 \mid (X\otimes I_E)U\psi_2\rangle = \sum_{j,k}\langle e_j \mid Xe_k\rangle\langle V_{1j}\psi_1 \mid V_{1k}\psi_2\rangle. \tag{6.12}$$

By (6.11)

$$\langle V_{1j}\psi_1 \mid V_{1k}\psi_2\rangle = \langle\psi_1 \mid V_{jk}\psi_2\rangle = \langle\psi_1 \mid \pi[|e_j\rangle\langle e_k|]\psi_2\rangle.$$

Therefore, the right-hand side of (6.12) is equal to

$$\sum_{j,k} \langle e_j \mid Xe_k \rangle \langle \psi_1 \mid \pi \left[|e_j\rangle \langle e_k| \right] \psi_2 \rangle = \langle \psi_1 \mid \pi[X]\psi_2 \rangle .$$

This implies (6.10). Taking $X = I$ and using the unitality of π, we obtain that U is an isometric map of $\mathcal{K}$ into $\mathcal{H} \otimes \mathcal{H}_E$.

Exercise 6.11 Show that the image of $\mathcal{K}$ under the map U coincides with $\mathcal{H} \otimes \mathcal{H}_E$. □

The Stinespring representation (6.6) for a given CP map is not unique. Representations for which $\dim \mathcal{H}_E$ is minimal are called minimal. In this case, the number $\dim \mathcal{H}_E$ is called the rank of the map Φ.

Theorem 6.12. Let

$$\Phi^*[X] = \tilde{V}^* \left(X \otimes \tilde{I}_E \right) \tilde{V}, \quad X \in \mathfrak{B}\left(\mathcal{H}_B\right) \tag{6.13}$$

be another Stinespring representation, where $\tilde{I}_E$ is the unit operator in $\tilde{\mathcal{H}}_E$. Then there exists a partial isometry W_E from $\mathcal{H}_E$ to $\tilde{\mathcal{H}}_E$, such that

$$\left(I_B \otimes W_E\right) V = \tilde{V}; \tag{6.14}$$

if both representations are minimal, then W_E isometrically maps $\mathcal{H}_E$ onto $\tilde{\mathcal{H}}_E$.

Proof. For the representation (6.6), consider the subspace

$$\mathcal{M} = \operatorname{lin} \left\{ \left(X \otimes I_E\right) V\psi : \psi \in \mathcal{H}_A, X \in \mathfrak{B}\left(\mathcal{H}_B\right) \right\} \subset \mathcal{K} = \mathcal{H}_B \otimes \mathcal{H}_E.$$

It is invariant under multiplication by operators of the form $Y \otimes I_E$. Hence, it has the form $\mathcal{M} = \mathcal{H}_B \otimes \mathcal{M}_E$, where $\mathcal{M}_E \subseteq \mathcal{H}_E$. For a minimal representation we should have $\mathcal{M}_E = \mathcal{H}_E$, because otherwise there would be a proper subrepresentation.

Consider a similar subspace $\tilde{\mathcal{M}} = \mathcal{H}_B \otimes \tilde{\mathcal{M}}_E$ of the space $\tilde{\mathcal{K}} = \mathcal{H}_B \otimes \tilde{\mathcal{H}}_E$ for the second representation (6.13). Define the operator W from $\mathcal{M}$ to $\tilde{\mathcal{M}}$ by the relation

$$W \left(X \otimes I_E\right) V\psi = \left(X \otimes \tilde{I}_E \right) \tilde{V}\psi. \tag{6.15}$$

Then W is isometric by polarization, since the norms of the vector $\left(X \otimes I_E\right) V\psi$ and of its image under W are both equal to $\langle \psi | \Phi^* \left[X^* X\right] | \psi \rangle$ by (6.6), (6.13).

From (6.15) we obtain, for all $Y \in \mathfrak{B}\left(\mathcal{H}_B\right)$,

$$W \left(YX \otimes I_E\right) V\psi = \left(Y \otimes \tilde{I}_E \right) W \left(X \otimes I_E\right) V\psi$$

and hence

$$W \left(Y \otimes I_E\right) = \left(Y \otimes \tilde{I}_E \right) W \tag{6.16}$$

on $\mathcal{M}$. Extend W to the whole of $\mathcal{K}$ by setting it equal to zero on the orthogonal complement to $\mathcal{M}$. Then (6.16) holds on $\mathcal{K}$. Therefore, $W = I_B \otimes W_E$, where W_E isometrically maps $\mathcal{M}_E$ onto $\tilde{\mathcal{M}}_E$. Relation (6.15) implies (6.14). If the first representation is minimal, W_E is an isometry of $\mathcal{H}_E$ into $\tilde{\mathcal{H}}_E$, and if both representations are minimal, W_E is unitary onto $\tilde{\mathcal{H}}_E$. □

Corollary 6.13. A map Φ^* is completely positive if and only if it can be represented in the form

$$\Phi^*[X] = \sum_{k=1}^{\tilde{d}} V_k^* X V_k, \quad X \in \mathfrak{B}\left(\mathcal{H}_B\right), \tag{6.17}$$

where $V_k : \mathcal{H}_A \to \mathcal{H}_B$, or dually

$$\Phi[S] = \sum_{k=1}^{\tilde{d}} V_k S V_k^*, \quad S \in \mathfrak{T}(\mathcal{H}_A). \tag{6.18}$$

The map Φ^* is unital (Φ is trace-preserving) if and only if

$$\sum_{k=1}^{\tilde{d}} V_k^* V_k = I. \tag{6.19}$$

This representation is often called the Kraus representation.

Proof. By writing $I_E = \sum_{k=1}^{\tilde{d}} |e_k^0\rangle \langle e_k^0|$, where $\{e_k^0\}$ is an orthonormal basis in $\mathcal{H}_E$ and $\tilde{d} = \dim \mathcal{H}_E$, consider the operators V_k acting from $\mathcal{H}_A$ to $\mathcal{H}_B$, defined by

$$\langle \phi | V_k | \psi \rangle = \left\langle \phi \otimes e_k^0 \right| V |\psi\rangle, \quad \phi \in \mathcal{H}_B, \psi \in \mathcal{H}_A. \tag{6.20}$$

For the operators defined like in (6.20) we shall sometimes use the notation $V_k = \langle e_k^0 | V$. The representation (6.17) then follows from formula (6.6). □

Given a representation (6.17) or (6.18), we can always restore the Stinespring representation by letting $\mathcal{H}_E = \mathbb{C}^{\tilde{d}}$ and

$$V|\psi\rangle = \sum_{k=1}^{\tilde{d}} V_k |\psi\rangle \otimes \left| e_k^0 \right\rangle.$$

Not surprisingly, the Kraus representation of a given completely positive map is not unique. Representations with a minimal number of components come from the minimal Stinespring representations and are also called minimal.

Exercise 6.14 Prove the following statement: the Kraus representation is minimal if and only if the operators $\{V_k\}$ are linearly independent. Hint: from (6.20)

$$\langle \phi | X \left(\sum_{k=1}^{\tilde{d}} c_k V_k \right) |\psi\rangle = \left\langle \phi \otimes \left(\sum_{k=1}^{\tilde{d}} \bar{c}_k e_k^0 \right) \right| (X \otimes I_E) V |\psi\rangle,$$

for all $\phi \in \mathcal{H}_B, \psi \in \mathcal{H}_A, X \in \mathfrak{B}(\mathcal{H}_B)$. Hence, $\sum_{k=1}^{\tilde{d}} c_k V_k = 0$ is equivalent to $\sum_{k=1}^{\tilde{d}} \bar{c}_k e_k^0 \perp \mathcal{M}_E$.

Exercise 6.15 Basing on Theorem 6.12, show that for any two Kraus representations of the same completely positive map, with the operators $V_j, \tilde{V}_k$, there exists a rectangular, partially isometric matrix $[u_{kj}]$, such that $\tilde{V}_k = \sum_j u_{kj} V_j$. If both representations are minimal, the matrix is unitary.

Exercise 6.16 Let $M = \{M_x\}$ be an observable. Show that if

$$M_x = V^* E_x V = \tilde{V}^* \tilde{E}_x \tilde{V} \tag{6.21}$$

are two Naimark dilations of M in $\mathcal{K}, \tilde{\mathcal{K}}$, then there exists a partial isometry $W : \mathcal{K} \to \tilde{\mathcal{K}}$, such that

$$WV = \tilde{V}, \quad W E_x = \tilde{E}_x W.$$

If the dilations are minimal in the sense of the dimensionality of $\mathcal{K}, \tilde{\mathcal{K}}$, then W is isometry of $\mathcal{K}$ onto $\tilde{\mathcal{K}}$.

The set of all CP maps that satisfy the normalization condition (6.19) is apparently convex. Extreme points of this set are given by the following Proposition.

Proposition 6.17 (Choi [46]). The unital CP map Φ^* is extreme if and only if it has a representation (6.17) where the system $\left\{V_j^* V_k\right\}$ is linearly independent.

Proof. Let Φ^* be extreme and let (6.17) be its minimal representation. Let $\sum_{jk} y_{jk} V_j^* V_k = 0$ and denote $Y = \sum_{jk} y_{jk} \left|e_j^0\right\rangle \left\langle e_k^0\right|$. Without loss of generality, we can assume that $Y = Y^*$ and $\|Y\| \leq 1$. Define

$$\Phi_{\pm}^*[X] = V^* \left(X \otimes \left(I_B \pm Y\right)\right) V = \sum_{jk} \left(\delta_{jk} \pm y_{jk}\right) V_j^* X V_k.$$

Then $\Phi_{\pm}^*$ are completely positive maps and $\Phi_{\pm}^*\left[I_B\right] = I_A$ by the assumption. Since Φ^* is extreme, one has $\Phi^* = \Phi_{\pm}^*$, implying $V^*(X \otimes Y)V = 0$ for all X, Y. It follows that

$$\left\langle\psi_2\right| V^* \left(X_2^* \otimes I_E\right) \left(I_B \otimes Y\right) \left(X_1 \otimes I_E\right) V \left|\psi_1\right\rangle \equiv 0.$$

Hence, the bilinear form of the operator $I_B \otimes Y$ vanishes on $\mathcal{M}$ and hence $Y = 0$, by the minimality of the representation. Thus, $y_{jk} \equiv 0$, i. e., the system $\left\{V_j^* V_k\right\}$ is linearly independent.

Conversely, let the system $\left\{V_j^* V_k\right\}$ be linearly independent. Let $\Phi^* = \frac{1}{2}\left(\Phi_1^* + \Phi_2^*\right)$, where Φ_j^* are unital CP maps. In this case, the Kraus operators for Φ_1^*, Φ_2^* are also Kraus operators for some representation of Φ^*, and hence are linearly expressible through $\{V_k\}$, by Exercise 6.15, so that $\Phi_1^*[X] = \sum_{jk} z_{jk} V_j^* X V_k$. Since $\Phi_1^*\left[I_B\right] = I_A$, we have

$$\sum_{jk} z_{jk} V_j^* V_k = \sum_{jk} \delta_{jk} V_j^* V_k.$$

Hence, $z_{jk} = \delta_{jk}$ by linear independence. Therefore, $\Phi_1^* = \Phi^*$ and thus Φ^* is extreme.

By Exercise 1.5, the dimensionality of $\mathfrak{B}\left(\mathcal{H}_A\right)$ is d_A^2. Hence, the rank $\tilde{d}$ of an extreme map should satisfy $\tilde{d}^2 \leq d_A^2$, i. e., $\tilde{d} \leq d_A$ as compared to $\tilde{d} \leq d_A d_B$ (see (6.9)) for an arbitrary map.

10.6.3 6.3 Definition of the Channel

Let us provide a physical interpretation of the property of complete positivity, via the picture of the (irreversible) evolution of an open system interacting with the environment. Let $\mathcal{H}$ be the Hilbert space of the system, $\mathcal{H}_E$ the Hilbert space of its environment, and S_E the initial state of the environment. Assume that the system interacts with the environment via a unitary operator U. The evolution of the system is then given by the formula

$$\Phi[S] = \operatorname{Tr}_E U \left(S \otimes S_E\right) U^*. \tag{6.22}$$

Theorem 6.18. Every linear trace-preserving completely positive map, with $\mathcal{H}_A = \mathcal{H}_B = \mathcal{H}$, can be extended to the evolution of an open system interacting with an environment so that relation (6.22) holds.

Proof. Consider the space $\mathcal{H}_E$ of $\tilde{d}$-dimensional vectors, where $\tilde{d}$ is the number of components in the Kraus representation of Φ. In this case, $\mathcal{H} \otimes \mathcal{H}_E$ can be considered as the direct sum of $\tilde{d}$ copies of $\mathcal{H}$, consisting of column vectors $\left[\psi_1, \ldots, \psi_{\tilde{d}}\right]^\top$, $\psi_j \in \mathcal{H}$, while operators in this space are the block matrices $\left[X_{jk}\right]_{j,k=1,\ldots,\tilde{d}}$, $X_{jk} \in \mathfrak{B}(\mathcal{H})$. Consider the vector $\left|\psi_E\right\rangle = [1, 0, \ldots, 0]^\top$. Then

$$S \otimes \left|\psi_E\right\rangle \left\langle\psi_E\right| = \begin{bmatrix} S & \ldots & 0 \\ \ldots & \ldots & \ldots \\ 0 & \ldots & 0 \end{bmatrix}.$$

Introduce the operator

$$U = \begin{bmatrix} V_1 & \dots & \dots \\ \dots & \dots & \dots \\ V_{\tilde{d}} & \dots & \dots \end{bmatrix}, \tag{6.23}$$

where the first column consists of $V_1, \dots, V_{\tilde{d}}$ and the rest of the columns are chosen to complement it to a unitary operator, which is possible due to (6.19). Now,

$$U\left(S \otimes |\psi_E\rangle \langle\psi_E|\right) U^* = \left[V_j S V_k^*\right]_{j,k=1,\dots,\tilde{d}}$$

The partial trace in $\mathcal{H} \otimes \mathcal{H}_E$, with respect to $\mathcal{H}_E$, is just the sum of the diagonal elements of this matrix, which coincides with the Kraus representation for the map Φ. $\square$

The preceding discussion motivates the following definition. We denote by A the input system of the channel and by B the output system.

Definition 6.19. A channel in the Schrödinger picture is a linear, completely positive trace-preserving map $\Phi : \mathfrak{T}(\mathcal{H}_A) \to \mathfrak{T}(\mathcal{H}_B)$. Dually, a channel in the Heisenberg picture is a linear, completely positive unital map $\Phi^* : \mathfrak{B}(\mathcal{H}_B) \to \mathfrak{B}(\mathcal{H}_A)$.

The channel Φ is called bistochastic if it maps the chaotic state in $\mathcal{H}_A$ into the chaotic state in $\mathcal{H}_B, \Phi[I_A/d_A] = I_B/d_B$. If the input and output systems have equal dimensionalities ($d_A = d_B$), the bistochastic channel Φ is unital. In this case, Φ^* is also trace-preserving, so that both Φ and Φ^* are channels in both the Schrödinger and the Heisenberg picture.

Let $S = S_A$ be an input state of a channel Φ. Denote by $\mathcal{L} = \operatorname{supp} S$ the support of the density operator S. Consider a purification $S_{AR} = |\psi_{AR}\rangle \langle\psi_{AR}|$ of the state S_A, where R labels the purifying system and

$$|\psi_{AR}\rangle = \sum_j \sqrt{\lambda_j}\, |e_j\rangle \otimes |h_j\rangle, \quad \lambda_j > 0, e_j \in \mathcal{L},$$

cf. (3.9). Let Id_R be the identity map in $\mathfrak{T}(\mathcal{H}_R)$. Then the tensor product $\Phi \otimes \mathrm{Id}_R$ describes a channel from AR to BR, transforming A into B and leaving R intact. Therefore, R is called the reference system. The output state of this channel is

$$(\Phi \otimes \mathrm{Id}_R)[S_{AR}] = S_{BR}. \tag{6.24}$$

Since the state S_{AR} is, in general, entangled, this operation is sometimes called "entanglement transmission." Note that by the trace preservation property of Φ, the state S_{BR} has the same partial state S_R as the input state S_{AR}. Since S_R is a copy of the state S_A, the state S_{BR} can be considered a quantum substitute of the joint distribution of the input A and the output B of the channel Φ.

Proposition 6.20. The state S_{BR} uniquely determines the restriction $\Phi_{\mathcal{L}}$ of the channel Φ to the states S with $\operatorname{supp} S \subset \mathcal{L}$. In particular, if S_A is nondegenerate, S_{BR} uniquely determines the channel Φ.

Proof. One has

$$(\Phi \otimes \mathrm{Id}_R)[S_{AR}] = \sum_{j,k} \sqrt{\lambda_j}\sqrt{\lambda_k}\, \Phi\left[|e_j\rangle \langle e_k|\right] \otimes |h_j\rangle \langle h_k|. \tag{6.25}$$

The collection of operators $\Phi[|e_j\rangle \langle e_k|]$ uniquely determines $\Phi_{\mathcal{L}}$. Hence, the statement follows. $\square$

In particular, taking the maximally entangled state

$$S_{AR} = \frac{1}{d} \sum_{j,k} |e_j\rangle \langle e_k| \otimes |h_j\rangle \langle h_k|,$$

we obtain from (6.25), for arbitrary state S,

$$\Phi[S] = d \operatorname{Tr}_R S_{BR} \left(I_B \otimes S_R^\top \right), \tag{6.26}$$

where $S_R^\top = \sum_{j,k} \langle e_k | S | e_j \rangle | h_j \rangle \langle h_k |$ and the state S_{BR} satisfies the characteristic condition $\operatorname{Tr}_B S_{BR} = \bar{S}_R = I_R/d$. This one-to-one correspondence between channels and states is called the Choi-Jamiołkowski correspondence.

10.6.4 6.4 Entanglement-Breaking and PPT Channels

In quantum information theory one often has to deal with both quantum and classical information. A usual device is to embed the classical system into a quantum system, as in Section 2.1.1, by representing classical states and observables on the phase space Ω as diagonal operators in the artificial Hilbert space $\mathcal{H}$ spanned by the orthonormal basis $\{|\omega\rangle; \omega \in \Omega\}$.
i. Any classical-quantum (c-q) channel $x \to S_x$ describing an encoding of the classical input x into the quantum state S_x, as considered in Chapter 5, can then be extended to the quantum channel,

$$\Phi[S] = \sum_x \langle e_x | S | e_x \rangle S_x, \quad S \in \mathfrak{S}(\mathcal{H}_A),$$

where $\{e_x\}$ is an orthonormal basis in $\mathcal{H}_A$.
ii. The quantum-classical ($\mathrm{q}-\mathrm{c}$) channel corresponding to the measurement of observable $M = \{M_y\}$ in $\mathcal{H}_A$ (see Section 6.5), which produces the probability distribution from a quantum state, gives rise to the quantum channel

$$\Phi[S] = \sum_y |e_y\rangle \langle e_y| \operatorname{Tr} S M_y, \quad S \in \mathfrak{S}(\mathcal{H}_A),$$

where $\{e_y\}$ is an orthonormal basis in $\mathcal{H}_B$. The dual channel acts as

$$\Phi^*[X] = \sum_y \langle e_y | X | e_y \rangle M_y. \tag{6.27}$$

The Stinespring representation (6.6) in this case provides Naimark's dilation for the observable M. By taking $X = |e_y\rangle \langle e_y|$, we obtain

$$M_y = V^* (|e_y\rangle \langle e_y| \otimes I_E) V,$$

where $E = \{|e_y\rangle \langle e_y| \otimes I_E\}$ is the sharp observable.
iii. Taking a composition of $\mathrm{q}-\mathrm{c}$ and $\mathrm{c}-\mathrm{q}$ channels with the same orthonormal basis $\{e_j\}$, we obtain the q-c-q channel

$$\Phi[S] = \sum_j S_j \operatorname{Tr} S M_j \tag{6.28}$$

of which i and ii are particular cases. Such channels have a classical system between the input and the output (represented by symbol j).

Definition 6.21. Channel Φ from A to B is entanglement-breaking if for an arbitrary input state S_{AR} of the channel $\Phi \otimes \mathrm{Id}$, its output state S_{BR} is separable (Definition 3.13), i. e., a mixture of product states

$$S_{BR} = \sum_j p_j S_B^j \otimes S_R^j \tag{6.29}$$

where $\{p_j\}$ is a probability distribution.

The following characterization is due to M. Horodecki, Shor, and Ruskai [142].

Proposition 6.22. The following properties are equivalent:

i. channel Φ is entanglement-breaking;

ii. the state S_{BR} in the Choi-Jamiotkowski representation (6.26) is separable;

iii. Φ is $q-c-q$ channel (6.28).

Proof.

i. $\Rightarrow$ ii. This is trivial.

ii. $\Rightarrow$ iii. Taking for S_{AR} the maximally entangled state, and using relations (6.29) and (6.26), we obtain the representation (6.28), in which $S_j = S_B^j, M_j = dp_j \left(S_R^j\right)^\top$.

iii. $\Rightarrow$ i. For a channel (6.28) and any input state S_{AR} of the channel $\Phi \otimes \mathrm{Id}_R$, relation (6.29) holds, with $S_B^j = S_j, p_j S_R^j = \mathrm{Tr}_A\, S_{AR}\,(M_j \otimes I_R)$. $\square$

Example 6.23. An important extreme case of a c – q channel is the completely depolarizing channel, describing the irreversible evolution to some final state S_f, i.e.,

$$\Phi[S] = S_f \cdot \mathrm{Tr}\, S, \quad S \in \mathfrak{T}(\mathcal{H}). \tag{6.30}$$

Exercise 6.24 Prove complete positivity and find a Kraus representation in the examples above.

Definition 6.25. Channel Φ from A to B is PPT if, for an arbitrary input state S_{AR} of the channel $\Phi\otimes$ Id, its output state S_{BR} has a positive partial transpose in the space $\mathcal{H}_R$ (see the end of Section 3.1.3).

Apparently, every entanglement-breaking channel is PPT (but not vice versa, see Horodeckis' paper [139]; a PPT channel which is not entanglement-breaking is called entanglement-binding). If the channel Φ is given by the Kraus decomposition (6.18), the channel $\Phi^\top$ is defined by the relation

$$\Phi^\top[S] = \sum_k V_k^{*\top} S V_k^\top$$

assuming some bases are fixed in the input and output spaces of the channel. Taking into account that $S_{AR}^\top = S_{AR}$, we obtain from (6.24), for the transposition in the basis $\{e_j \otimes h_k\}$,

$$\left(\Phi^\top \otimes \mathrm{Id}_R\right)[S_{AR}] = S_{BR}^\top.$$

It follows that the channels Φ and $\Phi^\top$ are simultaneously PPT or not PPT.

Exercise 6.26 Prove the relation

$$\Phi \circ T_A = T_B \circ \Phi^\top \tag{6.31}$$

where T_A, T_B denote transpositions in the corresponding spaces.

Proposition 6.27. The following conditions are equivalent:

i. the channel Φ is PPT;

ii. the state S_{BR} in the Choi-Jamiotkowski representation (6.26) has a positive partial transpose;

iii. $\Phi \circ T_A$ or $T_B \circ \Phi$ is a channel.

Proof. Again, i $\Rightarrow$ ii is trivial.

ii. $\Rightarrow$ iii. Taking for S_{AR} the maximally entangled state and using the relation (6.26), we obtain

$$(\Phi \circ T_A)[S] = d\,\mathrm{Tr}_R\, S_{BR}\,(I_B \otimes S_R) = d\,\mathrm{Tr}_R\, S_{BR}^{\top_R}\left(I_B \otimes S_R^\top\right)$$

which is a channel, because $S_{BR}^{\top_R} \geq 0$. By relation (6.31) and the remark preceding it, this is equivalent to $T_B \circ \Phi$ being a channel.
iii. $\Rightarrow$ i. Let $T_B \circ \Phi$ be a channel. In this case, for any input state S_{AR} of the channel $\Phi \otimes \mathrm{Id}_R$ we have

$$(\Phi \otimes \mathrm{Id}_R [S_{AR}])^{\top_R} = (T_B \circ \Phi \otimes \mathrm{Id}_R) [S_{AR}]^{\top} \geq 0.$$

10.6.5 6.5 Quantum Measurement Processes

An important example of irreversible evolution is the state change of the system due to a quantum measurement. A complete ideal quantum measurement is associated with an orthonormal basis $|e_x\rangle$, indexed by the measurement outcomes x. It is postulated that the initial state S of the system after such a measurement is transformed into one of the states $|e_x\rangle \langle e_x|$ with probability $\langle e_x| S |e_x\rangle$. Thus, the post-measurement statistical ensemble splits into subensembles corresponding to different measurement outcomes x, and, as a whole, is described by the density operator

$$S' = \sum_x |e_x\rangle \langle e_x| S |e_x\rangle \langle e_x| \tag{6.32}$$

Note that the map $S \to S'$ is a particular case of a q-c channel corresponding to the measurement of an observable $M = \{|e_x\rangle \langle e_x|\}$.

Under an incomplete ideal measurement some outcomes are joined together (coarse-grained), forming the orthogonal resolution of the identity $E = \{E_x\}$,

$$E_x E_{x'} = \delta_{xx'} E_x, \quad \sum_x E_x = I,$$

in other words, a sharp observable in the space $\mathcal{H}$. According to the von NeumannLüders projection postulate, the ideal measurement of the sharp observable E gives an outcome x with the probability

$$p_x = \mathrm{Tr}\, S E_x = \mathrm{Tr}\, E_x S E_x,$$

and the posterior state, i. e., the post-measurement state of the subensemble in which the outcome x has occurred, is

$$S_x = \frac{E_x S E_x}{\mathrm{Tr}\, E_x S E_x}, \quad \text{if } p_x > 0$$

We then have the quantum analog of the Bayes formula for the state of the whole ensemble

$$S' = \sum_x p_x S_x = \sum_x E_x S E_x = \mathcal{E}[S]. \tag{6.33}$$

Note that, as distinct from the classical Bayes formula, the quantum state (6.33) of the whole ensemble after the ideal measurement can be different from the initial state S. Thus, even an ideal quantum measurement does not reduce to a simple reading of the outcome and involves an inevitable interaction, which changes the state of the system. This is a fundamental difference between quantum observables and classical random variables, the observation of which does not change the statistical ensemble and reduces to mere selection of its representatives according to the values of a random variable.

In the Heisenberg picture, the transformation of observables due to an ideal measurement is described by the completely positive map

$$\mathcal{E}^*[X] = \sum_X E_X X E_X = \mathcal{E}[X], \tag{6.34}$$

which can be interpreted as a conditional expectation onto the algebra of operators commuting with all of E_x, characterized by the following properties:

i. $\mathcal{E}^2 = \mathcal{E}$,

ii. $\mathcal{E}[X\mathcal{E}[Y]] = \mathcal{E}[X]\mathcal{E}[Y], X, Y \in \mathfrak{B}(\mathcal{H})$.

An ideal quantum measurement satisfies the repeatability hypothesis: the outcome of the repeated measurement is equal, with probability one, to the outcome of the first measurement (provided no evolution occurred between the two measurements). Most of the real measurement procedures do not fulfill this requirement, and we pass to a mathematical description of nonideal measurements.

Consider the process of indirect measurement, when the system $\mathcal{H}$ in the state S first interacts with a probe system $\mathcal{H}_E$ in the initial state S_E, and next an ideal measurement of a sharp observable $\{E_x^0\}$ is made over the probe system. In this case, according to the above, the probability of an outcome x equals

$$p_x = \operatorname{Tr} U\left(S \otimes S_E\right) U^*\left(I \otimes E_x^0\right),$$

and the posterior state is described by the density operator S_x, such that

$$p_x S_x = \operatorname{Tr}_E U\left(S \otimes S_E\right) U^*\left(I \otimes E_x^0\right) \equiv \Phi_x[S]. \tag{6.35}$$

Thus, the state of the system after the measurement can be written as

$$\Phi[S] = \sum_x p_x S_x = \sum_x \Phi_x[S].$$

The maps Φ_x are completely positive, and their sum Φ is trace-preserving. Any such family $\{\Phi_x\}$ is called an instrument. The instruments describe the statistics and posterior states of nonideal measurements, which in general need not satisfy the repeatability hypothesis.

Note that

$$p_x = \operatorname{Tr} S M_x, \qquad \text{where } M_x = \Phi_x^*[I]$$

is the resolution of the identity describing the observable associated with the instrument and the indirect measurement. Conversely, given an observable $M = \{M_x\}$, one can construct a (nonunique) instrument and indirect measurement with which it is associated. Consider a decomposition $M_x = V_x^* V_x$ and the corresponding unitary operator (6.23) in the space $\mathcal{H} \otimes \mathcal{H}_E$. Then the family of completely positive maps

$$\Phi_x[S] = \operatorname{Tr}_E U\left(S \otimes |\psi_E\rangle\langle\psi_E|\right) U^*\left(I \otimes |e_x\rangle\langle e_x|\right), \tag{6.36}$$

where $|e_x\rangle$ is the column vector with 1 in the x th place and zeroes otherwise, so that $|\psi_E\rangle = |e_1\rangle$, forms an instrument. Further,

$$M_x = \operatorname{Tr}_E\left(I \otimes |\psi_E\rangle\langle\psi_E|\right) U^*\left(I \otimes |e_x\rangle\langle e_x|\right) U = \Phi_x^*[I]. \tag{6.37}$$

Thus, the process of indirect measurement of the observable M is realized by the probe system $\mathcal{H}_E$ in the initial state $|\psi_E\rangle\langle\psi_E|$, the unitary operator U in the space $\mathcal{H} \otimes \mathcal{H}_E$, and the sharp observable $\{|e_x\rangle\langle e_x|\}$ in $\mathcal{H}_E$.

Exercise 6.28 For a complete ideal measurement with $M_x = |e_x\rangle\langle e_x|$, set $V_x = M_x$ and construct the unitary operator U by use of formula (6.23) (in this case $\mathcal{H}_E = \mathcal{H}$). Show that

$$U\left(|e_x\rangle \otimes |e_1\rangle\right) = |e_x\rangle \otimes |e_x\rangle\,.$$

For an arbitrary vector $\psi \in \mathcal{H}$

$$U\left(|\psi\rangle \otimes |e_1\rangle\right) = \sum_x \langle e_x \mid \psi\rangle \left(|e_x\rangle \otimes |e_x\rangle\right),$$

thus, an interaction U produces entanglement between the main and the probe systems, which allows us to reduce the ideal measurement in the main system to the measurement of the sharp observable $\{|e_x\rangle\langle e_x|\}$ in the probe system.

10.6.6 6.6 Complementary Channels

Given three quantum systems A, B, C with the spaces $\mathcal{H}_A, \mathcal{H}_B, \mathcal{H}_C$ and a linear operator $V : \mathcal{H}_A \to \mathcal{H}_B \otimes \mathcal{H}_C$, the relations

$$\Phi_B[S] = \mathrm{Tr}_C\, VSV^*, \quad \Phi_C[S] = \mathrm{Tr}_B\, VSV^*, \quad S \in \mathfrak{T}\left(\mathcal{H}_A\right) \tag{6.38}$$

define two CP maps $\Phi_B : \mathfrak{T}\left(\mathcal{H}_A\right) \to \mathfrak{T}\left(\mathcal{H}_B\right), \Phi_C : \mathfrak{T}\left(\mathcal{H}_A\right) \to \mathfrak{T}\left(\mathcal{H}_C\right)$, which will be called mutually complementary (see Fig. 6.1). If V is an isometry, both maps are trace preserving, i. e., channels.

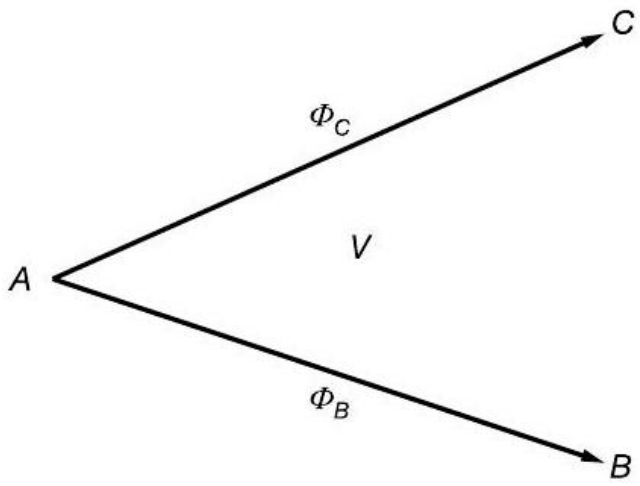


Figure 6.1: Complementary channel.

The Stinespring dilation theorem implies that for a given CP map (channel) a complementary always exists. Moreover, the complementary map is unique in the following sense: for a given CP map Φ_B, any two maps $\Phi_C, \Phi_{C'}$ complementary to Φ_B are isometrically equivalent in the sense that there is a partial isometry $W : \mathcal{H}_C \to \mathcal{H}_{C'}$ such that

$$\Phi_{C'}(S) = W\Phi_C(S)W^*, \quad \Phi_C(S) = W^*\Phi_{C'}(S)W, \tag{6.39}$$

for all S. This is a consequence of Theorem 6.12. If the dimensionalities of $\mathcal{H}_C, \mathcal{H}_{C'}$ are minimal, W is an isometry from $\mathcal{H}_C$ onto $\mathcal{H}_{C'}$. In this case, the complementary map is called minimal.

If $A = B$ is an open quantum system that interacts with the environment $C = E$ in an arbitrary initial state S_E, and Φ_B is the corresponding channel

$$\Phi_B[S] = \mathrm{Tr}_E\, U\left(S \otimes S_E\right) U^*, \tag{6.40}$$

describing the state change of A, the final state of the environment is the output of the channel

$$\Phi_E[S] = \mathrm{Tr}_B\, U\,(S \otimes S_E)\, U^*. \tag{6.41}$$

We will call the channels Φ_B, Φ_E mutually weakly complementary. If the state of the environment is pure, $S_E = |\psi_E\rangle\langle\psi_E|$, then introducing the isometry $V = U\,|\psi_E\rangle : \mathcal{H}_A \to \mathcal{H}_B \otimes \mathcal{H}_E$, which acts as follows:

$$V|\psi\rangle = U\,(|\psi\rangle \otimes |\psi_E\rangle)\,, \quad \psi \in \mathcal{H}_A.$$

We see that Φ_E is the complementary of Φ_B. If S_E is not pure, then by taking its purification $S_{E'}$ in the space $\mathcal{H}_{E'} = \mathcal{H}_E \otimes \mathcal{H}_R$ and letting $U' = U \otimes I_R$, we obtain a representation of the type (6.41), with E replaced by E', where $S_{E'}$ is a pure state. Hence, $\Phi_{E'}$ is the complementary of Φ_B and $\Phi_E[S] = \mathrm{Tr}_R\, \Phi_{E'}[S]$. In contrast to the complementary map, the weak complementary is not unique and depends on the representation (6.40).

To simplify the formulas we shall also use the notation $\tilde{\Phi}$ for the map that is complementary to Φ.

Assume that a CP map $\Phi : \mathfrak{T}(\mathcal{H}_A) \to \mathfrak{T}(\mathcal{H}_B)$ is given by the Kraus representation

$$\Phi[S] = \sum_{k=1}^{\tilde{d}} V_k S V_k^*$$

In this case, a complementary map $\tilde{\Phi} : \tilde{\mathfrak{T}}(\mathcal{H}) \to \mathfrak{M}_{\tilde{d}}$ is given by

$$\tilde{\Phi}[S] = [\mathrm{Tr}\, V_k S V_l^*]_{k,l=1,\tilde{d}} = \sum_{k,l=1}^{\tilde{d}} (\mathrm{Tr}\, S V_l^* V_k)\, |e_k\rangle\langle e_l|\,, \tag{6.42}$$

where $\{e_k\}$ is the canonical basis for the coordinate space $\mathbb{C}^d$, which plays the role of $\mathcal{H}_C$, so that $\tilde{d} = d_C$. This statement follows from the fact that

$$V = \sum_{k=1}^{\tilde{d}} \oplus V_k$$

is a map from $\mathcal{H}_A$ to $\sum_{k=1}^{\tilde{d}} \oplus \mathcal{H}_B \simeq \mathcal{H}_B \otimes \mathcal{H}_C$, for which $\Phi, \tilde{\Phi}$ are given by the partial traces (6.38); see Exercise 3.6.

Exercise 6.29 Check by direct computation that, applying the same procedure to $\tilde{\Phi}$, one obtains the map $\tilde{\tilde{\Phi}}$, which is isometrically equivalent in the sense of (6.39) to Φ.

Exercise 6.30 Prove the following statement: channel Φ is extreme if and only if there exists a complementary channel $\tilde{\Phi}$ such that $\mathrm{Ker}\, \tilde{\Phi}^* = 0$. Hint: prove the relation $\tilde{\Phi}^*[Y] = \sum_{jk} y_{jk} V_j^* V_k$, where $y_{jk} = \langle e_j^0 |\, Y\, |e_k^0\rangle$, and use Proposition 6.17.

Example 6.31. Consider the channel

$$\Phi(S) = S \otimes S_C, \tag{6.43}$$

where S_C is a fixed state in the space $\mathcal{H}_C$. By writing the spectral decomposition

$$S_C = \sum_{k=1}^{\tilde{d}} \lambda_k\, |e_k\rangle\langle e_k|\,,$$

one arrives at the Kraus representation with the operators $V_k = \sqrt{\lambda_k}\,(I \otimes |e_k\rangle) : \mathcal{H}_A \to \mathcal{H}_A \otimes \mathcal{H}_C$. Hence, one obtains from (6.42)

$$\tilde{\Phi}(S) = [\lambda_k \delta_{kl} \operatorname{Tr} S]_{k,l=1,\tilde{d}} \simeq S_C \operatorname{Tr} S,$$

which is a completely depolarizing channel. If S_C is pure, (6.43) is essentially the same as the ideal (identity) channel Id and $\tilde{\Phi}$ is its complementary. Whatever the state S_C, the ideal channel Id is weakly complementary for this channel.

This example illustrates the fact that perfect transmission of quantum information from input A to output B is equivalent to no information going from A to the environment C, and vice versa. Later in this book, we shall see that an approximate version of this complementarity plays a basic role in quantum capacity theorems: the closer channel Φ is to an ideal one, the closer its complement $\tilde{\Phi}$ is to the completely depolarizing one.

The completely depolarizing channel is an instance of entanglement-breaking (q-c-q) channel (see Section 6.4); the construction of the complementary channel can be generalized to the whole of this class. For this, we need the following characterization of entanglement-breaking channels.

Proposition 6.32. Channel $\Phi : \mathfrak{T}(\mathcal{H}_A) \to \mathfrak{T}(\mathcal{H}_B)$ is entanglement-breaking if and only if it has a Kraus representation with rank one operators V_k, i.e.,

$$\Phi[S] = \sum_{k=1}^{\tilde{d}} |\varphi_k\rangle \langle\psi_k| S |\psi_k\rangle \langle\varphi_k|, \tag{6.44}$$

where

$$\sum_{k=1}^{\tilde{d}} |\psi_k\rangle \langle\varphi_k \mid \varphi_k\rangle \langle\psi_k| = I.$$

Proof. Let the channel Φ admit the representation (6.44). In this case, making a renormalization, we can always assume that $\langle\varphi_k \mid \varphi_k\rangle = 1$, in which case $\{|\psi_k\rangle\}$ is an overcomplete system. Denoting $S_k = |\varphi_k\rangle \langle\varphi_k|$ and $M_k = |\psi_k\rangle \langle\psi_k|$, we rewrite (6.44) in the form (6.28). Hence, Φ is entanglement-breaking.

Conversely, by making the spectral decompositions of the operators S_j, M_j in (6.28), we obtain a Kraus representation of the form (6.44). □

The complementary channel $\tilde{\Phi} : \mathfrak{T}(\mathcal{H}_A) \to \mathfrak{T}\left(\mathbb{C}^{\tilde{d}}\right)$ has the form

$$\tilde{\Phi}[S] = [c_{kl} \langle\psi_k| S |\psi_l\rangle]_{k,l=\overline{1,\tilde{d}}} = \sum_{k,l=1}^{\tilde{d}} c_{kl} |e_k\rangle \langle\psi_k| S |\psi_l\rangle \langle e_l|, \tag{6.45}$$

where $c_{kl} = \langle\varphi_l \mid \varphi_k\rangle$. In the special case where the system $\{\psi_k\}_{k=\overline{1,\tilde{d}}}$ is an orthonormal basis in $\mathcal{H}_A$, (6.45) is a channel called dephasing. The reason for this name is that such channels describe the suppression of the off-diagonal elements of the density matrix, due to the fact that $|c_{kl}| \leq 1$. In particular, the completely dephasing channel corresponds to $c_{kl} = \delta_{kl}$. From (6.44) we see that the dephasing channels are complementary to c-q channels. Note that using the Schur (element-wise) product of matrices *, formula (6.45) can in this case be written in the compact form

$$\tilde{\Phi}[S] = C * S,$$

where $C = [c_{kl}]$ and S is the density matrix in the orthonormal basis $\{\psi_k\}$.
For q-c channels, $\{\varphi_k\}_{k=1,\tilde{d}}$ is an orthonormal basis in $\mathcal{H}$, so that $c_{kl} = \delta_{kl}$, and the complementary channel is again a q-c channel.

Noting that an arbitrary positive definite matrix $[c_{kl}]$ can be represented as $c_{kl} = \sum_j \bar{v}_{lj} v_{kj}$, and denoting

$$\tilde{V}_j = \sum_{k=1}^{\tilde{d}} v_{kj} \left|e_k\right\rangle \left\langle\psi_k\right|, \tag{6.46}$$

we have the Kraus representation

$$\tilde{\Phi}[S] = \sum_{j=1}^{d_B} \tilde{V}_j S \tilde{V}_j^* \tag{6.47}$$

for the complementary map. For the dephasing channel, we can take $|e_k\rangle = |\psi_k\rangle$. Hence, one sees from (6.46) that the dephasing maps are characterized by the property of having a Kraus representation with simultaneously diagonalizable (i. e., commuting normal) operators $\tilde{V}_j$.

Definition 6.33. Let $\{p_j\}$ be a finite probability distribution and $\Phi_j : \mathfrak{T}(\mathcal{H}) \to \mathfrak{T}\left(\mathcal{H}'_j\right)$ a collection of channels. Channel $\Phi : \mathfrak{T}(\mathcal{H}) \to \mathfrak{T}\left(\sum_j \oplus \mathcal{H}'_j\right)$ will be called orthogonal convex sum of the channels Φ_j,

$$\Phi = \sum_j \oplus p_j \Phi_j$$

if $\Phi[S] = \sum_j \oplus p_j \Phi_j[S]$ for all $S \in \mathfrak{S}(\mathcal{H})$.

Example 6.34. Quantum erasure channel. Let $p \in [0,1]$. Now, the channel $\Phi : \mathfrak{T}(\mathcal{H}) \to \mathfrak{T}(\mathcal{H} \oplus \mathbb{C})$, defined by the relation

$$\Phi(S) = \begin{bmatrix} (1-p)S & 0 \\ 0 & p \operatorname{Tr} S \end{bmatrix}$$

transmits the input state S with probability $1-p$ and "erases" it with probability p sending the erasure signal. This channel is the orthogonal convex sum of the ideal channel and the completely depolarizing channel (6.30), with a pure final state S_f.

Exercise 6.35 Show that the complementary to the orthogonal convex sum of the channels is the orthogonal convex sum of the complementary channels for the components, i. e.,

$$\widetilde{\sum_j \oplus p_j \Phi_j} = \sum_j \oplus p_j \tilde{\Phi}_j$$

Hint: write the Kraus representation for the orthogonal convex sum, basing on those for the summands, and then use the relation (6.42).

In particular, by using Example 6.31 (with $\tilde{d} = \dim \mathcal{H}_C = 1$), show that the complementary to the erasure channel Φ_p is unitarily equivalent to the erasure channel Φ_{1-p}.

10.6.7 6.7 Covariant Channels

Recall that a projective unitary representation of the group G is a family of unitary operators $\{V_g; g \in G\}$ in a Hilbert space $\mathcal{H}$, satisfying

$$V_g V_h = \lambda(g,h) V_{gh}$$

where $\lambda(g,h)$ is a complex multiplier (of modulus one). If $\lambda(g,h) \equiv 1$, we call it a unitary representation (see, e. g., [171] for more detail).

Let G be a group and $g \to V_g^{(j)}, g \in G$, be two (projective) unitary representations of G in $\mathcal{H}_j, j = A, B$. The channel $\Phi : \mathfrak{T}(\mathcal{H}_A) \to \mathfrak{T}(\mathcal{H}_B)$ is covariant if

$$\Phi\left[V_g^A S\left(V_g^A\right)^*\right] = V_g^B \Phi[S]\left(V_g^B\right)^* \tag{6.48}$$

for all $g \in G$ and S. If the representation V_g^B is irreducible, the channel Φ is bistochastic. Indeed, $V_g^B \Phi\left[I_A\right] = \Phi\left[I_A\right] V_g^B$ (for all g), and irreducibility of V_g^B implies that $\Phi\left[I_A\right]$ is proportional to I_B, with the coefficient obtained by taking the traces.

Definition 6.36. The depolarizing channel in $\mathcal{H}$ is defined by the relation

$$\Phi[S] = (1-p)S + p\frac{I}{d}\operatorname{Tr} S, \quad 0 \leq p \leq \frac{d^2}{d^2-1} \tag{6.49}$$

If $p \leq 1$, this describes a mixture of the ideal channel Id and the completely depolarizing channel which maps an arbitrary state to the chaotic state $\bar{S} = \frac{I}{d}$. For the whole range $0 \leq p \leq \frac{d^2}{d^2-1}$ complete positivity can be demonstrated by the explicit Kraus representation (see (6.54)).

Exercise 6.37 Show that the depolarizing channel can be characterized by the property of unitary covariance, $\Phi\left[USU^*\right] = U\Phi[S]U^*$ for an arbitrary unitary operator U in $\mathcal{H}$.

The depolarizing channel satisfies $\Phi^* = \Phi$ and is thus unital and bistochastic.

Exercise 6.38 Show that the channel complementary to a covariant channel is itself covariant, i.e.,

$$\Phi\left[V_g^A S\left(V_g^A\right)^*\right] = V_g^E \Phi[S]\left(V_g^E\right)^*$$

where $g \to V_g^E$ is a (projective) unitary representation of the group G in $\mathcal{H}_E$. Hint: use the fact that an arbitrary covariant channel has a Kraus representation (6.18), in which operators V_j satisfy the relations

$$V_g^B V_j \left(V_g^A\right)^* = \sum_k d_{jk}(g) V_k$$

where $g \to D(g) = [d_{jk}(g)]$ is a matrix unitary representation of the group G. It follows that the complementary map (6.42) is covariant and the role of the second representation V_g^E is played by $D(g)$.

For future use we introduce here an important general construction, namely, a discrete version of the Weyl operators and canonical commutation relations (CCRs) in a finite-dimensional Hilbert space. Fix an orthonormal basis $\{e_k; k = 1, \ldots, d\}$ in $\mathcal{H}$. The discrete Weyl operators are the unitary operators in $\mathcal{H}$ defined as

$$W_{\alpha\beta} = U^\alpha V^\beta, \quad \alpha, \beta = 0, \ldots, d-1, \tag{6.50}$$

where

$$V\left|e_k\right\rangle = \exp\left(\frac{2\pi i k}{d}\right)\left|e_k\right\rangle, \quad U\left|e_k\right\rangle = \left|e_{k+1(\bmod d)}\right\rangle, \quad k = 0, \ldots, d-1. \tag{6.51}$$

Note that $W_{00} = I$. These operators satisfy the discrete analog of the Weyl-Segal CCR for bosonic systems, which will appear in Chapter 12:

$$\begin{aligned} W_{\alpha\beta} W_{\alpha'\beta'} &= \exp\frac{2\pi i \beta\alpha'}{d} W_{\alpha+\alpha', \beta+\beta'} \\ &= \exp\frac{2\pi i\left(\beta\alpha' - \beta'\alpha\right)}{d} W_{\alpha'\beta'} W_{\alpha\beta}. \end{aligned} \tag{6.52}$$

The first equality expresses the fact that $(\alpha, \beta) \to W_{\alpha\beta}$ is a projective representation of the additive cyclic group $\mathbb{Z}_d \times \mathbb{Z}_d$.

The representation is irreducible: any operator A that commutes with all $W_{\alpha,\beta}$ is a multiple of the unit operator. Indeed, $[A,V]=0$ implies, by (6.51), that $A\left|e_k\right\rangle = a_k\left|e_k\right\rangle$ and $[A,U]=0$ implies $a_k \equiv a$. We then have an important identity: for all states S

$$\sum_{\alpha,\beta=0}^{d-1} W_{\alpha\beta} S W_{\alpha\beta}^* = d(\operatorname{Tr} S) I \tag{6.53}$$

since it follows from (6.52) that the left side commutes with all Weyl operators. The constant on the right is obtained by comparing traces. In fact, the identity (6.53) is a very special case of a general identity, following from orthogonality relations for an arbitrary irreducible representation (see, e. g., Section IV. 2 in [122]).

Exercise 6.39 Prove the Kraus representation for the depolarizing channel (6.49),

$$\Phi[S] = \left(1 - p\frac{d^2-1}{d^2}\right) S + \frac{p}{d^2} \sum_{\alpha+\beta>0} W_{\alpha\beta} S W_{\alpha\beta}^*, \tag{6.54}$$

where all coefficients are nonnegative, provided $0 \leq p \leq \frac{d^2}{d^2-1}$. Hint: substitute the expression for $\operatorname{Tr} S$ from (6.53) into (6.49).

Proposition 6.40. The depolarizing channel is entanglement-breaking for $p \geq \frac{d}{d+1}$.

Proof. To avoid notational confusion with the differential, in this proof we denote the dimensionality as $d_A = \dim \mathcal{H}$. Let Θ be the unit sphere in $\mathcal{H}$ and let $v(d\theta)$ be the uniform distribution on Θ. Thus, $|\theta\rangle \in \Theta$ is a unit vector in $\mathcal{H}$. Now, as we show below,

$$d_A \int_\Theta |\theta\rangle\langle\theta| v(d\theta) = I, \tag{6.55}$$

so that we have a continuous overcomplete system in $\mathcal{H}$. Then as we shall see in Section 11.7, the relation $M(d\theta) = d_A|\theta\rangle\langle\theta|v(d\theta)$ defines an observable in $\mathcal{H}$, with values in Θ, in the sense of Definition 11.29. Its probability distribution in the state S is given by

$$\mu_S^M(d\theta) = d_A\langle\theta|S|\theta\rangle v(d\theta).$$

We prove the statement by using the continuous analog of Proposition 6.32, which will be established later, in Section 11.7.

It is sufficient to prove the statement for $p = \frac{d_A}{d_A+1}$. Then the depolarizing channel for $p > \frac{d_A}{d_A+1}$ can be represented as a mixture of this channel and a completely depolarizing channel $S \to \frac{I}{d_A}\operatorname{Tr} S$, which are both entanglement-breaking. For $p = \frac{d_A}{d_A+1}$, we will prove

$$\Phi[S] \equiv \frac{1}{d_A+1} S + \frac{d_A}{d_A+1}\frac{I}{d_A} = d_A \int_\Theta |\theta\rangle\langle\theta|S|\theta\rangle\langle\theta| v(d\theta) \tag{6.56}$$

for all density operators S, which is a continuous analog of the Kraus representation (6.44), meaning that the channel is entanglement-breaking. We will use Lemma IV.4.1 from [122], according to which, for any continuous function F and a fixed $|\theta'\rangle$,

$$\int_\Theta F\left(|\langle\theta \mid \theta'\rangle|\right) v(d\theta) = -\int_0^1 F(r) d\left(1-r^2\right)^{d_A-1} \tag{6.57}$$

It suffices to establish (6.56) for all $S = |\theta'\rangle\langle\theta'|, \theta' \in \Theta$. Consider the operator

$$\sigma = d_A \int_\Theta |\theta\rangle \langle\theta \mid \theta'\rangle \langle\theta' \mid \theta\rangle \langle\theta| v(d\theta) \tag{6.58}$$

It has unit trace, since

$$\operatorname{Tr}\sigma = d_A \int_\Theta |\langle\theta \mid \theta'\rangle|^2 \, v(d\theta) = -d_A \int_0^1 r^2 d\left(1-r^2\right)^{d_A-1} = 1$$

by (6.57). From this, (6.55) follows by polarization.
Next, σ commutes with all unitaries leaving invariant $|\theta'\rangle$. Hence, it must have the form

$$\sigma = (1-p)\,|\theta'\rangle\,\langle\theta'| + p\frac{I}{d_A}$$

To find p take $\langle\theta'|\,\sigma\,|\theta'\rangle$. We then obtain from (6.58)

$$(1-p) + \frac{p}{d_A} = d_A \int_\Theta |\langle\theta \mid \theta'\rangle|^4 \, v(d\theta) = -d_A \int_0^1 r^4 d\left(1-r^2\right)^{d_A-1}$$

Computing the integral with formula (6.57) we obtain the value $\frac{2}{d_A+1}$, whence $p = \frac{d_A}{d_A+1}$. □

10.6.8 6.8 Qubit Channels

Let us consider channels in the qubit space $\mathcal{H}_2$ which are affine maps of the Bloch ball in $\mathbb{R}^3$, satisfying an additional restriction imposed by complete positivity.

Proposition 6.41. An arbitrary linear, positive, trace-preserving map Φ of the space $\mathfrak{T}(\mathcal{H}_2)$ can be represented in the form

$$\Phi[S] = U_2 \Lambda\left[U_1 S U_1^*\right] U_2^* \tag{6.59}$$

where U_1, U_2 are unitary operators and Λ has the following canonical form, in the basis of Pauli matrices:

$$\Lambda[I] = I + \sum_{y=x,y,z} t_y \sigma_y, \quad \Lambda\left[\sigma_y\right] = \lambda_y \sigma_y, \quad \gamma = x, y, z, \tag{6.60}$$

with λ_y, t_y real.
Proof. The restriction of Φ onto the qubit state space is an affine map, hence it maps the state $S(\vec{a})$, given by (2.8), into the state $S(T\vec{a}+\vec{b})$, where T is a real 3×3-matrix, $\vec{b}$ is a vector in $\mathbb{R}^3$. By using the polar decomposition for T and then the spectral decomposition for $|T|$, we have

$$T = O|T| = O_2 L O_1,$$

where O, O_1, O_2 are orthogonal matrices, $\det O_1 = \det O_2 = 1$, and $L = \operatorname{diag}\left[\lambda_x, \lambda_y, \lambda_z\right]$ is diagonal, with the λ s real but not necessarily nonnegative. Thus,

$$\Phi[S(\vec{a})] = S\left(O_2\left[L\left(O_1\vec{a}\right) + \vec{t}\right]\right), \tag{6.61}$$

where $\vec{t} = O_2^{-1}\vec{b}$.
The matrices O_1, O_2 describe rotations of the Bloch ball in $\mathbb{R}^3$. Let us show that they correspond to reversible evolutions in $\mathcal{H}$, generated by unitary operators U in $\mathcal{H}$ according to formula (6.2). It is sufficient to consider rotation O by an angle φ around the z axis. In this case, a unit vector $\vec{a}$ with the Euler angles θ, ϕ is rotated to $O\vec{a}$, with the angles $\theta, \phi+\varphi$ so that the corresponding state vector (2.9) in $\mathcal{H}$ is transformed into

$$|\psi(O\vec{a})\rangle = \begin{bmatrix} \cos\frac{\theta}{2} e^{-i(\phi+\varphi)/2} \\ \sin\frac{\theta}{2} e^{i(\phi+\varphi)/2} \end{bmatrix} = U|\psi(\vec{a})\rangle, \tag{6.62}$$

where $U = \operatorname{diag}\left[e^{-i\varphi/2}, e^{i\varphi/2}\right]$ is a unitary matrix. Then

$$S(O\vec{a}) = US(\vec{a})U^* \tag{6.63}$$

for all $\vec{a}$.

By using (6.61) we obtain the required statement (6.59). □

Exercise 6.42 Show that a rotation of the Bloch ball around the axis $\vec{a}$ by the angle φ is implemented by the unitary operator

$$U = \exp\left[-\frac{i\varphi}{2}\sigma(\vec{a})\right] = \cos\frac{\varphi}{2}I - i\sin\frac{\varphi}{2}\sigma(\vec{a}).$$

Let us focus our attention on the maps of the form (6.60). Of course, complete positivity imposes nontrivial restrictions on the parameters λ_y, t_y [197]. Especially simple is the case where $t_y \equiv 0$, when the map Φ, and hence Λ, is unital. In this case Λ is a contraction of the Bloch ball along the x, y, z axes, with coefficients $|\lambda_x|, |\lambda_y|, |\lambda_z|$, combined with reflections in case some of the numbers λ_y are negative (for example, $\lambda_y < 0$ implies reflection with respect to the xz plane). Transposition of the density matrix $S(\vec{a})$, which is not completely positive, corresponds to Λ with the parameters $\lambda_x = 1$, $\lambda_y = -1, \lambda_z = 1$. It follows, in particular, that the relation of the type (6.63) also holds for orthogonal matrices O with $\det O = -1$, but with antiunitary operator U. Since any affine bijection of the Bloch ball is apparently implemented by an orthogonal matrix O, this implies Theorem 6.5 in the case of qubits.

Exercise 6.43 By using the multiplication rules (2.17), show that in the case $t_\gamma \equiv 0$

$$\Lambda[S] = \sum_{\gamma=0,x,y,z} \mu_\gamma \sigma_\gamma S \sigma_\gamma, \tag{6.64}$$

where

$$\mu_0 = \tfrac{1}{4}(1 + \lambda_x + \lambda_y + \lambda_z), \quad \mu_x = \tfrac{1}{4}(1 + \lambda_x - \lambda_y - \lambda_z),$$
$$\mu_y = \tfrac{1}{4}(1 - \lambda_x + \lambda_y - \lambda_z), \quad \mu_z = \tfrac{1}{4}(1 - \lambda_x - \lambda_y + \lambda_z).$$

Nonnegativity of these numbers is the necessary and sufficient condition for the complete positivity of Λ and hence of Φ.

In the case $d = 2$, the "discrete Weyl operators" are nothing but the Pauli matrices, namely, with the convention $|e_0\rangle = |\uparrow\rangle, |e_1\rangle = |\downarrow\rangle$, we have

$$W_{01} = V = \sigma_z, \quad W_{10} = U = \sigma_x, \quad W_{11} = UV = -i\sigma_y, \tag{6.65}$$

and the "discrete CCR" are the multiplication rules (2.17).

Exercise 6.44 Show that qubit unital channels (6.64) are covariant with respect to the projective unitary representation of the group $\mathbb{Z}_2 \times \mathbb{Z}_2$ defined by (6.65).

10.6.9 6.9 Notes and References

1. The proof of Theorem 6.5, going back to the famous Wigner theorem [247], follows the book of Davies (see Section 2.3 and Comments in [56]).

2. The notion of a completely positive map, introduced by Stinespring [226] in the more general context of C^*-algebras, was thoroughly studied in the paper of Arveson [10]. A useful survey of the properties of CP maps, including the proof of the inequality from Exercise 6.7, is in the paper of Størmer (pp. 85-106 in the volume [73]). In the finite-dimensional case, which has its own special features, CP maps were considered in detail in the work of Choi [46]. In these works one can find the conditions for extremality of CP maps.

This proof of Theorem 6.9 relies upon Gelfand-Naimark-Segal (GNS) construction, where from an object having a positivity property, one constructs a representation in a Hilbert space. The above proof, with a minor modification, works for CP maps of C^*-algebras in infinite dimensions. In the case of the algebra $\mathfrak{B}(\mathcal{H})$, Lemma 6.10 allows us to obtain the more special result (6.6).

3. The characteristic CP property of the dynamics of an open quantum system was observed in particular by Lindblad [166] and Holevo [108]. However, it was already implicit in the notion of "dynamical matrix" introduced by Sudarshan et al. [230], as well as the representation (6.18). Equivalence of this representation with complete positivity was proved by Choi [46]. Later it was independently considered in great detail in the book of Kraus [157]. Some authors use the name operator-sum representation for (6.17), (6.18). The correspondence (6.26) was introduced by Jamiołkowski [144] for positive maps and by Choi [46] in the case of CP maps. Many interesting applications of this correspondence in the field of quantum information theory are considered by Verstraete and Verschelde [238].

Extensive literature is devoted to the Markovian dynamics of an open system described by a quantum dynamical semigroup, i. e., the semigroup of normalized positive or completely positive maps. A survey of quantum dynamical semigroups and closely related quantum stochastic processes can be found in the books [56], [115].

4. Q-c-q channels were introduced in the paper [114]. A detailed study of entan-glement-breaking channels, including proof of Proposition 6.22, is given in the paper of M. Horodecki, Shor, and Ruskai [142].

Entanglement-binding channels were introduced in Horodeckis' paper [139], where examples of PPT channels that are not entanglement-breaking are given.

5. For detailed discussions of mathematical models for the quantum measurement process, see the books of Ludwig [170], Davies [56], Kraus [157], and Holevo [115] and the papers of Lindblad [164] and Ozawa [184].

6. The notion of complementary channel was introduced in the paper of Devetak and Shor [63]. The results in this section are due to Holevo [118] and to King, Matsumoto, Natanson, and Ruskai [152].

7. Discrete Weyl operators were used in the famous paper of Bennett, Brassard, Crépeau, Jozsa, Peres, and Wootters [22] on quantum teleportation. Concerning the covariance of the complementary channel (Exercise 6.38) see [118]. The ChoiJamiołkowski state of the depolarizing channel is the isotropic state (a mixture of chaotic and maximally entangled states) [192], and a usual way to prove Proposition 6.40, as well as its converse, is to study the separability of that state (see, e. g., [149]).

8. Realistic examples of qubit channels are considered in detail in the book of Nielsen and Chuang [179]. The structure of general qubit channels is described in detail by Ruskai, Szarek, and E. Werner [197]; see also Verstraete and Verschelde [238].

10.7 7 Quantum Entropy and Information Quantities

10.7.1 7.1 Quantum Relative Entropy

The classical relative entropy was considered in Section 4.2, where its monotonicity property and relation to the Shannon mutual information were established. The following definition introduces the noncommutative analog of the relative entropy, which plays an important role in quantum information theory. Many properties of the relative entropy are generalized to the quantum case, but some proofs become much more involved.

Definition 7.1. Let S, T be two density operators. If T is nondegenerate, the quantum relative entropy is defined by the formula

$$H(S;T) = -H(S) - \operatorname{Tr} S \log T = \operatorname{Tr} S(\log S - \log T) \tag{7.1}$$

The case where $\operatorname{supp} S \subseteq \operatorname{supp} T$($\operatorname{supp} S$ denotes support of S, see Section 1.3) is reduced to the previous situation by considering the restrictions of the operators S, T to $\operatorname{supp} T$, where T is nondegenerate. If however $\operatorname{supp} S \nsubseteq \operatorname{supp} T$, then, by definition, $H(S;T) = +\infty$.

Exercise 7.2 Let λ_j, μ_k be the eigenvalues and $|e_j\rangle, |h_k\rangle$ the respective eigenvectors of the density operators S, T. Prove the formula

$$H(S;T) = \sum_{j,k} |\langle e_j \mid h_k\rangle|^2 (\lambda_j \log \lambda_j - \lambda_j \log \mu_k). \tag{7.2}$$

Proposition 7.3. We have

$$H(S;T) \geq \frac{\log e}{2} \operatorname{Tr}(S-T)^2 \geq 0, \tag{7.3}$$

with equalities if and only if $S = T$.

Proof. By using the formula

$$\eta(\lambda) - \eta(\mu) = (\lambda - \mu)\eta'(\mu) + \frac{1}{2}(\lambda - \mu)^2 \eta''(\xi),$$

where ξ lies between λ and μ, we obtain for (4.2) the inequality

$$\lambda \log \lambda - \lambda \log \mu \geq \log \mathrm{e} \left[(\lambda - \mu) + \frac{1}{2}(\lambda - \mu)^2 \right].$$

Substituting this into (7.2), we get the result. □

Corollary 7.4 (Subadditivity of Quantum Entropy). Let S_{12} be a density operator in $\mathcal{H}_1 \otimes \mathcal{H}_2$, with partial states $S_1 = \operatorname{Tr}_{\mathcal{H}_2} S_{12}$ and $S_2 = \operatorname{Tr}_{\mathcal{H}_1} S_{12}$. Then

$$H(S_{12}) \leq H(S_1) + H(S_2), \tag{7.4}$$

with equality if and only if $S_{12} = S_1 \otimes S_2$.

Proof. This follows from the equality

$$H(S_1) + H(S_2) - H(S_{12}) = H(S_{12}; S_1 \otimes S_2)$$

and inequality (7.3). □

Similar to the ordinary entropy (see Exercise 5.3), the relative entropy has the following elementary properties, to be proved in the following exercise.

Exercise 7.5

i. Isometry invariance: $H(VSV^*; VS'V^*) = H(S; S')$ for an arbitrary operator V isometric on the supports of S, S'.

ii. Additivity: $H(S_1 \otimes S_2; S_1' \otimes S_2') = H(S_1; S_1') + H(S_2; S_2')$.

10.7.2 7.2 Monotonicity of the Relative Entropy

The following key property is the noncommutative analog of inequality (4.18).

Theorem 7.6 (Lindblad [166]). For arbitrary density operators S, T in $\mathcal{H}_1$ and arbitrary channel $\Phi : \mathfrak{T}(\mathcal{H}_1) \to \mathfrak{T}(\mathcal{H}_2)$

$$H(\Phi[S]; \Phi[T]) \leq H(S;T). \tag{7.5}$$

This important result follows from Theorem 7.7, to be proved below, which establishes a similar monotonicity property for a whole class of functions of a pair of quantum states.

Consider the Hilbert space $L^2(\mathcal{H})$ of linear operators in $\mathcal{H}$, with the inner product

$$(X, Y) = \operatorname{Tr} X^* Y.$$

Let S, T be nondegenerate operators. In $L^2(\mathcal{H})$, we introduce the operator L_T of left multiplication by T and the operator R_S of right multiplication by S, namely, $L_T X = TX, R_S X = XS$. They are positive commuting Hermitian operators in the Hilbert space $L^2(\mathcal{H})$.

The relative g-entropy of operators S, T is defined by the relation

$$H_g(S;T) = \left(S^{1/2}, g\left(L_T R_S^{-1}\right) S^{1/2}\right), \tag{7.6}$$

for any function $g \in \mathcal{G}$, where $\mathcal{G}$ is the class of functions of the form

$$g(w) = a(w-1) + b(w-1)^2 + \int_0^\infty \frac{(w-1)^2}{w+s} dv(s) \tag{7.7}$$

with a real, $b \geq 0$, and v a positive measure on $[0, \infty)$ such that $\int_0^\infty \frac{1}{s+1} dv(s) < \infty$ (concerning the inner characterization of $\mathcal{G}$ as the class of operator-convex functions such that $g(1) = 0$, see Section 7.8). For the proof of the following theorem it is only important that the function $g(w)$ admits such a representation.

Theorem 7.7 (Petz [189]). For arbitrary $g \in \mathcal{G}$, the relative g-entropy $H_g(S;T)$ has the monotonicity property

$$H_g(\Phi[S]; \Phi[T]) \leq H_g(S;T), \tag{7.8}$$

where Φ is an arbitrary channel.

Theorem 7.6 then follows from the two following observations:

i. the function $g(w) = -\log w$ belongs to the class $\mathcal{G}$. Indeed, by performing integration by parts, one can check that

$$-\ln w = \int_0^\infty \left[\frac{1}{w+s} - \frac{1}{1+s}\right] ds = -(w-1) + \int_0^\infty \frac{(w-1)^2}{(w+s)(s+1)^2} ds$$

ii.

$$H_{-\log}(S;T) = H(S;T).$$

We have

$$-\log\left(L_T R_S^{-1}\right) X = (\log R_S) X - (\log L_T) X = X(\log S) - (\log T)X$$

because of the commutativity of the operators L_T, R_S, whence we obtain $-\log\left(L_T R_S^{-1}\right) S^{1/2} = (\log S - \log T) S^{1/2}$, and the result follows from (7.6).

Proof of Theorem 7.7.

Lemma 7.8. For an arbitrary function $g \in \mathcal{G}$,

$$\begin{aligned} H_g(S;T) =& b \operatorname{Tr}(T-S) S^{-1} (T-S) \\ &+ \int_0^\infty \operatorname{Tr}(T-S) \left(L_T + s R_S\right)^{-1} (T-S) dv(s) \end{aligned} \tag{7.9}$$

Proof. By introducing the notation $\Delta_{T,S} = L_T R_S^{-1}$, we see that

$$(\Delta_{T,S} - I)\, S^{1/2} = (T-S)S^{-1/2} = R_{S^{-1/2}}(T-S), \tag{7.10}$$

hence,

$$H_{w-1}(S;T) = \operatorname{Tr} S^{1/2}(T-S)S^{-1/2} = 0, \tag{7.11}$$

so that the linear term in (7.7) does not contribute to (7.9). For $g(w) = \frac{(w-1)^2}{(w+s)}, s > 0$, we find, by using (7.10),

$$\begin{aligned} H_g(S;T) &= \left((\Delta_{T,S} - I)\, S^{1/2}, (\Delta_{T,S} + SI)^{-1} (\Delta_{T,S} - I)\, S^{1/2}\right) \\ &= \operatorname{Tr}\left[(T-S)\,(\Delta_{T,S} + sI)^{-1} R_{S^{-1}}(T-S)\right] \\ &= \operatorname{Tr}(T-S)\,(L_T + sR_S)^{-1}\,(T-S) \end{aligned} \tag{7.12}$$

For $s = 0$ we get

$$H_{(w-1)^2/w}(S;T) = \operatorname{Tr}(T-S)T^{-1}(T-S) = H_{(w-1)^2}(T;S). \tag{7.13}$$

By substituting this into (7.7), we get (7.9). □

If we neglect the first term in (7.7) (which does not contribute to $H_g(S;T)$), the functions (7.7) are "continual convex combinations" of the functions $(w-1)^2$ and $\frac{(w-1)^2}{w+s}$, $s \geq 0$. Thus, it is sufficient to prove monotonicity of the relative g-entropy for such functions g, i. e., for (7.12).

The proof of Theorem 7.7 now follows from the integral representation (7.9) and the following.

Lemma 7.9. For an arbitrary channel $\Phi, s \geq 0$, and an operator A

$$\operatorname{Tr} A^* \,(L_T + sR_S)^{-1}\, A \geq \operatorname{Tr} \Phi\,[A^*]\left(L_{\Phi[T]} + sR_{\Phi[S]}\right)^{-1} \Phi[A]. \tag{7.14}$$

Proof. Note that positive maps respect Hermitian conjugation, so that $\Phi\,[X^*] = \Phi[X]^*$, and similarly for Φ^*.

Since L_T, R_S are positive operators in $L^2(\mathcal{H})$, the operator $L_T + sR_S$ is also positive. Set $X = (L_T + sR_S)^{-1/2}\, A - (L_T + sR_S)^{1/2}\, \Phi^*[B]$, where $B = \left(L_{\Phi[T]} + sR_{\Phi[S]}\right)^{-1} \Phi[A]$. Then $\operatorname{Tr} X^*X \geq 0$, so that

$$\begin{aligned} &\operatorname{Tr} A^* \,(L_T + sR_S)^{-1}\, A - \operatorname{Tr} A^*\Phi^*[B] \\ &\quad - \operatorname{Tr} \Phi^*\,[B^*]\, A + \operatorname{Tr} \Phi^*\,[B^*]\,(L_T + sR_S)\,\Phi^*[B] \geq 0. \end{aligned} \tag{7.15}$$

We have

$$\operatorname{Tr} A^*\Phi^*[B] + \operatorname{Tr} \Phi^*\,[B^*]\, A = 2 \operatorname{Tr} \Phi\,[A^*]\left(L_{\Phi[T]} + sR_{\Phi[S]}\right)^{-1} \Phi[A]$$

and therefore, in order to prove the lemma, it is sufficient to show that the last term in (7.15) is less than or equal to the right-hand side of (7.14). Thus,

$$\begin{aligned} \operatorname{Tr} \Phi^*\,[B^*]\,(L_T + sR_S)\,\Phi^*[B] &= \operatorname{Tr}\left[s\Phi^*\,[B^*]\,\Phi^*[B]S + \Phi^*\,[B^*]\,T\Phi^*[B]\right] \\ &= \operatorname{Tr}\left[s\Phi^*\,[B^*]\,\Phi^*[B]S + \Phi^*[B]\Phi^*\,[B^*]\,T\right] \\ &\leq \operatorname{Tr}\left[s\Phi^*\,[B^*B]\,S + \Phi^*\,[BB^*]\,T\right] \end{aligned}$$

where the inequality follows from the positivity of S, T and the Kadison inequality (6.5), which in the case of a channel Φ takes the form

$$\Phi^*[B^*]\,\Phi^*[B] \le \Phi^*[B^*B].$$

Then by using the relation $\operatorname{Tr}\Phi^*[B^*B]\,S = \operatorname{Tr} B^*B\Phi[S]$, we find

$$\begin{aligned}\operatorname{Tr}\Phi^*[B^*]\,(L_T + sR_S)\,\Phi^*[B] &\le \operatorname{Tr}\left(sB^*B\Phi[S] + BB^*\Phi[T]\right)\\ &= \operatorname{Tr} B^*(sB\Phi[S] + \Phi[T]B)\\ &= \operatorname{Tr} B^*\left(L_{\Phi[T]} + sR_{\Phi[S]}\right)(B) = \operatorname{Tr} B^*\Phi[A]\\ &= \operatorname{Tr}\Phi[A^*]\left(L_{\Phi[T]} + sR_{\Phi[S]}\right)^{-1}\Phi[A]\end{aligned}$$

□

This proves Theorem 7.7 in the case of nondegenerate S, T. In the general case, either $H(S;T) = +\infty$ and inequality (7.5) is trivial, or $\operatorname{supp} S \subseteq \operatorname{supp} T$, in which case we can assume that $\operatorname{supp} T = \mathcal{H}$, i. e., the operator T is nondegenerate and for $H(S;T)$ formula (7.1) holds. Approximating an arbitrary operator S by nondegenerate operators and using the continuity of the entropy (see Section 7.4), the statement of the theorem in the general case can be proved. □

We now consider a number of useful corollaries of the monotonicity theorem, Theorem 7.6.

Corollary 7.10 (Generalized H-Theorem). Let Φ be a bistochastic (unital) channel in $\mathcal{H} = \mathcal{H}_1 = \mathcal{H}_2$. Then, for any state S,

$$H(\Phi[S]) \ge H(S). \tag{7.16}$$

Proof. From (7.1) it follows that

$$H(S) = \log d - H(S;\bar{S}) \tag{7.17}$$

where $\bar{S} = \frac{1}{d}I$ is the chaotic state, hence

$$H(\Phi[S]) = \log d - H(\Phi[S];\Phi[\bar{S}])$$

because $\Phi[\bar{S}] = \bar{S}$. The corollary now follows by virtue of the monotonicity Theorem 7.6. □

Corollary 7.11. The quantity (5.8) is monotone under the action of the arbitrary channel Φ, i.e.,

$$\chi(\{\pi_\chi\};\Phi[\{S_\chi\}]) \le \chi(\{\pi_\chi\};\{S_\chi\}). \tag{7.18}$$

Proof. By introducing the average state $\bar{S}_\pi = \sum \pi_x S_x$, we obtain the important identity generalizing (4.21)

$$\chi(\{\pi_x\};\{S_x\}) \equiv H\left(\bar{S}_\pi\right) - \sum \pi_x H(S_x) = \sum_x \pi_x H\left(S_x;\bar{S}_\pi\right). \tag{7.19}$$

Therefore (7.18) follows directly from (7.5). □

In particular, Theorem 7.6 implies the bound (5.16) on the Shannon information. Take an arbitrary basis $\{e_y\}$ in $\mathcal{H}$ and consider the q-c channel

$$\Psi[S] = \sum_y \operatorname{Tr} SM_y\,|e_y\rangle\langle e_y|,$$

corresponding to the measurement of the observable $M = \{M_y\}$. Then

$$\Psi\left[S_x\right]=\sum_y p_M(y\mid x)\left|e_y\right\rangle\left\langle e_y\right|,$$

$$\Psi\left[\bar{S}_\pi\right]=\sum_y\left(\sum_x \pi_x p_M(y\mid x)\right)\left|e_y\right\rangle\left\langle e_y\right|,$$

where $p_M(y\mid x)=\operatorname{Tr} S_x M_y$ are the density operators that are diagonal in the basis $\{e_y\}$. Therefore, the quantum relative entropy at the output of the channel Ψ becomes the classical relative entropy, and relation (4.21) implies

$$\sum_x \pi_x H\left(\Psi\left[S_x\right];\Psi\left[\bar{S}_\pi\right]\right)=\mathcal{I}_1(\pi,M).$$

By using the relation (7.18) for the channel Ψ we obtain the required inequality.
A useful quantity, motivated by Corollary 7.10, is the entropy gain

$$G_\Phi[S]=H(\Phi[S])-H(S). \tag{7.20}$$

Corollary 7.12. The entropy gain is convex as a function of S and is superadditive, i.e.,

$$G_{\Phi_1\otimes\Phi_2}\left[S_{12}\right]\geq G_{\Phi_1}\left[S_1\right]+G_{\Phi_2}\left[S_2\right]. \tag{7.21}$$

Proof. Taking into account the first identity in (7.19), the convexity of $G_\Phi[S]$ is just a reformulation of relation (7.18). The superadditivity (7.21) is equivalent to the relation

$$H\left(\left(\Phi_1\otimes\Phi_2\right)\left[S_{12}\right];\left(\Phi_1\otimes\Phi_2\right)\left[S_1\otimes S_2\right]\right)\leq H\left(S_{12};S_1\otimes S_2\right),$$

which follows from the monotonicity theorem, Theorem 7.6. □

10.7.3 7.3 Strong Subadditivity of the Quantum Entropy

Theorem 7.13. The following properties are equivalent:
i. monotonicity of the quantum relative entropy;
ii. strong subadditivity of the quantum entropy; let S_{123} be a density operator in $\mathcal{H}_1\otimes\mathcal{H}_2\otimes\mathcal{H}_3$; in this case, with the obvious notations for the partial states,

$$H\left(S_{123}\right)+H\left(S_2\right)\leq H\left(S_{12}\right)+H\left(S_{23}\right) \tag{7.22}$$

iii. joint convexity of the quantum relative entropy $H(S;T)$ with respect to the arguments S,T.

Proof. i. $\Rightarrow$ ii. Denoting by $\bar{S}_\alpha=\left(\dim\mathcal{H}_\alpha\right)^{-1}I_\alpha$ the chaotic state in $\mathcal{H}_\alpha$, we have

$$H\left(S_{123};\bar{S}_{123}\right)=H\left(S_{123};S_{12}\otimes\bar{S}_3\right)+H\left(S_{12};\bar{S}_{12}\right)$$
$$H\left(S_{23};\bar{S}_{23}\right)=H\left(S_{23};S_2\otimes\bar{S}_3\right)+H\left(S_2;\bar{S}_2\right)$$

Performing subtraction and using (7.17), we get

$$H\left(S_{12}\right)+H\left(S_{23}\right)-H\left(S_{123}\right)-H\left(S_2\right)=H\left(S_{123};S_{12}\otimes\bar{S}_3\right)-H\left(S_{23};S_2\otimes\bar{S}_3\right)$$

Consider the partial trace channel $\Phi\left[S_{123}\right]=S_{23}$. Applying Theorem 7.6 to it, we deduce the nonnegativity of the right-hand side, i. e., the strong subadditivity.
ii. $\Rightarrow$ iii. Consider the density operator in $\mathcal{H}_1\otimes\mathcal{H}_2\otimes\mathcal{H}_3$ of the form

$$S_{123} = \sum_{kl} |e_k\rangle \langle e_k| \otimes A_{kl} \otimes |h_l\rangle \langle h_l| ,$$

where $\{e_k\}$ is an orthonormal basis in $\mathcal{H}_1$, $\{h_l\}$ is an orthonormal basis in $\mathcal{H}_3$, and A_{kl} are positive operators in $\mathcal{H}_2$, which become density operators with an appropriate normalization. Then

$$S_{12} = \sum_k |e_k\rangle \langle e_k| \otimes \sum_l A_{kl}, \quad S_{23} = \sum_{kl} A_{kl} \otimes |h_l\rangle \langle h_l| , \quad S_2 = \sum_{kl} A_{kl},$$

and the strong subadditivity implies

$$-\sum_{kl} H(A_{kl}) + \sum_k H\left(\sum_l A_{kl}\right) + \sum_l H\left(\sum_k A_{kl}\right) - H\left(\sum_{kl} A_{kl}\right) \geq 0,$$

where we denoted $H(A) = -\operatorname{Tr} A \log A$ for a positive operator A. In particular, for arbitrary positive operators A_1, A_2, B_1, B_2,

$$\begin{aligned} & H(A_1 + A_2 + B_1 + B_2) \\ -H(A_1 + A_2) - H(B_1 + B_2) \leq & H(A_1 + B_1) - H(A_1) - H(B_1) \\ & + H(A_2 + B_2) - H(A_2) - H(B_2) \end{aligned}$$

which is equivalent to the joint convexity of the function

$$\Delta(A, B) = H(A + B) - H(A) - H(B)$$

with respect to A, B. On the other hand, the following lemma implies that $H(A; B)$ is convex as a supremum of a family of convex functions.

Lemma 7.14. For any two density operators A, B

$$H(A; B) = \sup_{\lambda > 0} \lambda^{-1} \chi_\lambda(A; B), \tag{7.23}$$

where

$$\begin{aligned} \chi_\lambda(A; B) &= H(\lambda A + (1 - \lambda)B) - \lambda H(A) - (1 - \lambda)H(B) \\ &= \Delta(\lambda A, (1 - \lambda)B) + h(\lambda). \end{aligned}$$

Proof. From the proof above, it follows that the function $\chi_\lambda(A; B)$ is convex with respect to A, B. As a function of $\lambda \in [0, 1]$ it is concave and equal to zero for $\lambda = 0, 1$ (this was proved in Section 5.3). Hence, for fixed A, B

$$\sup_{\lambda > 0} \lambda^{-1} \chi_\lambda(A; B) = \lim_{\lambda \to +0} \lambda^{-1} \chi_\lambda(A; B) = \frac{d}{d\lambda} \chi_\lambda(A; B) \Big|_{\lambda = 0}.$$

Exercise 7.15 Let F be a continuously differentiable function on $(\ 0, +\infty\ )$. Show that for any two positive operators A, B the following holds:

$$\frac{d}{d\lambda} \operatorname{Tr} F(\lambda A + (1 - \lambda)B) = \operatorname{Tr} F'(\lambda A + (1 - \lambda)B)(A - B). \tag{7.24}$$

Hint: prove (7.24) for the case where $F(x) = x^k$, implying the result for polynomials, and then use the Weierstrass uniform approximation theorem.

Now let $\operatorname{supp} A \subseteq \operatorname{supp} B$, so that $H(A; B) < +\infty$. Without loss of generality we assume that the operator B is nondegenerate. Computing the derivative of

$$H(\lambda A + (1-\lambda)B) = \operatorname{Tr} \eta(\lambda A + (1-\lambda)B)$$

by formula (7.24) we obtain

$$\frac{d}{d\lambda}\chi_\lambda(A;B)\Big|_{\lambda=0} = \operatorname{Tr} A(\log A - \log B) + (\log \mathrm{e}) \operatorname{Tr}(B-A) = H(A;B),$$

from which (7.23) follows. □

Exercise 7.16 Prove the statement (7.23) for the case $H(A;B) = +\infty$.

iii. ⇒ i. Consider the density operator S_{12} in $\mathcal{H}_1 \otimes \mathcal{H}_2$ and let $S_1 = \operatorname{Tr}_2 S_{12}$. From the property (6.53) of the discrete Weyl operators, we obtain

$$S_1 \otimes \bar{S}_2 = \frac{1}{d^2} \sum_{\alpha,\beta=0}^{d-1} (I_1 \otimes W_{\alpha\beta})\, S_{12}\, (I_1 \otimes W_{\alpha\beta})^*$$

The joint convexity of the relative entropy and the properties from Exercise 7.5 then imply

$$H\left(S_1; S_1'\right) \leq H\left(S_{12}; S_{12}'\right),$$

which is monotonicity with respect to the partial trace channel. But, according to Theorem 6.9, every channel can be represented as a concatenation of an isometric embedding (preserving the relative entropy) and a partial trace. This proves i. □

By using (7.17) and the convexity of the relative entropy we also obtain the following.

Corollary 7.17. The quantum entropy is concave, i.e., for arbitrary states S_j and probability distribution $\{p_j\}$,

$$H\left(\sum_j p_j S_j\right) \geq \sum_j p_j H\left(S_j\right).$$

Exercise 7.18 Find a direct proof of the concavity, using the spectral decomposition of the operator $\sum_j p_j S_j$ and the concavity of the function $\eta(t)$.

10.7.4 7.4 Continuity Properties

In the finite-dimensional case that we consider here, the quantum entropy is a continuous function of a state. Indeed, the function $\eta(x) = -x \log x$ is (uniformly) continuous on the segment $[0,1]$. Hence, $S_n \to S$ implies $\|\eta(S_n) - \eta(S)\| \to 0$, where $\|\cdot\|$ is the operator norm. Therefore,

$$|H(S_n) - H(S)| = |\operatorname{Tr}(\eta(S_n) - \eta(S))| \leq d\,\|\eta(S_n) - \eta(S)\| \to 0.$$

A more precise estimate, which we will need later, is given by the following.

Lemma 7.19 (Fannes [69]). Let S_1, S_2 be two density operators in d-dimensional Hilbert space, such that $\|S_1 - S_2\|_1 \leq \frac{1}{e}$. In this case,

$$|H(S_1) - H(S_2)| \leq \log d \cdot \|S_1 - S_2\|_1 + \eta\left(\|S_1 - S_2\|_1\right). \tag{7.25}$$

Since the function $\eta(x)$ is monotonously increasing for $x \in \left[0, \frac{1}{e}\right]$, the lemma implies the estimate

$$|H(S_1) - H(S_2)| \leq \log d \cdot \|S_1 - S_2\|_1 + \frac{\log e}{e}. \tag{7.26}$$

Proof. Let $\lambda_1 \geq \lambda_2 \geq \cdots (\mu_1 \geq \mu_2 \geq \cdots)$ be the eigenvalues of S_1 (correspondingly, S_2). Lemma 7.20. Denoting $\Delta_i = |\lambda_i - \mu_i|$, one has

$$\Delta = \sum_{i=1}^{d} \Delta_i \leq \|S_1 - S_2\|_1 . \tag{7.27}$$

Proof. Let $v_1 \geq v_2 \geq \cdots$ be the eigenvalues of the operator

$$A = S_1 + [S_1 - S_2]_- = S_2 + [S_1 - S_2]_+ .$$

Since $A \geq S_1, S_2$, we have $v_i \geq \lambda_i, \mu_i$, so that

$$|\lambda_i - \mu_i| \leq 2v_i - \lambda_i - \mu_i.$$

Therefore,

$$\begin{aligned}\Delta \leq \sum_{i=1}^{d} (2v_i - \lambda_i - \mu_i) &= \operatorname{Tr}(2A - S_1 - S_2) = \operatorname{Tr}[S_1 - S_2]_+ + \operatorname{Tr}[S_1 - S_2]_- \\ &= \|S_1 - S_2\|_1 .\end{aligned}$$

□

Exercise 7.21 Prove the inequality

$$|\eta(y) - \eta(x)| \leq \eta(y - x), \quad 0 \leq x \leq y \leq 1.$$

Combining these statements, we obtain

$$\begin{aligned}|H(S_1) - H(S_2)| &\leq \sum_{i=1}^{d} |\eta(\lambda_i) - \eta(\mu_i)| \leq \sum_{i=1}^{d} \eta(\Delta_i) \\ &= \Delta \sum_{i=1}^{d} \eta(\Delta_i/\Delta) + \eta(\Delta) \leq \Delta \log d + \eta(\Delta)\end{aligned}$$

Taking into account the monotonicity of $\eta(x)$ and combining this with (7.27) produces (7.25). □

Exercise 7.22 Show that the relative entropy is lower semicontinuous in the following sense: if $S_n \to S$ and $S'_n \to S'$, then

$$\lim_{n\to\infty} \inf_n H(S_n; S'_n) \geq H(S; S') .$$

Hint: use the continuity of the entropy, representation (7.23), and the fact that the supremum of a family of continuous functions is lower semicontinuous.

As we shall in Chapter 11, this property holds for both the entropy and the relative entropy in the infinite-dimensional Hilbert space, while the global continuity of the entropy no longer holds.

10.7.5 7.5 Information Correlation, Entanglement of Formation, and Conditional Entropy

In the classical case, the amount of information transmitted by the channel $X \to Y$ is measured by the quantity $I(X;Y) = H(X) + H(Y) - H(XY)$. In quantum statistics there is no general analog of the quantity $H(XY)$, as the joint distribution of observables exists only in special cases. One such case is that of the composite system.

Let S_{12} be a state of a bipartite quantum system in the Hilbert space $\mathcal{H}_1 \otimes \mathcal{H}_2$. In this situation, an obvious quantum analogue of the Shannon mutual information is

$$I(1;2) = H(S_1) + H(S_2) - H(S_{12}) = H(S_{12}; S_1 \otimes S_2). \tag{7.28}$$

We call this information correlation. From Corollary 7.4, it follows that $I(1;2) \geq 0$ and $I(1;2) = 0$ if and only if $S_{12} = S_1 \otimes S_2$.

Take a bipartite system and perform the measurements of observables M_1, M_2 in the corresponding subsystems. Their joint distribution exists and is given by the formula $p(x,y) = \operatorname{Tr} S_{12}(M_{1x} \otimes M_{2y})$. Let $I(M_1; M_2)$ denote the Shannon mutual information between the outcomes of these measurements.

Exercise 7.23 Show that for a pure state $S_{12} = |\psi\rangle\langle\psi|$

$$I(1;2) = 2 \max_{M_1, M_2} I(M_1, M_2). \tag{7.29}$$

In the case of the pure state S_{12} we have $H(S_{12}) = 0$, and Theorem 3.10 implies that

$$H(S_1) = H(S_2)$$

and

$$I(1;2) = H(S_1) + H(S_2) = 2H(S_1). \tag{7.31}$$

The quantity $H(S_1) = H(S_2) = \max I(M_1, M_2)$ then is a natural measure of entanglement of a pure bipartite state S_{12}. It is equal to zero for unentangled states and takes the maximal value $\log d$ for the state (3.7), which explains the name "maximally entangled state."

The question of measures of entanglement for mixed states is substantially more complicated than that for pure states. Unlike the case of pure states there are many
different measures of entanglement for mixed states. Of main interest for us will be entanglement of formation, which is defined for an arbitrary state S_{12} in $\mathcal{H}_1 \otimes \mathcal{H}_2$ as

$$E_F(S_{12}) = \inf \sum_j \pi_j H\left(\operatorname{Tr}_2 S_{12}^j\right), \tag{7.32}$$

where the infimum is taken over all possible decompositions of the density operator

$$S_{12} = \sum_j \pi_j S_{12}^j$$

as convex combinations of some density operators S_{12}^j (in terms of convex analysis, $E_F(S_{12})$ is the convex hull of the continuous function $S_{12} \to H(S_1)$).

Proposition 7.24. The function $S_{12} \to E_F(S_{12})$ is continuous and convex, and the infimum in (7.32) is attained on a convex combination of no more than $(d_1 d_2)^2$ pure states S_{12}^j. Moreover, the duality relation holds, i.e.,

$$E_F(S_{12}) = \max_{A_{12}} \operatorname{Tr} S_{12} A_{12}, \tag{7.33}$$

where the maximization is over the Hermitian operators A_{12} in $\mathcal{H}_1 \otimes \mathcal{H}_2$, satisfying

$$\operatorname{Tr} T_{12} A_{12} \leq H(\operatorname{Tr}_2 T_{12}), \tag{7.34}$$

for all (pure) states T_{12} in $\mathcal{H}_1 \otimes \mathcal{H}_2$.

Proof. Let $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2, S = S_{12}$, and $f(S) = H(\operatorname{Tr}_2 S_{12})$. In this case, f is a continuous concave function on the compact convex set of quantum states $\mathfrak{S} = \mathfrak{S}(\mathcal{H})$. The proof below uses

very few of the other special properties of f and $\mathfrak{S}$, and could be entirely based on references to the convex duality theory. However, we here provide a selfcontained proof.

A finite collection of states with the corresponding probabilities is usually called an ensemble. [1] For our proof it is useful to consider "continual" generalization of ensembles, described by the probability measures $\pi(dS)$ on the set $\mathfrak{S}(\mathcal{H})$ (the concept of a generalized ensemble will be systematically explored in Chapter 11). Now, the usual ensembles correspond to finitely supported measures. By using general facts from measure theory (see, e. g., [186]) one can show that the set $\mathcal{P}(\mathfrak{S}(\mathcal{H}))$ of all probability measures on $\mathfrak{S}(\mathcal{H})$ is itself compact with respect to the topology of weak convergence, which is defined as the convergence of integrals of all bounded continuous functions on $\mathfrak{S}(\mathcal{H})$.

Consider the functional

$$F(\pi) = \int_{\mathfrak{S}} f(T)\pi(dT) \tag{7.35}$$

on $\mathcal{P}(\mathfrak{S}(\mathcal{H}))$, which for finitely supported π coincides with the minimized expression in (7.32). From the definition, it is a continuous, affine functional. We are interested in the minimization of this functional, on the closed convex subset $\mathcal{P}_S$ of probability measures π with the given barycenter

$$S = \int_{\mathfrak{S}(\mathcal{H})} T\pi(dT). \tag{7.36}$$

The continuous functional $F(\pi)$ attains its minimum on the compact set $\mathcal{P}_S$. The concavity of f then implies that we can choose the minimizing measure π to be supported by the pure states, since we can always perform decompositions of all density operators $T = T_{12}$ into pure states, without changing the barycenter and without increasing the value $F(\pi)$.

Let us now show that such an extreme π is supported by no more than $(d_1 d_2)^2$ states. Note that the states supporting π are linearly independent in the sense that if

$$\int_{\mathfrak{S}(\mathcal{H})} c(T)T\pi(dT) = 0 \tag{7.37}$$

for some real bounded measurable function $c(T)$, then $c(T) = 0$ almost everywhere with respect to π. Indeed, it follows from (7.37) that $\pi = \frac{1}{2}\pi_+ + \frac{1}{2}\pi_-$, where

$$\pi_\pm(dT) = (1 \pm \varepsilon c(T))\pi(dT)$$

for sufficiently small ε, so that extremality implies $\pi_\pm(dT) = \pi(dT)$, and hence $c(T) = 0(\mathrm{mod}\pi)$, i. e., almost everywhere with respect to the measure π. By taking the matrix elements of (7.37), we see that the real Hilbert space $L^2_{\mathbb{R}}(\pi)$ is spanned by $(d_1 d_2)^2$ functions

$$\begin{aligned} T &\to \mathrm{Re}\,\langle e_j|\,T\,|e_k\rangle\,, \quad 1 \le j \le k \le d_1 d_2 \\ T &\to \mathrm{Im}\,\langle e_j|\,T\,|e_k\rangle\,, \quad 1 \le j < k \le d_1 d_2. \end{aligned}$$

Indeed, any function $c(T)$ that is orthogonal to all these functions in $L^2_{\mathbb{R}}(\pi)$ must be zero $(\mathrm{mod}\pi)$. The rest follows from the following exercise.

Exercise 7.25 Show that if $\dim L^2_{\mathbb{R}}(\pi) = n$, then π is finitely supported by n points.

The inequality $\ge$ in the duality relation follows from integrating the inequality $f(T) \ge \mathrm{Tr}\,TA$ with respect to an arbitrary probability measure π that satisfies the constraint (7.36). In the proof of the reverse inequality we can consider only those measures which have a fixed (but arbitrary) finite support, containing the support of the optimal (minimizing) measure π^0. In

[0]1 This notion is different from the "statistical ensemble" in Section 2.1.2, which means a statistical sample of identically prepared systems.

this case, the minimization in (7.32) becomes a finitedimensional problem with a finite number of linear constraints, defined by (7.36). Note
that these constraints also imply the constraint expressed by the normalization of a probability measure. Applying the elementary Lagrange method, we then obtain that there exists a Hermitian operator Λ such that π^0 minimizes the functional

$$F(\pi) - \operatorname{Tr}\left(\int_{\mathfrak{S}} \mathrm{T}\,\pi(dT)\right)\Lambda = \int_{\mathfrak{S}} [f(T) - \operatorname{Tr} T\Lambda]\pi(dT) \tag{7.38}$$

over all (nonnormalized) positive measures π with the given finite support. Here, the Hermitian operator Λ simply describes the collection of real Lagrange multipliers for the constraints (7.36). It follows that

$$f(T) - \operatorname{Tr} T\Lambda \geq 0, \tag{7.39}$$

$$f(T) - \operatorname{Tr} T\Lambda = 0 \left(\operatorname{mod}\pi^0\right). \tag{7.40}$$

Inequality (7.39) follows from the fact that otherwise the infimum of the functional (7.38) would be $-\infty$, while equality (7.40) guarantees that the infimum, equal to 0 , is attained. By integrating the second equality with respect to π^0, and taking into account (7.36), we obtain $\operatorname{Tr} S\Lambda = \int_{\mathfrak{S}} f(T)\pi^0(dS)$, which, together with inequality (7.39), implies that Λ is the solution of the dual problem, and (7.33) holds with the common value $\operatorname{Tr} S\Lambda$.

The duality relation implies that the function $E_F(S)$ is lower semicontinuous, as the maximum of the family of continuous (affine) functions $S \to \operatorname{Tr} SA$. It now suffices to show that it is upper semicontinuous, i.e.,

$$\limsup_{n\to\infty} E_F\left(S^{(n)}\right) \leq E_F(S),$$

for any sequence of states $S^{(n)} \to S$. In this proof we follow Shirokov [210]. Let

$$E_F(S) = \sum_{j=1}^{N} \pi_j^0 H\left(\operatorname{Tr}_{\mathcal{H}_2} S_j\right), \tag{7.41}$$

where $S = \sum_{j=1}^{N} \pi_j^0 S_j$. Now, if S is nondegenerate, put

$$S^{(n)} = \sum_{j=1}^{N} \pi_j^{(n)} S_j^{(n)},$$

where

$$\pi_j^{(n)} = t_j^{(n)}\pi_j^0$$
$$S_j^{(n)} = \left(t_j^{(n)}\right)^{-1} \left(S^{(n)}\right)^{1/2} S^{-1/2} S_j S^{-1/2} \left(S^{(n)}\right)^{1/2},$$

and

$$t_j^{(n)} = \operatorname{Tr}\left(S^{(n)}\right)^{1/2} S^{-1/2} S_j S^{-1/2} \left(S^{(n)}\right)^{1/2}.$$

These expressions also make sense for degenerate S, if by $S^{-1/2}$ we denote the generalized inverse of $S^{1/2}$, i. e., the operator that is equal to the inverse on the support of S and zero on its orthogonal complement (see [210] for detail). Now,

$$E_F\left(S^{(n)}\right) \leq \sum_{j=1}^{N} \pi_j^{(n)} H\left(\mathrm{Tr}_{\mathcal{H}_2} S_j^{(n)}\right)$$

and the right-hand side tends to (7.41). Therefore

$$\limsup_{n\to\infty} E_F\left(S^{(n)}\right) \leq E_F(S),$$

that is, E_F is upper semicontinuous, and hence continuous. □

Let us come back to the case of the pure state S_{12}. Note that in classical statistics, partial states of a pure state (marginal distributions of a degenerate distribution) are again pure, and purification has no classical counterpart. Related to this fact is the following unusual property of the quantum analog of conditional entropy. In the classical case, the conditional entropy is always nonnegative, i.e.,

$$H(X \mid Y) = H(XY) - H(Y) = \sum_y p_y H(X \mid Y = y) \geq 0. \tag{7.42}$$

Defining the quantum conditional entropy as

$$H(1 \mid 2) = H\left(S_{12}\right) - H\left(S_2\right),$$

we see that it is negative if S_{12} is a pure entangled state. In other words, unlike the classical entropy, the quantum entropy is not monotone with respect to enlargement of the system, i. e., $H\left(S_1\right) \not\leq H\left(S_{12}\right)$. Nevertheless, similar to the classical case, the following properties hold:
i. monotonicity of the conditional entropy: $H(1 \mid 23) \leq H(1 \mid 2)$;
ii. $H(1 \mid 2) + H(1 \mid 3) \geq 0$.

Exercise 7.26 Show that these properties are reformulations of the strong subadditivity of the quantum entropy (7.22). Hint: use purification of the total state.

Another useful property of the quantum conditional entropy is the following.
Corollary 7.27. The conditional entropy $H(1 \mid 2)$ is a concave function of the state S_{12}. It is subadditive in the following sense:

$$H(13 \mid 24) \leq H(1 \mid 2) + H(3 \mid 4). \tag{7.43}$$

The statements follow from Corollary 7.12 by observing that the conditional entropy is equal to minus the entropy gain that corresponds to the partial trace channel, i.e., $H(1 \mid 2) = -G_{\mathrm{Tr}_1}\left(S_{12}\right)$.

These properties make the conditional entropy a useful tool in quantum information theory.

10.7.6 7.6 Entropy Exchange

Let Φ be a channel from the input system A to the output system B, and let $S = S_A$ be a density operator in $\mathcal{H}_A$ denoting the input state. By Theorem 6.9, the channel admits the Stinespring representation

$$\Phi\left[S_A\right] = \mathrm{Tr}_E\, V S_A V^*, \tag{7.44}$$

where V is an isometric operator from $\mathcal{H}_A$ to $\mathcal{H}_{BE} = \mathcal{H}_B \otimes \mathcal{H}_E$ and $\mathcal{H}_E$ can be thought of as the "environment" of the channel. Transmission of the state S_A produces the state of the environment

$$S_E = \mathrm{Tr}_B\, V S_A V^* = \tilde{\Phi}\left[S_A\right], \tag{7.45}$$

where $\tilde{\Phi}$ is the complementary channel from the input to the environment. In what follows we will simplify notations for the entropies by omitting the notation for the state, i.e., replace $H(S_A)$ by $H(A)$, etc., as we already did in the previous section.

Definition 7.28. The quantity $H(S_E) = H\left(\tilde{\Phi}[S_A]\right)$, which is equal to the output entropy of the environment, is called the entropy exchange and will be denoted $H(S, \Phi)$, or simply $H(E)$.

By using the construction of the complementary channel from (6.42), we see that S_E is given by the density matrix $\left[\operatorname{Tr} SV_j^* V_k\right]_{j,k=\overline{1,N}}$. Hence, we obtain the following result.

Proposition 7.29. Let $\Phi[S] = \sum_{j=1}^N V_j S V_j^*$, with $\sum_{j=1}^N V_j^* V_j = I$. Then

$$H(S, \Phi) = H\left(\left[\operatorname{Tr} SV_j^* V_k\right]_{j,k=\overline{1,N}}\right). \tag{7.46}$$

To obtain another useful expression for $H(S, \Phi)$, we take a reference system $\mathcal{H}_R$. Then we can purify the state S_A to $|\psi_{AR}\rangle\langle\psi_{AR}|$ in $\mathcal{H}_A \otimes \mathcal{H}_R$. Next, compute (see Fig. 7.1)

$$H\left((\Phi \otimes \mathrm{Id}_R)|\psi_{AR}\rangle\langle\psi_{AR}|\right) = H(S_{BR}). \tag{7.47}$$

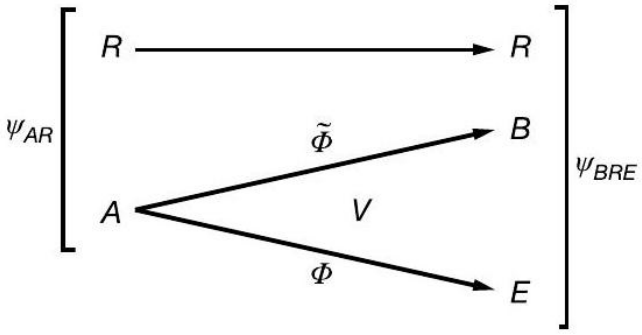


Figure 7.1: Purification with the reference system.

Now, the tripartite system BRE described by the Hilbert space $\mathcal{H}_{BRE} = \mathcal{H}_B \otimes \mathcal{H}_R \otimes \mathcal{H}_E$ is in the pure state

$$|\psi_{BRE}\rangle = (V \otimes I_R)|\psi_{AR}\rangle \tag{7.48}$$

Looking at the split $BR \mid E$ we have a bipartite system in the pure state and therefore, by (7.30),

$$H(S_E) = H(S_{BR}) \tag{7.49}$$

Formula (7.49) provides an alternative expression for the entropy exchange as the output entropy of the extended channel $\Phi \otimes \mathrm{Id}_R$ applied to the purified input state S_{AR}. Since the left-hand side does not involve R, this also shows that $H(S_{BR})$ does not depend on a particular way of purification of the state $S = S_A$.

The entropy exchange satisfies a simple but useful inequality. Let $S = \sum_j p_j S_j$ be a mixture of pure states S_j. In this case,

$$H(S, \Phi) \geq \sum_j p_j H(\Phi[S_j]) \tag{7.50}$$

Indeed, by concavity of the quantum entropy,

$$H(S, \Phi) = H\left(\tilde{\Phi}\left[\sum_j p_j S_j\right]\right) \geq \sum_j p_j H\left(\tilde{\Phi}[S_j]\right)$$

But $H\left(\tilde{\Phi}\left[S_j\right]\right) = H\left(\Phi\left[S_j\right]\right)$, because the system BE is in a pure state as soon as the input S_j is pure.

Example 7.30. Consider the depolarizing channel (6.49) and the input chaotic state $\bar{S} = I_d/d$. By using representation (6.54) with the Kraus operators $V_{\alpha\beta}$ and the properties of discrete Weyl operators, we find

$$\operatorname{Tr} \bar{S} V_{\alpha\beta}^* V_{\alpha'\beta'} = \delta_{(\alpha\beta),(\alpha'\beta')} \begin{cases} \frac{p}{d^2}, & (\alpha\beta) \neq (00) \\ 1 - p\frac{d^2-1}{d^2}, & (\alpha\beta) = (00) \end{cases}$$

Hence,

$$H(\bar{S}, \Phi) = -\left(1 - p\frac{d^2-1}{d^2}\right) \log \left(1 - p\frac{d^2-1}{d^2}\right) - p\frac{d^2-1}{d^2} \log \frac{p}{d^2} \tag{7.51}$$

10.7.7 7.7 Quantum Mutual Information

So far, we have encountered three entropic quantities: the input entropy $H(S)$, the output entropy $H(\Phi[S])$, and the entropy exchange $H(S, \Phi)$. The relation between them allows us to interpret them as the sides of a triangle: the sum of any two of them is larger than the third. For example, the difference in length of the upper two sides of the triangle and its basis can be seen as the information correlation between R and B, i. e.,

$$\begin{aligned} I(S, \Phi) &= H(S) + H(\Phi[S]) - H(S, \Phi) \\ &= H(A) + H(B) - H(E) \\ &= H(R) + H(B) - H(BR) \geq 0 \end{aligned} \tag{7.52}$$

by the subadditivity of the quantum entropy.
Since R has the same entropy as A, this quantity can be thought of as the quantum mutual information between the input and output. The mutual information $I(S, \Phi)$ has a number of nice properties, similar to that of the Shannon information.

Proposition 7.31. The quantum mutual information $I(S, \Phi)$
i. is concave in S;
ii. is convex in Φ;
iii. is subadditive: $I\left(S_{12}, \Phi_1 \otimes \Phi_2\right) \leq I\left(S_1, \Phi_1\right) + I\left(S_2, \Phi_2\right)$;
iv. satisfies the data processing inequalities, i.e.,

$$I\left(S, \Phi_2 \circ \Phi_1\right) \leq \min\left\{I\left(S, \Phi_1\right), I\left(\Phi_1(S), \Phi_2\right)\right\}$$

Proof. The proof is based on playing with different splits of the tripartite system BRE, which is in the pure state (7.48), and on the properties of the conditional entropy.
i. We have

$$\begin{aligned} I(S, \Phi) &= H(R) + H(B) - H(E) \\ &= H(BE) + H(B) - H(E) \\ &= H(B \mid E) + H(B) \end{aligned} \tag{7.53}$$

where the first term is concave in S_{BE} by Corollary 7.27, and the second is concave in S_B. It remains for us to observe that the maps $S \to S_{BE}$ and $S \to S_B$ are affine.
ii. We have

$$
\begin{aligned}
I(S,\Phi) &= H(R) + H(B) - H(E) \\
&= H(R) + H(B) - H(BR) \\
&= H(R) - H(R \mid B)
\end{aligned}
$$

where the first term does not depend on Φ, while the second is concave in $S_{BR} = (\Phi \otimes \mathrm{Id}_R)[S_{AR}]$, which is affine in Φ.

iii. This follows from the expression $I(S,\Phi) = H(B \mid E) + H(B)$ (see (7.53)), the subadditivity (7.43) of the conditional entropy $H(B \mid E)$, and the subadditivity (7.4) of the quantum entropy $H(B)$.

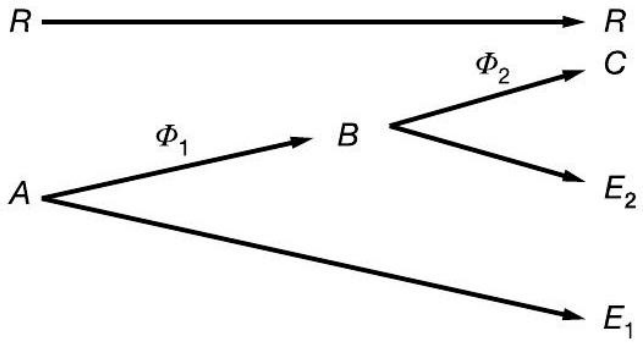


Figure 7.2: Composition of channels.

iv. Denote by A the input of Φ_1, by B the common output of Φ_1 and input of Φ_2, and by C the output of Φ_2. Let also $E_{1,2}$ denote the environments for $\Phi_{1,2}$ (see Fig. 7.2). We have

$$
I(S, \Phi_2 \circ \Phi_1) = H(R) + H(C) - H(E_1 E_2). \tag{7.54}
$$

To prove the first data processing inequality, note that

$$
I(S, \Phi_1) = H(R) + H(B) - H(E_1), \tag{7.55}
$$

so we have to show that $H(C) - H(E_1 E_2) \leq H(B) - H(E_1)$. But since the systems CRE_1E_2 and BRE_1 are in pure states, this is equivalent to

$$
H(R \mid E_1 E_2) \leq H(R \mid E_1),
$$

which is true because of the monotonicity of the conditional entropy. To prove the second data processing inequality, note that

$$
I(\Phi_1[S], \Phi_2) = H(B) + H(C) - H(E_2), \tag{7.56}
$$

so we have to show that $H(R) - H(E_1 E_2) \leq H(B) - H(E_2)$. But since the systems BRE_1 and CRE_1E_2 are in pure states, this is the same as $H(R) - H(CR) \leq H(RE_1) - H(CRE_1)$ or

$$
H(C \mid RE_1) \leq H(C \mid R).
$$

However, the last inequality holds due to the monotonicity of the conditional entropy. □

10.7.8 7.8 Notes and References

1. The entropy of a density operator was introduced by von Neumann [237]. A detailed survey of the properties of the quantum entropy and the quantum relative entropy can be found in the article of Wehrl [242] and in the books of Ohya and Petz [182] and Petz [190].

Inequality (7.3) can be strengthened by replacing $\mathrm{Tr}(S-T)^2$ by $\|S-T\|_1^2$; see [203]. The proof is based on the corresponding classical Pinsker's inequality; see Lemma 12.6.1 in [47].

2. A real function g, defined on the interval $I \subseteq \mathbb{R}$, is called operator-monotone if, for arbitrary natural n and Hermitian $n \times n$-matrices $A \leq B$ with spectra in I, the inequality $g(A) \leq g(B)$ holds. Operator-convex functions are defined in a similar fashion. The main results concerning operator-monotone and operator-convex functions, as well as a number of useful matrix inequalities, can be found in the book of Bhatia [31]. By using the classical results from the theory of operator-monotone and operatorconvex functions one can show that the class $\mathcal{G}$, defined by the relation (7.7), consists of operator-convex functions g on $(0,\infty)$ such that $g(1)=0$.

There are several proofs of the monotonicity theorem, Theorem 7.6. A usual approach is to derive it as a corollary of the celebrated "Lieb concavity" [182], [179]. In a series of papers [164], [165], and [166], Lindblad obtained a number of approximations to the monotonicity property and finally proved its equivalence to the strong subadditivity of the quantum entropy, established earlier by Lieb and Ruskai [163]. Uhlmann [234] gave a different proof based on an interpolation method. Quantum "quasi-entropies," including the relative g-entropies, were introduced by Petz [189], who gave a proof of Theorem 7.7 for maps satisfying (6.5), based on an operator generalization of the Jensen inequality. Here, we follow the paper of Lesniewski and Ruskai [161], where a direct proof of the monotonicity is given that makes no use of the Lieb concavity. This proof is based, after all, on a generalization of the CauchySchwarz inequality and allows us to establish the monotonicity of a whole class of invariants of pairs of states in quantum "geometro-statistics," initiated by Morozova and Chentzov [44]. Effros pointed to the connection of these problems with the notion of the matrix perspective of an operator-convex function [67]. The condition for the equality in the monotonicity property was established by Petz (see also the survey of Ruskai [196]).

A new, "natural" proof of the monotonicity property of the relative entropy was suggested by Bjelaković and Siegmund-Schultze [32] (see also Hayashi [95]), based on the operational interpretation of the quantum relative entropy as the optimal error exponent in the problem of asymptotic discrimination between two quantum states (for the quantum analog of Stein's lemma in mathematical statistics, see Theorem 12.8.1 in [47]). In the paper [178], basing on the properties of "sandwiched Renyi divergence" introduced and studied by Beigi [19], the authors extended the monotonicity property (7.5) to positive maps.

The entropy gain was introduced and studied by Alicki [7].

3. In this section we follow Lindblad [166]; see also the book of Ohya and Petz [182].

4. Lemma 7.19 is due to Fannes [69]. Audenaert [14] obtained the sharp bound

$$|H(S_1) - H(S_2)| \leq \log(d-1) \cdot \|S_1 - S_2\|_1 + h_2\left(\|S_1 - S_2\|_1\right).$$

The connection of this inequality with Fano's lemma, Lemma 4.14, is indicated in the book of Petz [190].

5. The information correlation was considered by Stratonovich [227] and by Lindblad [164]. The entanglement of formation was introduced in the fundamental work of Bennett, DiVincenzo, Smolin, and Wootters [25]. For mixed states, there is a whole variety of measures of entanglement. The quantitative theory of entanglement is another separate chapter of quantum information science, in which the mathematical methods are substantially applied and

developed; see, e. g., the surveys of Keyl [149] and Alber et al. [6] and the book of Hayashi [95].

The definition and properties of the convex hull, as well as the general duality theorem of convex programming, are presented in, e. g., the books of Rockafellar [194] and Magaril-Il'yaev and Tikhomirov [172]. The proof of upper semicontinuity of the entanglement of formation is based on a construction from the work of Shirokov [210].

The quantum conditional entropy was introduced by Adami and Cerf [2]. The operational interpretation of the negative values of the conditional entropy as a "credit" for future quantum communication based on state merging protocol was proposed by M. Horodecki, Oppenheim, and Winter [141].

6. Entropy exchange was introduced (without using this name) by Lindblad [167] and later, independently, in the context of quantum information theory, by Barnum, Nielsen, and Schumacher [18].

7. The quantum mutual information also first appeared in the paper of Lindblad [167] and later, independently, in the paper of Adami and Cerf [2], who studied its properties in detail in an information-theoretic context.

10.8 8 The Classical Capacity of Quantum Channels

10.8.1 8.1 The Coding Theorem

In Chapter 5, the basic coding theorem for a classical-quantum (c-q) communication channel was established. In this chapter, we will use this result to obtain the coding theorem for an arbitrary quantum channel.

Consider the channel $\Phi : \mathfrak{T}(\mathcal{H}_A) \to \mathfrak{T}(\mathcal{H}_B)$ and the corresponding composite, "memoryless" channel $\Phi^{\otimes n} = \Phi \otimes \cdots \otimes \Phi : \mathfrak{T}\left(\mathcal{H}_A^{\otimes n}\right) \to \mathfrak{T}\left(\mathcal{H}_B^{\otimes n}\right)$. The block code for such a composite channel comprises a c-q channel $i \to S_i^{(n)}$ encoding classical messages i into input states $S_i^{(n)}$ in the space $\mathcal{H}_A^{\otimes n}$, and a q-c channel (observable $M^{(n)}$) in the space $\mathcal{H}_B^{\otimes n}$, decoding the output states $\Phi^{\otimes n}\left[S_i^{(n)}\right]$ into classical messages j, i. e.,

$$i \to S_i^{(n)} \to \Phi^{\otimes n}\left[S_i^{(n)}\right] \to j.$$

This leads to the following definition.

Definition 8.1. A code $\left(\Sigma^{(n)}, M^{(n)}\right)$ of length n and of size N for the composite channel $\Phi^{\otimes n}$ consists of an encoding, given by a collection of states $\Sigma^{(n)} = \left\{S_i^{(n)}; i = 1, \ldots, N\right\}$ in $\mathcal{H}_A^{\otimes n}$, and a decoding, described by an observable $M^{(n)} = \left\{M_j^{(n)}; j = 0, 1, \ldots, N\right\}$ in $\mathcal{H}_B^{\otimes n}$.

The maximal error probability of the code is equal to

$$P_e\left(\Sigma^{(n)}, M^{(n)}\right) = \max_{i=1,\ldots,N}\left[1 - p_{\Sigma M}(i \mid i)\right] \tag{8.1}$$

where

$$p_{\Sigma M}(j \mid i) = \operatorname{Tr} \Phi^{\otimes n}\left[S_i^{(n)}\right] M_j^{(n)} \tag{8.2}$$

is the probability to make a decision j under the condition that a message i was sent. The minimum of the error $P_e\left(\Sigma^{(n)}, M^{(n)}\right)$ over all codes of length n and size N is again denoted $p_e(n, N)$. The classical capacity $C(\Phi)$ of the quantum channel Φ is defined as the least upper bound of the rates R for which

$$\lim_{n\to\infty} p_e\left(n, 2^{nR}\right) = 0$$

Let us recall that a finite probability distribution π on the set of quantum states $\mathfrak{S}(\mathcal{H})$, that assigns the probabilities π_i to states S_i, is called an ensemble. If an ensemble $\pi^{(n)}$ with probabilities $\left\{\pi_i^{(n)}\right\}$ of the input states $S_i^{(n)}$ is given, then using the transition probability $p_{\Sigma M}(j \mid i)$, we can find the joint distribution of input i and output j and
compute the Shannon information $\mathcal{I}_n\left(\pi^{(n)}, M^{(n)}\right)$ according to formula (5.14). Applying Shannon's coding theorem, we obtain, as in Proposition 5.15,

$$C(\Phi) = \lim_{n\to\infty} \frac{1}{n} \sup_{\left\{\pi^{(n)}, M^{(n)}\right\}} \mathcal{I}_n\left(\pi^{(n)}, M^{(n)}\right). \tag{8.3}$$

In contrast to the case of c − q channels, there is no fixed alphabet here, and one has to optimize not only with respect to the output observable $M^{(n)}$ and the input distribution $\left\{\pi_i^{(n)}\right\}$, but also with respect to all possible states $S_i^{(n)}$ at the input of the channel $\Phi^{\otimes n}$.

Proposition 8.2. The classical capacity of channel Φ is equal to

$$C(\Phi) = \lim_{n\to\infty} \frac{1}{n} C_\chi\left(\Phi^{\otimes n}\right), \tag{8.4}$$

where

$$C_\chi(\Phi) = \sup_\pi \chi\left(\{\pi_i\}; \{\Phi[S_i]\}\right), \tag{8.5}$$

the quantity χ is defined by the relation (5.8), and the supremum is taken over all input ensembles $\pi = \{\pi_i, S_i\}$ in $\mathfrak{S}(\mathcal{H})$.

Note that, similar to Proposition 5.15, the limit in the relations (8.3), (8.4) as $n \to \infty$ is equal to the supremum over n, due to superadditivity of the corresponding sequences.

Proof. From the upper bound of Theorem 5.9

$$\mathcal{I}_n\left(\pi^{(n)}, M^{(n)}\right) \le C_\chi\left(\Phi^{\otimes n}\right).$$

The inequality $\le$ in (8.4) then follows from (8.3).
Let us show that

$$C(\Phi) \ge \lim_{n\to\infty} \frac{1}{n} C_\chi\left(\Phi^{\otimes n}\right) \equiv \bar{C}(\Phi). \tag{8.6}$$

Take $R < \bar{C}(\Phi)$. In this case, we can choose n_0 and an ensemble $\pi^{(n_0)} = \left\{\pi_i^{(n_0)}, S_i^{(n_0)}\right\}$ in $\mathcal{H}_A^{\otimes n_0}$ such that

$$n_0 R < \chi\left(\left\{\pi_i^{(n_0)}\right\}; \left\{\Phi^{\otimes n_0}\left[S_i^{(n_0)}\right]\right\}\right). \tag{8.7}$$

Consider the c-q channel $\tilde{\Phi}$ in $\mathcal{H}_B^{\otimes n_0}$ defined by the formula

$$i \to \Phi^{\otimes n_0}\left[S_i^{(n_0)}\right]. \tag{8.8}$$

By the coding theorem, Theorem 5.4, for c-q channels, the capacity of $\tilde{\Phi}$ is

$$C(\tilde{\Phi}) = \max_{\{\pi_i\}} \chi\left(\{\pi_i\}; \left\{\Phi^{\otimes n_0}\left[S_i^{(n_0)}\right]\right\}\right), \tag{8.9}$$

where the states $S_i^{(n_0)}$ are fixed and the maximum is taken over the probability distributions $\{\pi_i\}$. By (8.7), this is greater than $n_0 R$. Denoting by $\tilde{p}_e(n, N)$ the minimal error probability for $\tilde{\Phi}$, we have

$$p_e\left(nn_0, 2^{(nn_0)R}\right) \leq \tilde{p}_e\left(n, 2^{n(n_0R)}\right), \tag{8.10}$$

since every code of size N for $\tilde{\Phi}$ is also a code of the same size for Φ. Thus, having chosen $R < \bar{C}(\Phi)$, we can make the right-hand side and hence the left-hand side of (8.10) tend to zero as $n \to \infty$. Via the same argument as in Proposition 5.15 we can prove that $p_e\left(n', 2^{n'R}\right) \to 0$, when $n' \to \infty$, and hence (8.6) follows. □

10.8.2 8.2 The χ-Capacity

We shall call the quantity $C_\chi(\Phi)$, defined in (8.5), the χ-capacity of the channel Φ. Thus,

$$C_\chi(\Phi) = \sup_\pi \left[H\left(\sum_i \pi_i \Phi\left[S_i\right]\right) - \sum_i \pi_i H\left(\Phi\left[S_i\right]\right)\right], \tag{8.11}$$

where $\pi = \{\pi_i, S_i\}$. It can also be rewritten as

$$C_\chi(\Phi) = \sup_{S \in \mathfrak{S}(\mathcal{H})} \left[H(\Phi(S)) - \hat{H}_\Phi(S)\right] \tag{8.12}$$

where the new channel characteristic

$$\hat{H}_\Phi[S] = \inf_{\pi: \sum_i \pi_i S_i = S} \sum_i \pi_i H\left(\Phi\left[S_i\right]\right) \tag{8.13}$$

was introduced, which is called the convex hull of the output entropy $H(\Phi[S])$. Here, the infimum is taken over all ensembles $\pi = \{\pi_i, S_i\}$, with the fixed average state $\sum_i \pi_i S_i = S$. Note that, by concavity of the quantum entropy, it is sufficient to take the infimum with respect to the convex decompositions of S into the pure states S_i.

Exercise 8.3 Prove that for the ideal channel $\hat{H}_{\mathrm{id}}(S) \equiv 0$. Hint: consider the spectral decomposition of S.

The quantity (8.13) is closely related to the entanglement of formation (7.32), namely,

$$\hat{H}_\Phi(S) = E_F\left(VSV^*\right),$$

where V is the isometry in the Stinespring representation (6.7) of the channel Φ, so that VSV^* is the state of the composite system "output-environment." The proof of the following lemma is similar to that of Proposition 7.24, with the dimensionality $d_1 d_2$ of $\mathcal{H}_1 \otimes \mathcal{H}_2$ replaced with the dimensionality d_1 of $\mathcal{H}_1$.

Lemma 8.4. The convex hull of the output entropy $\hat{H}_\Phi(S)$ is a continuous convex function on $\mathfrak{S}(\mathcal{H})$. The infimum in (8.13) is attained on an ensemble consisting of no more than d_A^2 pure states, $d_A = \dim \mathcal{H}_A$.

Corollary 8.5. The supremum in the expression (8.11) for the χ-capacity is attained on an ensemble consisting of no more than d_A^2 pure states.

Exercise 8.6 By using Exercise 4.8, show that an ensemble $\pi = \{\pi_i, S_i\}$ with the average state $\bar{S}_\pi = \sum_i \pi_i S_i$ is optimal for the supremum in expression (8.11) if and only if the following maximal distance condition holds: there exists a positive μ such that

$$H\left(\Phi[S]; \Phi\left[\bar{S}_\pi\right]\right) \leq \mu, \qquad \text{for all (pure) input states } S, \tag{8.14}$$

with equality for members $S = S_i$ of the ensemble with $\pi_i > 0$. In this case, necessarily, $\mu = C_X(\Phi)$. Hint:

$$\frac{\partial}{\partial \pi_j} \chi\left(\{\pi_i\}; \{\Phi\left[S_i\right]\}\right) = H\left(\Phi\left[S_j\right]; \Phi\left[\bar{S}_\pi\right]\right) - \log \mathrm{e}.$$

The χ-capacity can be computed for a number of interesting channels.

Exercise 8.7 Show that $C_X(\mathrm{Id}) = \log d$ for the ideal channel in d-dimensional Hilbert space. For the quantum erasure channel $C_X(\Phi_p) = (1-p)\log d$, where p is the probability of erasure. In both cases the optimal ensemble consists of equiprobable pure states corresponding to an orthonormal basis in $\mathcal{H}$.

Proposition 8.8. Let Φ be a covariant channel (see Section 6.7),

$$\Phi\left[U_g^A S \left(U_g^A\right)^*\right] = U_g^B \Phi[S] \left(U_g^B\right)^*.$$

If the representation U_g^A is irreducible (in which case Φ is called irreducibly covariant),

$$C_\chi(\Phi) = H\left(\Phi\left[\frac{I_A}{d_A}\right]\right) - \min_S H(\Phi[S]), \tag{8.15}$$

where the minimum is taken over the set of pure states.

Proof. Assume first that the symmetry group is finite. Irreducibility of the representation means that it has no nontrivial invariant subspaces, which is equivalent to the following: any operator that commutes with all U_g^A is a multiple of the unit operator. It follows, similar to the proof of relation (6.53), that for all states S

$$\frac{1}{|G|}\sum_{g\in G} U_g^A S \left(U_g^A\right)^* = \frac{I_A}{d_A}. \tag{8.16}$$

Let us show that

$$\max_{S\in\mathfrak{S}(\mathcal{H})} H(\Phi[S]) = H\left(\Phi\left[\frac{I_A}{d_A}\right]\right). \tag{8.17}$$

This follows from the fact that the function $S \to H(\Phi[S])$ is concave and invariant with respect to the transformations $S \to U_g^A S U_g^{A*}$. Therefore, for arbitrary state S,

$$\begin{aligned} H(\Phi[S]) &= |G|^{-1}\sum_{g\in G} H\left(\Phi\left[U_g^A S \left(U_g^A\right)^*\right]\right) \\ &\le H\left(\Phi\left[|G|^{-1}\sum_{g\in G} U_g^A S \left(U_g^A\right)^*\right]\right) \end{aligned}$$

The inequality $\le$ in (8.15) then follows from (8.16), and it is sufficient to show that

$$C_\chi(\Phi) \ge H\left(\Phi\left[\frac{I_A}{d_A}\right]\right) - \min_S H(\Phi[S]). \tag{8.18}$$

Let us choose a state S_0 that minimizes the output entropy. Since the entropy is concave, it attains the minimum on pure states. Then the value in the right-hand side of (8.15) is attained for the ensemble of states $S_g = U_g^A S_0 U_g^{A*}$, $g \in G$, with equal probabilities $\pi_g = |G|^{-1}$.

If the group is continuous, a similar argument applies, but the optimizing distribution will be continuous, namely, the uniform distribution on G. One can then use a finite approximation and the continuity of the entropy.

Example 8.9. For the depolarizing channel (6.49)

$$C_\chi(\Phi) = \log d + \left(1 - p\frac{d-1}{d}\right)\log\left(1 - p\frac{d-1}{d}\right) + p\frac{d-1}{d}\log\frac{p}{d} \tag{8.19}$$

which is achieved for an ensemble of equiprobable, orthogonal pure states forming an orthonormal basis in $\mathcal{H}$.

Indeed, the channel is irreducibly covariant, hence (8.15) applies. The output entropy is concave. Hence, it achieves the minimum on the set of pure states. For an arbitrary pure input state, the output $\Phi[|\psi\rangle\langle\psi|]$ has the simple eigenvalue $\left(\ 1-p\frac{d-1}{d}\ \right)$ and $d-1$ eigenvalues $\frac{p}{d}$. Hence, the output entropy has the same value

$$-\left(1-p\frac{d-1}{d}\right)\log\left(1-p\frac{d-1}{d}\right)-p\frac{d-1}{d}\log\frac{p}{d}$$

for all pure input states, and (8.19) follows.

Example 8.10. Let us compute the χ-capacity of an arbitrary qubit unital channel Φ. Such a channel is irreducibly covariant with respect to the representation (6.65) (see Exercise 6.44). Hence, we can again apply Proposition 8.8.

In computing $\min_{S\in\mathfrak{S}(\mathcal{H})} H(\Phi(S))$ it is sufficient to consider $\Phi=\Lambda$, by taking into account the unitary invariance of the quantum entropy. We also remark that by Exercise 2.5 the entropy of the qubit state (2.8) is equal to

$$H(S(\vec{a}))=h_2\left(\frac{1-|\vec{a}|}{2}\right) \tag{8.20}$$

Now, the Bloch ball is contracted, by the channel Λ, to the ellipsoid with lengths of the axes $|\lambda_y|\,,\gamma=x,y,z$, and the minimal output entropy is attained at the top of the longest axis, which corresponds to the state with the eigenvalues $\frac{1\pm\max_y|\lambda_y|}{2}$. This gives the χ-capacity

$$C_\chi(\Phi)=1-h_2\left(\frac{1-\max_y|\lambda_y|}{2}\right). \tag{8.21}$$

10.8.3 8.3 The Additivity Problem

10.8.4 8.3.1 The Effect of Entanglement in Encoding and Decoding

Several interesting and difficult mathematical problems in quantum information theory are related to the proof or disproof of the additivity property, i.e.,

$$C_\chi\left(\Phi_1\otimes\Phi_2\right)=C_\chi\left(\Phi_1\right)+C_\chi\left(\Phi_2\right), \tag{8.22}$$

for some channels Φ_1,Φ_2. Obviously, always

$$C_\chi\left(\Phi_1\otimes\Phi_2\right)\geq C_\chi\left(\Phi_1\right)+C_\chi\left(\Phi_2\right).$$

If (8.22) is fulfilled for the channel $\Phi=\Phi_1$ and an arbitrary channel Φ_2, then

$$C_\chi\left(\Phi^{\otimes n}\right)=nC_\chi(\Phi) \tag{8.23}$$

and due to relation (8.4) the classical capacity of the channel Φ is equal to the χ-capacity,

$$C(\Phi)=C_\chi(\Phi) \tag{8.24}$$

Property (8.22) was established for some important classes of channels $\Phi=\Phi_1$ (and arbitrary Φ_2) such as entanglement-breaking channels (Shor [215]), unital qubit channels (King [150]), depolarizing channels (King [151]), and several others. In particular, equality (8.24) holds for the classical capacity of all these channels. There was a strong belief that the additivity should hold for arbitrary channels Φ_1,Φ_2, supported by the absence of counterexamples and intensive numerical search in low dimensions. However, it was finally shown that in very high dimensions there exist channels that violate (8.22), (8.23), (8.24). We will discuss these results in Section 8.3.5.

The additivity of the Shannon capacity for classical channels, after all, relies upon the absence of entanglement in the classical systems. To see this, let us try to generalize the classical proof based on the Kuhn-Tucker conditions (see Proposition 4.9) to the quantum case. Let Φ_1, Φ_2 be two channels with the optimal ensembles having averages $\bar{S}_{\pi^1}, \bar{S}_{\pi^2}$. We wish to prove that

$$C_\chi(\Phi_1 \otimes \Phi_2) \leq C_\chi(\Phi_1) + C_\chi(\Phi_2). \tag{8.25}$$

Then condition (8.14), applied to the product channel $\Phi_1 \otimes \Phi_2$, requires the inequality

$$H\left((\Phi_1 \otimes \Phi_2)[S_{12}]; (\Phi_1 \otimes \Phi_2)\left[\bar{S}_{\pi^1} \otimes \bar{S}_{\pi^2}\right]\right) \leq C_\chi(\Phi_1) + C_\chi(\Phi_2) \tag{8.26}$$

to hold for all pure input states S_{12} of the product channel. Moreover, equality must hold for the tensor products of the members of the optimal ensembles with positive probabilities, which easily follows from the corresponding equalities for the channels Φ_1, Φ_2, as well as inequality (8.26) for product states. However, proving (8.26) for entangled states is no simpler than proving the inequality

$$C_\chi(\Phi_1 \otimes \Phi_2) \leq C_\chi(\Phi_1) + C_\chi(\Phi_2)$$

which is the main problem with (8.22), since the opposite inequality follows from the definition of C_χ.

Additivity of $C_\chi(\Phi)$ would have a surprising physical consequence - it would mean that using entangled input states does not increase the classical capacity of a quantum channel. However, as shown in Section 5.4, using entangled observables at the output of any essentially quantum channel (i.e., a channel with noncommuting output states) increases the capacity. From this point of view it is surprising that the additivity of $C_\chi(\Phi)$ is a rather widespread phenomenon. Let us discuss entangled inputs in more detail.

The encoding $\Sigma^{(n)} = \left\{S_i^{(n)}\right\}$ in Definition 8.1 of a code will be called unentangled if

$$S_i^{(n)} = \sum_{\chi^n} p(\chi^n \mid i)\, S_{x_1} \otimes \cdots \otimes S_{x_n} \tag{8.27}$$

where S_{x_k} is a state in the k th copy of the space $\mathcal{H}_A$ and $p(x^n \mid i)$ is a conditional probability describing preliminary processing of the input message. Let us recall that a decoding $M^{(n)}$ is unentangled if it has the form (5.36).

Given a quantum channel Φ, one can define the four classical capacities $C_{1,1}, C_{1,\infty}$, $C_{\infty,1}, C_{\infty,\infty}$, where the first (second) index refers to the inputs (outputs), ∞ means using arbitrary entangled inputs (outputs), and 1 means restriction to unentangled inputs (outputs) in Definition 8.1 and correspondingly in formula (8.3). By definition,

$$C_{\infty,\infty} = C(\Phi)$$

Exercise 8.11 Show, by using (8.27), the data-processing inequality (4.20), and the Shannon coding theorem, Theorem 4.13, that

$$C_{1,1} = \max_{\pi, M} \mathcal{I}_1(\pi, M).$$

Here, π is an arbitrary ensemble at the input of the channel Φ, and M is an arbitrary observable at the output.

The quantity $C_{1,1}$ is sometimes called the Shannon capacity of the quantum channel Φ.

Exercise 8.12 By using the coding theorem, Theorem 5.4 for c-q channels, show that

$$C_{1,\infty} = C_X(\Phi).$$

The relations between these four capacities are shown in the following diagram:

$$\begin{array}{c} C_{\infty,1} \leq C_{\infty,\infty} (= C) \\ \| \quad \| \\ C_{1,1} \leq C_{1,\infty} \, (= C_\chi) \, , \end{array} \tag{8.28}$$

where $\leq$ should be understood as "always less than or equal to, and strictly less for some channels."

The equality

$$C_{1,1} = C_{\infty,1} \tag{8.29}$$

shows that using entangled input states with unentangled output measurements does not increase the accessible information. It will be proved below. The upper inequality $C_{\infty,1} \neq C_{\infty,\infty}$ follows from this and from the lower inequality, which expresses the strict superadditivity with respect to the output measurements demonstrated in Section 5.4.

Proof of equality (8.29). Let Φ be a channel, let π be a probability distribution, assigning probability π_k to a state S_k at the input of the channel, and let $M = \{M_j\}$ be the observable measured at the output of the channel. Denote by $\mathcal{I}_\Phi(\pi, M)$ the Shannon information corresponding to the input probability distribution $\{\pi_k\}$ and transition probability $p(j \mid k) = \operatorname{Tr} \Phi \left[S_k\right] M_j = \operatorname{Tr} S_k \Phi^* \left[M_j\right]$. In order to prove (8.29), it is sufficient to establish the inequality

$$\begin{aligned} \max_{\{\pi, M^1, M^2\}} \mathcal{I}_{\Phi_1 \otimes \Phi_2} \left(\pi, M^1 \otimes M^2\right) \leq & \max_{\{\pi^1, M^1\}} \mathcal{I}_{\Phi_1} \left(\pi^1, M^1\right) \\ & + \max_{\{\pi^2, M^2\}} \mathcal{I}_{\Phi_2} \left(\pi^2, M^2\right) \end{aligned} \tag{8.30}$$

In terms of the classical mutual information

$$\mathcal{I}_\Phi(\pi, M) = I(X; Y),$$

where X is the input random variable, taking values k, and Y is the output random variable, taking values j. In order to prove (8.30), consider the states S_k in the Hilbert space $\mathcal{H}_1 \otimes \mathcal{H}_2$ of the channel $\Phi_1 \otimes \Phi_2$, with a product observable $M^1 \otimes M^2$. In this case, the conditional probability is

$$p\left(j_1, j_2 \mid k\right) = \operatorname{Tr} S_k \left(\Phi_1^* \left[M_{j_1}^1\right] \otimes \Phi_2^* \left[M_{j_2}^2\right]\right) = p^1 \left(j_1 \mid j_2, k\right) p^2 \left(j_2 \mid k\right), \tag{8.31}$$

where

$$p^1 \left(j_1 \mid j_2, k\right) = \operatorname{Tr} S_{j_2,k}^1 \Phi_1^* \left[M_{j_1}^1\right], \quad p^2 \left(j_2 \mid k\right) = \operatorname{Tr} S_k^2 \Phi_2^* \left[M_{j_2}^2\right]$$

and

$$S_k^2 = \operatorname{Tr}_1 S_k, \quad S_{j_2,k}^1 = \frac{\operatorname{Tr}_2 S_k \left(I \otimes \Phi_2^* \left[M_{j_2}^2\right]\right)}{\operatorname{Tr} S_k \left(I \otimes \Phi_2^* \left[M_{j_2}^2\right]\right)}$$

Here, Tr_s denotes the partial trace in the sth subsystem ($s = 1, 2$) in $\mathcal{H}_1 \otimes \mathcal{H}_2$.
We then have

$$I\left(X; Y_1 Y_2\right) = H\left(Y_1 Y_2\right) - H\left(Y_1 Y_2 \mid X\right)$$

where $H(\cdot), H(\cdot \mid \cdot)$ are the entropy and conditional entropy, respectively, of the random variables describing the common classical input (X) and the outputs (Y_1, Y_2) of the two channels. By the subadditivity of the classical entropy,

$$H(Y_1Y_2) \leq H(Y_1) + H(Y_2)$$

On the other hand,

$$H(Y_1Y_2 \mid X) = H(Y_1 \mid Y_2X) + H(Y_2 \mid X).$$

Combining, we get

$$I(X; Y_1Y_2) \leq I(XY_2; Y_1) + I(X; Y_2),$$

which, due to (8.31), amounts to

$$\mathcal{I}_{\Phi_1 \otimes \Phi_2}\left(\pi, M^1 \otimes M^2\right) \leq \mathcal{I}_{\Phi_1}\left(\pi^1, M^1\right) + \mathcal{I}_{\Phi_2}\left(\pi^2, M^2\right)$$

where π^1 is the probability distribution that assigns a probability $\pi_k p^2(j_2 \mid k)$ to the state $S^1_{j_2,k}$, and π^2 is the probability distribution that assigns probability π_k to the state S^2_k. Taking the maximum over π and S gives (8.30).

10.8.5 8.3.2 A Hierarchy of Additivity Properties

An important characteristic of a quantum channel Φ, which already appeared in Section 8.2, is the minimal output entropy

$$\check{H}(\Phi) = \min_{S \in \mathfrak{S}(\mathcal{H})} H(\Phi[S]). \tag{8.32}$$

The corresponding hypothetical additivity property is

$$\check{H}(\Phi_1 \otimes \Phi_2) = \check{H}(\Phi_1) + \check{H}(\Phi_2). \tag{8.33}$$

By the concavity of the entropy, the minimum in (8.32) is attained on a pure state $S \in \operatorname{extr} \mathfrak{S}(\mathcal{H})$. Therefore, the classical analog of the quantity $\check{H}(\Phi)$ is additive, because any pure state of a composite classical system is a product of the pure states of the subsystems. Instead, for a tensor product $\mathcal{H}_1 \otimes \mathcal{H}_2$ describing a composite quantum system, one has

$$\operatorname{extr} \mathfrak{S}(\mathcal{H}_1 \otimes \mathcal{H}_2) \supsetneqq \operatorname{extr} \mathfrak{S}(\mathcal{H}_1) \times \operatorname{extr} \mathfrak{S}(\mathcal{H}_2), \tag{8.34}$$

due to the presence of the entangled states. Hence, there is no obvious reason for the additivity (8.33) in the quantum case.

Clearly, inequality $\leq$ always holds in (8.33). This implies that (8.33) obviously holds for channels with zero minimal output entropy, i.e., those for which there exists a pure output state, such as an ideal channel.

Exercise 8.13 Prove the following statement: the additivity properties (8.22) and (8.33) are equivalent for a pair of covariant channels satisfying the conditions of Proposition 8.8. Hint: use the fact that the tensor product of the irreducible representations of two symmetry groups G_1, G_2 is an irreducible representation of the group $G_1 \times G_2$.

Exercise 8.14 Consider the minimal entropy gain

$$\check{G}(\Phi) = \min_{S \in \mathfrak{S}(\mathcal{H})} (H(\Phi[S]) - H(S)).$$

Use the superadditivity property (7.21) to show that it is additive, i.e.,

$$\check{G}\left(\Phi_1 \otimes \Phi_2\right) = \check{G}\left(\Phi_1\right) + \check{G}\left(\Phi_2\right). \tag{8.35}$$

Now consider the convex hull $\hat{H}_\Phi(S)$ of the output entropy, defined by relation (8.13). The hypothetical superadditivity property for this quantity is formulated in the following way: for arbitrary state $S_{12} \in \mathfrak{S}\left(\mathcal{H}_1 \otimes \mathcal{H}_2\right)$ and channels Φ_1, Φ_2

$$\hat{H}_{\Phi_1 \otimes \Phi_2}\left(S_{12}\right) \geq \hat{H}_{\Phi_1}\left(S_1\right) + \hat{H}_{\Phi_2}\left(S_2\right), \tag{8.36}$$

where S_1, S_2 are the partial traces of S_{12} in $\mathcal{H}_1, \mathcal{H}_2$.
This superadditivity property is maximal in the sense that its validity for a pair of channels Φ_1, Φ_2 implies all the other additivity properties for this pair of channels.

Proposition 8.15. For two given channels Φ_1, Φ_2 the superadditivity property (8.36) implies both the additivity of the minimal output entropy (8.33) and of the χ-capacity (8.22).

Proof. Indeed, let S_{12}^0 be a minimizer for $H\left(\left(\Phi_1 \otimes \Phi_2\right)\left[S_{12}\right]\right)$. In this case,

$$\begin{aligned}\check{H}\left(\Phi_1 \otimes \Phi_2\right) &= H\left(\left(\Phi_1 \otimes \Phi_2\right)\left[S_{12}^0\right]\right) = \hat{H}_{\Phi_1 \otimes \Phi_2}\left(S_{12}^0\right) \\ &\geq \hat{H}_{\Phi_1}\left(S_1^0\right) + \hat{H}_{\Phi_2}\left(S_2^0\right) \geq \check{H}\left(\Phi_1\right) + \check{H}\left(\Phi_2\right),\end{aligned}$$

from which (8.33) follows. On the other hand, (8.36) and the subadditivity of the quantum entropy imply

$$\begin{aligned}&H\left(\left(\Phi_1 \otimes \Phi_2\right)\left[S_{12}\right]\right) - \hat{H}_{\Phi_1 \otimes \Phi_2}\left(S_{12}\right) \\ &\quad \leq H\left(\left(\Phi_1 \otimes \Phi_2\right)\left[S_{12}\right]\right) - \hat{H}_{\Phi_1}\left(S_1\right) - \hat{H}_{\Phi_2}\left(S_2\right) \\ &\quad \leq \left[H\left(\Phi_1\left[S_1\right]\right) - \hat{H}_{\Phi_1}\left(S_1\right)\right] + \left[H\left(\Phi_2\left[S_2\right]\right) - \hat{H}_{\Phi_2}\left(S_2\right)\right]\end{aligned} \tag{8.37}$$

By using (8.12), we get

$$C_\chi\left(\Phi_1 \otimes \Phi_2\right) \leq C_\chi\left(\Phi_1\right) + C_\chi\left(\Phi_2\right),$$

i. e., (8.22). □

Moreover, the property (8.36) is closely related to the additivity of the χ-capacity with input constraints. Let F be a positive operator in the input Hilbert space $\mathcal{H}$ of the channel, and let E be a positive constant. Consider the χ-capacity under the linear constraint $\operatorname{Tr} SF \leq E$ on the input state S, i.e.,

$$C_\chi(\Phi, F, E) = \max_{S:\operatorname{Tr} SF \leq E}\left[H(\Phi[S]) - \hat{H}_\Phi(S)\right]. \tag{8.38}$$

Exercise 8.16 Assume that we have two channels Φ_1, Φ_2 with corresponding constraint operators F_1, F_2. Then inequality (8.36), along with (8.12), implies

$$\begin{aligned}C_X\left(\Phi_1 \otimes \Phi_2, F_1 \otimes I_2 + I_1 \otimes F_2, E\right) = \max_{E_1+E_2=E}[&C_X\left(\Phi_1, F_1, E_1\right) \\ &+C_X\left(\Phi_2, F_2, E_2\right)].\end{aligned} \tag{8.39}$$

The property of superadditivity (8.36) is closely related to the following hypothetical property of the entanglement of formation: let $\mathcal{H}_1 = \mathcal{H}_1^A \otimes \mathcal{H}_1^B$ and $\mathcal{H}_2 = \mathcal{H}_2^A \otimes \mathcal{H}_2^B$, and let S_{12}^{AB} be a state in $\mathcal{H}_1 \otimes \mathcal{H}_2$; then

$$E_F\left(S_{12}^{AB}\right) \geq E_F\left(S_1^{AB}\right) + E_F\left(S_2^{AB}\right), \tag{8.40}$$

where the entanglement of formation is defined relative to the subdivision $A \mid B$. Namely, if property (8.40) would hold for all states S_{12}^{AB}, this would imply (8.36) for all channels Φ_1, Φ_2 and all states S_{12}, while if (8.36) would hold for all states S_{12} and partial trace channels, (8.40) would hold for all states S_{12}^{AB}.

The most complete conditional result in this direction is the following,

Theorem 8.17. The conjectured properties (8.33), (8.22), (8.23), and (8.36) are globally equivalent in the following sense: assuming that one of them holds for all channels Φ_1, Φ_2, any other is also true for all channels. Moreover, they are globally equivalent to the superadditivity of the entanglement of formation (8.40) and to the additivity of the χ-capacity with arbitrary input constraints.

When (parts of this) theorem were proved, there was hope that it would help to reduce the proof of more complicated global conjectures, such as additivity of the χ-capacity or superadditivity of entanglement of formation to a seemingly less complicated one - the global additivity of the minimal output entropy. However, with the disproof of the last conjecture, this theorem implies that none of the additivity properties holds globally (see Section 8.4 for more detail).

We will not consider the proof of this theorem here; instead we discuss some restricted classes of channels for which the maximal property (8.36) can be proved.

10.8.6 8.3.3 Some Entropy Inequalities

Here, we obtain inequalities that allow us to prove, in some cases, the superadditivity of the convex hull (8.36) and hence the additivity of the minimal output entropy (8.33) and of the χ-capacity (8.22).

Consider a state S and a nonideal measurement, described by a collection of operators A_k that satisfy the normalization condition $\sum_k A_k^* A_k = I$, so that an outcome k occurs with probability $\pi_k = \operatorname{Tr} S A_k^* A_k$, resulting in a posterior state of the system $S_k = A_k S A_k^* / \pi_k$. The entropies of the initial and posterior states are related by the Lindblad-Ozawa inequality

$$H(S) \geq \sum_k \pi_k H\left(S_k\right). \tag{8.41}$$

Proof. To prove this, take $\mathcal{H} = \mathcal{H}_1$ and consider a purification $|\psi\rangle$ of the state S in $\mathcal{H}_1 \otimes \mathcal{H}_2$. Then

$$\pi_k S_k = \operatorname{Tr}_{\mathcal{H}_2} \left(A_k \otimes I\right) |\psi\rangle\langle\psi| \left(A_k \otimes I\right)^*,$$

and $S_2 = \operatorname{Tr}_{\mathcal{H}_1} |\psi\rangle\langle\psi| = \sum_k \pi_k S_2^k$, where

$$\pi_k S_2^k = \operatorname{Tr}_{\mathcal{H}_1} \left(A_k \otimes I\right) |\psi\rangle\langle\psi| \left(A_k \otimes I\right)^*.$$

Using Theorem 3.10 twice and applying the concavity of the quantum entropy,

$$H(S) = H\left(S_2\right) = H\left(\sum_k \pi_k S_2^k\right) \geq \sum_k \pi_k H\left(S_2^k\right) = \sum_k \pi_k H\left(S_k\right).$$

□

A particular case of the above is the following inequality for composite systems. Let S_{12} be a state of the composite system 12 and let $\{|e_k^2\rangle\}$ be an orthonormal basis in $\mathcal{H}_2$. Taking $A_k = I_1 \otimes |e_k^2\rangle \langle e_k^2|$, one obtains

$$H\left(S_{12}\right) \geq \sum_k \pi_k H\left(S_1^k\right), \tag{8.42}$$

where $\pi_k S_1^k = \langle e_k^2| S_{12} |e_k^2\rangle$. This can be used to prove a particular case of the additivity conjecture.

Proposition 8.18. The maximal property (8.36) holds in the case where $\Phi_1 = \Phi$ is an arbitrary channel in $\mathcal{H}_1$ and $\Phi_2 = \mathrm{Id}_2$ is the ideal channel in $\mathcal{H}_2$.

Proof. Since $\hat{H}_{\mathrm{Id}}(S) \equiv 0$, according to Exercise 8.3, we have to prove that

$$\hat{H}_{(\Phi\otimes I\ \mathrm{d}_2)}(S_{12}) \geq \hat{H}_\Phi(S_1). \tag{8.43}$$

Let $S_{12} = \sum_i \pi_i S_{12}^i$ be the optimal decomposition, i. e.,

$$\hat{H}_{(\Phi\otimes \mathrm{Id}_2)}(S_{12}) = \sum_i \pi_i H\left((\Phi\otimes \mathrm{Id}_2)\left[S_{12}^i\right]\right).$$

By using (8.42), we obtain

$$\sum_i \pi_i H\left((\Phi\otimes \mathrm{Id}_2)\left[S_{12}^i\right]\right) \geq \sum_{ik} \pi_i\pi_{ik} H\left(\Phi\left[S_1^{ik}\right]\right) \tag{8.44}$$

where $\pi_{ik} S_1^{ik} = \langle e_k^2| S_{12}^i |e_k^2\rangle$. Now, we have the decomposition of S_1 into the states S_1^{ik} with probabilities $\pi_i\pi_{ik}$ for channel Φ. Hence, the right-hand side of (8.44) is greater than or equal to $\hat{H}_\Phi(S_1)$. □

Proposition 8.19. The maximal property (8.36) (and hence the additivity of the minimal output entropy (8.33) and of the χ-capacity (8.22)) holds in the case where $\Phi_1 = \Phi$ is an entanglement-breaking channel (see Section 6.4) and $\Phi_2 = \Psi$ is an arbitrary channel.

Lemma 8.20. Let $\pi_j \geq 0, \sum \pi_j = 1$, and S_1^j, S_2^j be arbitrary states of the systems 1,2 . Then

$$H\left(\sum_j \pi_j S_1^j \otimes S_2^j\right) \geq H\left(\sum_j \pi_j S_1^j\right) + \sum_j \pi_j H\left(S_2^j\right).$$

Proof. We introduce the notation

$$\left(\bar{S}_{12}\right)_\pi = \sum_j \pi_j S_1^j \otimes S_2^j, \quad \left(\bar{S}_1\right)_\pi = \sum_j \pi_j S_1^j$$

Now, using the additivity of the entropy, the inequality can be rewritten as

$$H\left(\left(\bar{S}_{12}\right)_\pi\right) - \sum_j \pi_j H\left(S_1^j \otimes S_2^j\right) \geq H\left(\left(\bar{S}_1\right)_\pi\right) - \sum_j \pi_j H\left(S_1^j\right),$$

which by identity (7.19) is equivalent to

$$\sum_j \pi_j H\left(S_1^j \otimes S_2^j; \left(\bar{S}_{12}\right)_\pi\right) \geq \sum_j \pi_j H\left(S_1^j; \left(\bar{S}_1\right)_\pi\right).$$

However, the last inequality follows from the monotonicity of the relative entropy (with respect to partial trace in the second system). □

Proof. Coming back to the proof of the proposition, assume that Φ is an entanglement-breaking channel, so that $\Phi[S] = \sum_j S_1^j \operatorname{Tr} S M_1^j$, where $\left\{M_1^j\right\}$ is an observable in system 1 . In this case,

$$(\Phi\otimes \mathrm{Id}_2)[S_{12}] = \sum_j p_j S_1^j \otimes S_2^j, \tag{8.45}$$

where $p_j S_2^j = \operatorname{Tr}_{\mathcal{H}_1} S_{12}\left(M_1^j \otimes I_2\right)$ for an arbitrary state S_{12} of the composite system. Taking the partial trace, we obtain, in particular,

$$\Phi\left[S_1\right] = \sum_j p_j S_1^j, \quad S_2 = \sum_j p_j S_2^j. \tag{8.46}$$

If Ψ is an arbitrary channel in system 2,

$$(\Phi \otimes \Psi)\left[S_{12}\right] = \sum_j p_j S_1^j \otimes \Psi\left[S_2^j\right]. \tag{8.47}$$

We have

$$\hat{H}_{\Phi\otimes\Psi}\left(S_{12}\right) = \inf \sum_i \pi_i H\left((\Phi \otimes \Psi)\left[S_{12}^i\right]\right), \tag{8.48}$$

where $S_{12} = \sum_i \pi_i S_{12}^i$ is an arbitrary decomposition. By writing relation (8.45) for S_{12}^i we obtain

$$(\Phi \otimes \mathrm{Id}_2)\left[S_{12}^i\right] = \sum_j p_{ij} S_1^{ij} \otimes S_2^{ij}$$

along with the decompositions

$$S_1 = \sum_i \pi_i S_1^i, \quad S_2 = \sum_{ij} \pi_i p_{ij} S_2^{ij}. \tag{8.49}$$

By using (8.47), the lemma that we just proved, and (8.46), we obtain

$$\begin{aligned} H\left((\Phi \otimes \Psi)\left[S_{12}^i\right]\right) &= H\left(\sum_j p_{ij} S_1^{ij} \otimes \Psi\left[S_2^{ij}\right]\right) \\ &\geq H\left(\sum_j p_{ij} S_1^{ij}\right) + \sum_j p_{ij} H\left(\Psi\left[S_2^{ij}\right]\right) \\ &\geq H\left(\Phi\left[S_1^i\right]\right) + \sum_j p_{ij} H\left(\Psi\left[S_2^{ij}\right]\right) \end{aligned}$$

which in combination with (8.48) and (8.49) implies

$$\hat{H}_{\Phi\otimes\Psi}\left(S_{12}\right) \geq \hat{H}_\Phi\left[S_1\right] + \hat{H}_\Psi\left[S_2\right].$$

□

10.8.7 8.3.4 Additivity for Complementary Channels

Lemma 8.21. If S is a pure state, then it holds for any channel Φ,

$$H(\Phi[S]) = H(\tilde{\Phi}[S]), \tag{8.50}$$

where $\tilde{\Phi}$ is the complementary of Φ. Therefore, if either of the properties (8.36), (8.33) holds for channels Φ_1, Φ_2, the similar property holds for the complementary channels $\tilde{\Phi}_1, \tilde{\Phi}_2$.

Proof. As follows from the definition (6.38) of the complementary channels, the states $\Phi[S]$ and $\tilde{\Phi}[S]$ are partial states of the pure state VSV^*. Hence, by equality (7.30), they have equal entropies.

From (8.50) we conclude

$$\check{H}(\Phi) = \check{H}(\tilde{\Phi}), \quad \hat{H}_\Phi(S) = \hat{H}_{\tilde{\Phi}}(S)$$

for an arbitrary state S, due to the expressions for $\check{H}(\Phi), \hat{H}_\Phi(S)$ in terms of the output entropies for pure input states. Hence, the second statement follows. □

Proposition 8.19 then implies the following.

Corollary 8.22. The maximal property (8.36) (and hence the additivity of the minimal output entropy (8.33) and of the χ-capacity (8.22)) hold in the case where $\Phi_1 = \Phi$ is the channel (6.45), in particular, a dephasing channel, and $\Phi_2 = \Psi$ is an arbitrary channel.

Proposition 8.23. Let Φ_2 be an arbitrary channel. The maximal property (8.36) holds for Φ_1, Φ_2 if Φ_1 is an orthogonal convex sum (see Definition 6.33) of the ideal channel and a channel $\Phi^{(0)}$ such that the maximal property holds for $\Phi^{(0)}$ and Φ_2.

It follows that such a Φ_1 fulfills the additivity of the minimal output entropy (8.33) and of the χ-capacity (8.22), with an arbitrary Φ_2. For example, this holds for the erasure channel, because it is an orthogonal convex sum of the ideal channel and an entanglement-breaking channel for which the property (8.36) was established in Section 8.3.3.

Proof. Denote $\Phi^{(q)} = q\,\mathrm{Id} \oplus (1-q)\Phi^{(0)}$. Now,

$$H\left(\Phi^{(q)}[S]\right) = qH(S) + (1-q)H\left(\Phi^{(0)}[S]\right) + h_2(q),$$

where $h_2(q) = -q\log q - (1-q)\log(1-q)$ is the binary entropy and

$$\hat{H}_{\Phi^{(q)}}(S) = (1-q)\hat{H}_{\Phi^{(0)}}(S) + h_2(q), \tag{8.51}$$

because the minimum in the expression for $\hat{H}_{\Phi^{(0)}}(S)$ is attained for an ensemble of pure states S_j for which $H(S_j) = 0$. For an arbitrary channel Φ_2 we have

$$\Phi^{(q)} \otimes \Phi_2 = q\,(\mathrm{Id} \otimes \Phi_2) \oplus (1-q)\left(\Phi^{(0)} \otimes \Phi_2\right).$$

Then

$$\begin{aligned}\hat{H}_{\Phi^{(q)}\otimes\Phi_2}(S_{12}) &\geq q\hat{H}_{\mathrm{Id}\otimes\Phi_2}(S_{12}) + (1-q)\hat{H}_{\Phi^{(0)}\otimes\Phi_2}(S_{12}) + h_2(q)\\ &\geq q\hat{H}_{\Phi_2}(S_2) + (1-q)\left[\hat{H}_{\Phi^{(0)}}(S_1) + \hat{H}_{\Phi_2}(S_2)\right] + h_2(q),\end{aligned}$$

where we have used the superadditivity of $\hat{H}_{\mathrm{Id}\otimes\Phi_2}(S_{12}), \hat{H}_{\Phi^{(0)}\otimes\Phi_2}(S_{12})$ and the fact that $\hat{H}_{\mathrm{Id}}(S_1) \equiv 0$. By using (8.51), we obtain that the right-hand side is equal to $\hat{H}_{\Phi^{(q)}}(S_1) + \hat{H}_{\Phi_2}(S_2)$. □

Corollary 8.22 implies that Proposition 8.23 holds with the replacement of the ideal channel by its complementary, the completely depolarizing channel.

10.8.8 8.3.5 Nonadditivity of Quantum Entropy Quantities

The quantum Rényi entropy of order $p > 1$ of a density operator S is defined as

$$R_p(S) = \frac{1}{1-p}\log \mathrm{Tr}\, S^p, \tag{8.52}$$

and in the limit $p \to 1$ the quantum Rényi entropies converge uniformly to the von Neumann entropy of a density operator S,

$$\lim_{p\to 1} R_p(S) = -\mathrm{Tr}\, S\log S \equiv H(S).$$

Defining the minimal output Rényi entropy of the channel Φ as

$$\check{R}_p(\Phi) = \min_{S\in\mathfrak{S}(\mathcal{H})} R_p(\Phi[S]),$$

one may ask for an additivity property similar to (8.33), namely,

$$\check{R}_p\left(\Phi_1 \otimes \Phi_2\right) = \check{R}_p\left(\Phi_1\right) + \check{R}_p\left(\Phi_2\right). \tag{8.53}$$

Again, inequality $\leq$ is obvious here. Note that the validity of (8.53) for some specific channels Φ_1, Φ_2 and p close to 1 implies (8.33) for these Φ_1, Φ_2. This raised interest in the problem (8.53) in the hope that its solution could shed light on the additivity problems in quantum information theory.

A counterexample of the transpose-depolarizing channel [243] soon appeared, i. e.,

$$\Phi[S] = \frac{1}{d-1}\left(I - S^T\right), \tag{8.54}$$

for which (8.53) with $\Phi_1 = \Phi_2 = \Phi$ fails to hold for $d = \dim \mathcal{H} \geq 3$ and large enough p.

Exercise 8.24 Prove the complete positivity of the map (8.54) by establishing the Kraus representation

$$\Phi[S] = \frac{1}{2(d-1)} \sum_{j,k=1}^{d} \left(|e_j\rangle\langle e_k| - |e_k\rangle\langle e_j|\right) S \left(|e_k\rangle\langle e_j| - |e_j\rangle\langle e_k|\right), \tag{8.55}$$

where $\{e_j\}$ is an orthonormal basis.

A breakthrough in the negative solution of the global conjecture (8.53) came in 2007. Winter [255] had shown that in very high dimensions there always exist channels for which (8.53) does not hold for any $p > 2$. Next, Hayden [97] proved this for any $1 < p < 2$. Winter showed that the additivity of the Rényi entropy with $p > 2$ breaks for the pair of channels $\Phi, \bar{\Phi}$ (complex conjugate in a fixed basis), where

$$\Phi[S] = \frac{1}{n} \sum_{j=1}^{n} U_j S U_j^* \tag{8.56}$$

is the uniform mixture of unitary evolutions in $\mathcal{H}$ and $n, d = \dim \mathcal{H}$ are large enough. The proof relies upon the two estimates. A simple but efficient upper bound for $\check{R}_p(\Phi \otimes \bar{\Phi})$ is given by the inequality

$$\check{R}_p(\Phi \otimes \bar{\Phi}) \leq R_p(\Phi \otimes \bar{\Phi})[|\Omega\rangle\langle\Omega|] \leq \frac{p}{p-1} \log n, \tag{8.57}$$

where $|\Omega\rangle$ is the maximally entangled vector in the same basis. Indeed,

$$\begin{aligned}
(\Phi \otimes \bar{\Phi})[|\Omega\rangle\langle\Omega|] &= \frac{1}{n^2} \sum_{j,k=1}^{n} \left(U_j \otimes \bar{U}_k\right) |\Omega\rangle\langle\Omega| \left(U_j \otimes \bar{U}_k\right)^* \\
&= \frac{1}{n}|\Omega\rangle\langle\Omega| + \frac{1}{n^2} \sum_{j \neq k} \left(U_j \otimes \bar{U}_k\right) |\Omega\rangle\langle\Omega| \left(U_j \otimes \bar{U}_k\right)^* \\
&\geq \frac{1}{n}|\Omega\rangle\langle\Omega|,
\end{aligned}$$

where in the second equality we used the property $(U \otimes \bar{U})|\Omega\rangle = |\Omega\rangle$ for arbitrary unitary U. It follows that the maximal eigenvalue of the density operator $(\Phi \otimes \bar{\Phi})[|\Omega\rangle\langle\Omega|]$, i. e., its operator norm, is greater than or equal to $\frac{1}{n}$, i.e.,

$$\|(\Phi \otimes \bar{\Phi})[|\Omega\rangle\langle\Omega|]\| \geq \frac{1}{n}. \tag{8.58}$$

Hence,

$$R_p((\Phi\otimes\bar\Phi)[|\Omega\rangle\langle\Omega|]) \le \frac{1}{1-p}\log\left(\frac{1}{n}\right)^p = \frac{p}{p-1}\log n, \tag{8.59}$$

and (8.57) follows.

The next step is to consider random independent unitary operators $U_j, j = 1,\dots,n$, distributed according to the normalized Haar measure on the group of unitaries in $\mathcal{H}$. In this case, the expectation of each term in (8.56) is $\mathrm{E}U_jSU_j^* = I/d$, since it is the only density operator that is invariant under unitary conjugations, and one can expect that $\Phi[S]$ is close to I/d in a probabilistic sense for n large enough. A key ingredient of the proof is the large deviation estimate for the sums of random operators, inspired by the classical Bernstein-Chernoff-Hoeffding inequality, which implies that the probability of the inequality

$$\left\|\Phi[S] - \frac{I}{d}\right\| \le \frac{\varepsilon}{d} \tag{8.60}$$

tends to 1 when $d\to\infty, n\sim d\log d$ (compare this result with Theorem 10.34). From inequality (8.60) it follows that $\|\Phi[S]\| \le \frac{1+\varepsilon}{d}$ and hence

$$\operatorname{Tr}\Phi[S]^p = \operatorname{Tr}\Phi[S]\Phi[S]^{p-1} \le \|\Phi[S]\|^{p-1}\operatorname{Tr}\Phi[S] \le \left(\frac{1+\varepsilon}{d}\right)^{p-1} \tag{8.61}$$

so that

$$\check R_p(\Phi) = -\frac{1}{p-1}\max_{S\in\mathfrak{S}(\mathcal{H})}\log\operatorname{Tr}\Phi[S]^p \ge \log\frac{d}{1+\varepsilon}.$$

This implies the probabilistic lower bound

$$\lim_{d\to\infty}\mathrm{P}\left\{\check R_p(\Phi) \ge \log\frac{d}{1+\varepsilon}\right\} = 1$$

for random Φ of the form (8.56), with $n\sim d\log d$. Taking into account that $\check R_p(\Phi) = \check R_p(\bar\Phi)$, and comparing with (8.57), one sees that with probability close to 1 ,

$$\check R_p(\Phi\otimes\bar\Phi) \le \frac{p}{p-1}\log n < 2\log\left(\frac{d}{1+\varepsilon}\right) \le \check R_p(\Phi) + \check R_p(\bar\Phi)$$

if $p>2, d\to\infty, n\sim d\log d$.

The estimate (8.58) can be generalized to an arbitrary channel Φ as follows.

Lemma 8.25. Let Φ be a quantum channel from A to B which has the Kraus representation with d_E components, and let $|\Omega_{AA}\rangle$ be the maximally entangled vector in $\mathcal{H}_A\otimes\mathcal{H}_A$. Then

$$\left\|(\Phi\otimes\bar\Phi)\left[|\Omega_{AA}\rangle\langle\Omega_{AA}|\right]\right\| \ge \frac{d_A}{d_Bd_E} \equiv D. \tag{8.62}$$

Proof. We have

$$(\Phi\otimes\bar\Phi)\left[|\Omega_{AA}\rangle\langle\Omega_{AA}|\right] = \sum_{r,S=1}^{d_E}\left(V_r\otimes\bar V_S\right)|\Omega_{AA}\rangle\langle\Omega_{AA}|\left(V_r\otimes\bar V_S\right)^*$$

and

$$\langle\Omega_{BB}|\left(X\otimes Y\right)|\Omega_{AA}\rangle = \frac{1}{d_Ad_B}\operatorname{Tr}Y^\top X,$$

for any operators X, Y acting from $\mathcal{H}_A$ to $\mathcal{H}_B$.

By using these identities, we have

$$\begin{aligned}
\left\|(\Phi\otimes\bar{\Phi})\left[|\Omega_{AA}\rangle\langle\Omega_{AA}|\right]\right\| &\geq \langle\Omega_{BB}|\,(\Phi\otimes\bar{\Phi})\left[|\Omega_{AA}\rangle\langle\Omega_{AA}|\right]|\Omega_{BB}\rangle \\
&= \sum_{r,s=1}^{d_E}\left|\langle\Omega_{BB}|\left(V_r\otimes\bar{V}_s\right)|\,\Omega_{AA}\right\rangle|^2 \\
&= \frac{1}{d_A d_B}\sum_{r,s=1}^{d_E}|\mathrm{Tr}\,V_s^*V_r|^2 \\
&\geq \frac{1}{d_A d_B}\sum_{r=1}^{d_E}|\mathrm{Tr}\,V_r^*V_r|^2 \\
&\geq \frac{1}{d_A d_B d_E}\left|\mathrm{Tr}\sum_{r=1}^{d_E}V_r^*V_r\right|^2 \\
&= \frac{1}{d_A d_B d_E}|\mathrm{Tr}\,I_A|^2 = \frac{d_A}{d_B d_E}
\end{aligned}$$

where the Cauchy-Schwarz inequality was used. □

This estimate is one part of proving that in very high dimensions there exist channels that violate the additivity of the minimal Rényi entropies for all $p>1$ (Winter and Hayden [100]). To this end one considers the pair of channels $\Phi,\bar{\Phi}$, where Φ is a generic channel given by a general open system representation (6.22) with the random unitary evolution operator uniformly distributed over the group of unitaries. Moreover, $d_B=d_E=d\longrightarrow\infty$, and $d_A\sim d^{1+1/p}$ so that $D\sim d^{1/p-1}$. The upper bound

$$\check{R}_p(\Phi\otimes\bar{\Phi})\leqslant\log d \tag{8.63}$$

then follows from (8.62) similarly to (8.59).

The most difficult part of the proof is the probabilistic lower estimate

$$\lim_{d\to\infty}\mathrm{P}\left\{\check{R}_p(\Phi)\geq\log d-c\right\}=1, \tag{8.64}$$

which is also based on a large deviation phenomenon, namely, the measure concentration, used to establish the concentration of the output entropy. This is closely related to the early observations that, given a random uniformly distributed pure state vector $|\psi_{AB}\rangle$ of a composite system AB, the entropy of the partial state S_B of the smaller
system tends to its maximal value $\log d_B$ as $d_A\to\infty$, and hence S_B becomes almost chaotic while $|\psi_{AB}\rangle$ is almost maximally entangled.

The relations (8.63) and (8.64), together with $\check{R}_p(\Phi)=\check{R}_p(\Phi)$, imply that

$$\check{R}_p(\Phi\otimes\bar{\Phi})<\check{R}_p(\Phi)+\check{R}_p(\bar{\Phi})$$

with probability close to 1 .

Notably, these estimates for $p>1$ are not strong enough to imply the violation of additivity for $p\to1$ and the case of the minimal von Neumann entropy requires additional efforts which were accomplished by Hastings [93]. His original argument was improved and simplified in subsequent works [76], [34], and [13]. Following [34], consider the random unitary evolution channels with $d_B=d\longrightarrow\infty$, and $d_E=d_A\gg d$. In this case $D=1/d$, and Lemma 8.25 implies that the density operator $(\Phi\otimes\bar{\Phi})\left[|\Omega_{AA}\rangle\langle\Omega_{AA}|\right]$, acting in the space of dimensionality d^2, has an eigenvalue greater than or equal to $1/d$.

Exercise 8.26 Let $P=[\lambda_1,\ldots,\lambda_{d^2}]$ run through all probability distributions, such that $\lambda_1\geq1/d$. Then

$$\max_P H(P) = \log d + \frac{d-1}{d}\log(d+1) \leq 2\log d - \frac{\log(d/\mathrm{e})}{d},$$

where the maximum is attained for the distribution P such that $\lambda_1 = 1/d$ and all other probabilities are equal to $1/d(d+1)$.

It follows that

$$\check{H}(\Phi \otimes \bar{\Phi}) \leq H\left((\Phi \otimes \bar{\Phi})\left[|\Omega_{AA}\rangle\langle\Omega_{AA}|\right]\right) \leq 2\log d - \frac{\log(d/\mathrm{e})}{d}, \tag{8.65}$$

which gives the "easier" part of the argument. The difficult part is again the probabilistic estimate, exploring at full strength the phenomenon of entropy concentration,

$$\mathbf{P}\left\{\check{H}(\Phi) > \log d - \frac{C}{d}\right\} > 0$$

for $d, d_A/d$ large enough, where C is a positive constant. Together with (8.65), this proves the existence of channels violating the additivity of the minimal von Neumann entropy.

Although, when combined with Theorem 8.17, this gives a definite negative answer to all global additivity conjectures, including the one which concerns the χ-capacity, several important issues remain open. All the above proofs use the technique of random unitary operators or random states and, as such, are not constructive. They only provide evidence for existence of counterexamples but do not allow us to actually produce them. Attempts at providing estimates for the dimensions in which
nonadditivity can happen have so far led to overwhelmingly high values. The detailed estimates made in [76] gave $d \approx 3.9\times10^4, d_A \approx 7.8\times10^{32}$, breaking the additivity by a quantity of the order of 10^{-5}. While this does not exclude the possibility of better estimates, perhaps to be based on a different (but yet unknown) approach, it casts doubt on finding concrete counterexamples by computer simulation of random unitary channels. It remains a mystery what happens in realistic dimensions. Perhaps, for some unknown reason, the additivity still holds generically or its violation is so tiny that it cannot be caught by numerical simulations.

From this point of view, the following explicit construction is of interest. Following [88], we shall consider an explicit example of a simple channel closely related to (8.54), for which the minimal Rényi entropies are nonadditive for all $p > 2$ and sufficiently large d. This more recent explicit construction thus achieves the same goal as the first Winter proposal (8.56). However, it is not clear if it could be extended to the most interesting range $p \geq 1$.

Exercise 8.27 By using formula (6.42) and the Kraus representation (8.55), show that the complementary channel of (8.54) is

$$\tilde{\Phi}[S] = \frac{2}{(d-1)} P_-\,(S \otimes I_2)\,P_- \tag{8.66}$$

where $P_- = \frac{I_{12}-F}{2}$ is the projector onto the antisymmetric subspace $\mathcal{H}_-$of $\mathcal{H}\otimes\mathcal{H}$, which has dimensionality $\frac{d(d-1)}{2}$, and F is the flip operator acting as

$$F\,(|\psi_1\rangle \otimes |\psi_2\rangle) = |\psi_2\rangle \otimes |\psi_1\rangle \tag{8.67}$$

By Lemma 8.21, this channel shares the additivity properties with the channel (8.54).
Now consider the completely positive map $\frac{(d-1)}{2}\tilde{\Phi}^*$, where $\tilde{\Phi}^*$ is the dual to the channel (8.66), i. e.,

$$S_{12} \longrightarrow \frac{(d-1)}{2}\tilde{\Phi}^*\left[S_{12}\right] = \mathrm{Tr}_2\, P_- S_{12} P_- \tag{8.68}$$

Its restriction to operators with support in the subspace $\mathcal{H}_-$is trace-preserving and hence it is a channel, which we denote Φ_-. For this channel, the input dimensionality is $\dim \mathcal{H}_- = \frac{d(d-1)}{2}$, while the output dimensionality is d and the environment dimensionality also is d, because (8.68) involves the partial trace with respect to the second copy of $\mathcal{H}$. Thus, we have $d_A = \frac{d(d-1)}{2}, d_B = d_E = d$, whence $D = \frac{(d-1)}{2d}$ in (8.62), so that

$$\operatorname{Tr}(\Phi \otimes \bar{\Phi}) \left[|\Omega_{AA}\rangle \langle \Omega_{AA}|\right]^p \geq \left\|(\Phi \otimes \bar{\Phi}) \left[|\Omega_{AA}\rangle \langle \Omega_{AA}|\right]\right\|^p \geq D^p$$

and

$$\check{R}_p(\Phi \otimes \bar{\Phi}) \leq \frac{p}{p-1} \log D. \tag{8.69}$$

The channel (8.68) breaks the additivity of the quantum Rényi entropies for $p > 2$.

Proposition 8.28. For any $p > 2$ and $d > \left(1 - 2^{2/p-1}\right)^{-1}$

$$\check{R}_p \left(\Phi_- \otimes \Phi_-\right) < \check{R}_p \left(\Phi_-\right) + \check{R}_p \left(\bar{\Phi}_-\right).$$

Proof. Let us show that

$$\check{R}_p \left(\Phi_-\right) = 1. \tag{8.70}$$

Let $S_{12} = |\psi_{12}\rangle \langle \psi_{12}|$ be a pure input state of the channel (8.68), where the vector $|\psi_{12}\rangle \in \mathcal{H}_-$has the Schmidt decomposition $|\psi_{12}\rangle = \sum_{j=1}^d \sqrt{\lambda_j} |e_j \otimes h_j\rangle$. From the definition (8.68) of the channel,

$$\Phi_- \left[S_{12}\right] = S_1 = \sum_{j=1}^d \lambda_j |e_j\rangle \langle e_j|.$$

We have

$$\begin{aligned}
\lambda_j &= |\langle \psi_{12} \mid e_j \otimes h_j \rangle|^2 \\
&\leq \langle e_j \otimes h_j| P_- |e_j \otimes h_j\rangle \\
&= \frac{1}{2} \langle e_j \otimes h_j| \left(I_{12} - F\right) |e_j \otimes h_j\rangle \\
&= \frac{1}{2} \left(1 - |\langle e_j \mid h_j \rangle|^2\right) \leq \frac{1}{2},
\end{aligned}$$

with equality in the last inequality if $\langle e_j \mid h_j \rangle = 0$. Therefore,

$$\|\Phi_- \left[S_{12}\right]\| = \max_j \lambda_j \leq \frac{1}{2}.$$

Hence, similar to (8.61),

$$\operatorname{Tr} \Phi_- \left[S_{12}\right]^p = \operatorname{Tr} \Phi_- \left[S_{12}\right] \Phi_- \left[S_{12}\right]^{p-1} \leq \|\Phi_- \left[S_{12}\right]\|^{p-1} \operatorname{Tr} \Phi_- \left[S_{12}\right] \leq \left(\frac{1}{2}\right)^{p-1}$$

and $R_p \left(\Phi_- \left[S_{12}\right]\right) = \frac{1}{1-p} \log \operatorname{Tr} \Phi_- \left[S_{12}\right]^p \geq 1$. Equality is attained for $|\psi_{12}\rangle = \frac{1}{\sqrt{2}}(|e\rangle \otimes |h\rangle - |h\rangle \otimes |e\rangle)$, where $\langle e \mid h \rangle = 0$. This proves (8.70).

Now, (8.69) together with $\Phi = \bar{\Phi}$ implies

$$\check{R}_p \left(\Phi_- \otimes \Phi_-\right) \leq \frac{p}{p-1} \log \frac{(d-1)}{2d} < 2 = \check{R}_p \left(\Phi_-\right) + \check{R}_p \left(\bar{\Phi}_-\right),$$

provided p, d satisfy the conditions of the proposition. □

10.8.9 8.4 Notes and References

1. The memoryless channel model is the simplest, yet is basic in information theory. Already for this case, the coding theorems are not at all trivial. At the same time they give a basis for considering more complicated and realistic scenarios, taking into account memory effects. Moreover, the effects of entanglement are demonstrated in the memoryless case in a most spectacular way. Therefore, in our presentation throughout the book we concentrate on the memoryless configurations. Proposition 8.2, proved in the paper [114], was later generalized to memory channels by Kretschmann and Werner [159]. A generalization to arbitrary channels in the spirit of Han and Verdú's information spectrum approach was given by Hayashi and Nagaoka [96], [95].

2. The fruitful connection between the χ-capacity and the relative entropy, in particular the maximal distance property, was observed by Schumacher and Westmoreland [202].

3. One of the first mentions of the additivity problem was in the paper of Bennett, Fuchs, and Smolin [26]. The formulation in terms of the four capacities was given by Bennett and Shor [27]. Remarkably, as shown by Shor [217], there is an intermediate capacity, which is obtained by allowing adaptive measurement on the output, and which lies strictly between $C_{1,1}$ and $C_{1,\infty}$ for the "lifted trines" channel.

Theorem 8.17 consists of several implications, some of which are individual, i. e., hold for any fixed pair of channels, while others only hold globally, e. g., "if the minimal output entropy is additive for all channels, so is the (constrained) χ-capacity." Matsumoto, Shimono, and Winter [176] observed the relation between a constrained version of the χ-capacity and the entanglement of formation. Audenaert and Braunstein [15] demonstrated the relevance of the methods of convex analysis, while the most profound global implications were established by Shor, who developed an ingenious extension construction that allows one to strengthen the individual channel's properties. See the paper of Shor [218] for a detailed account as well as for further references. Additional information on the equivalences of various additivity properties can be found in Chapter 9 of Hayashi's book [95]. The fact that global validity of the property (8.23) implies additivity (8.22) for all pairs of channels Φ_1, Φ_2 (and a similar implication for the minimal output entropy) was proved by Fukuda and Wolf [77].

The relation between the additivity properties of complementary channels was noticed and studied by Holevo [118] and by King, Matsumoto, Natanson, and Ruskai [152]. Proposition 8.23 is proved in the paper of Holevo and Shirokov [129], where a mathematical description was given to the channel extension construction, and the superadditivity conjecture (8.36) and its equivalence to the additivity of constrained χ-capacity were studied systematically.

The Lindblad-Ozawa inequality was established in its final form in [183]. The validity of the additivity conjecture for entanglement-breaking channels was established by Shor [215]. Other notable results include King's proofs of conjectures (8.22) and (8.33) for unital qubits [150] and depolarizing channels, as well as their complementary channels [118], [152]. Most of these results can be derived by proving the additivity of the minimal output Renýi entropies (8.53) for all values of p. A significant role in these proofs is played by the Lieb-Thirring inequality (see [31], Section X.2). For a detailed account of these and other partial results on the additivity problem, see the survey [119].

The counterexample of a transpose-depolarizing channel was proposed by Werner and Holevo [243]. A breakthrough came with the results of Winter [255] and Hayden [97], who showed that the additivity of the minimal Renýi entropy with parameter values $p > 2$ and $1 < p \leq 2$, correspondingly, does not hold in sufficiently high dimensions. The phenomenon of entropy concentration was explored in [99], basing on a noncommutative generalization of the Bernstein-Chernoff-Hoeffding inequality. Basing himself on the methods of these works,

Hastings [93] considered mixtures of random unitary operators and sketched a proof of the violation of additivity for the minimal von Neumann entropy for large $n, n/d$. By Theorem 8.17, this implies the existence of counterexamples to all forms of the additivity, as well as to equality (8.24), as follows from [77]. The original argument of Hastings was improved and simplified in the subsequent works of Fukuda, King, and Moser [76] and Brandão and M. Horodecki [34]. Aubrun, Szarek, and E. Werner [13] pointed out a profound connection of these results to Dvoretzky-Milman's theorem in the asymptotic theory of finite-dimensional Banach spaces. The constructive counterexample to the additivity of minimum output Rényi entropy of quantum channels for $p > 2$ is due to Grudka, M. Horodecky, and Pankowski [88].

An important corollary of these negative results is that, in general, the classical capacity $C(\Phi) \neq C_\chi(\Phi)$. By definition, $C\left(\Phi^{\otimes n}\right) = nC(\Phi)$. However, whether the classical capacity $C(\Phi)$ can be nonadditive for a pair of different quantum channels Φ_1, Φ_2 remains an open question. Further discussion of the additivity problem can be found in the books of Aubrun and Szarek [12] and of Watrous [240].

10.9 9 Entanglement-Assisted Classical Communication

10.9.1 9.1 The Gain of Entanglement Assistance

The construction of the superdense coding protocol (Section 3.3.3) allows for generalization to the case of a nonideal channel Φ between arbitrary finite-dimensional quantum systems A and A'. Consider the following protocol of the classical information transmission through the channel Φ. Systems A (transmitter) and B (receiver) share an entangled (pure) state S_{AB}, which is distributed to them with a procedure of the kind described in Section 3.2.1. We shall assume that $\dim \mathcal{H}_A \leq \dim \mathcal{H}_B$. System A does some encoding of classical messages i, arriving with probabilities π_i, into operations (channels) $\mathcal{E}_A^i$ acting in $\mathcal{H}_A$. These operations are applied by A to its part of the state S_{AB}, so that the state of the system AB is transformed into $\left(\mathcal{E}_A^i \otimes \mathrm{Id}_B\right)[S_{AB}]$. After that, A sends its part of this state through the channel Φ, thus driving the whole system AB into the state $\left(\Phi \circ \mathcal{E}_A^i \otimes \mathrm{Id}_B\right)[S_{AB}]$, accessible to B. Next, B makes a measurement in the space $\mathcal{H}_{A'B}$ in order to extract the classical information. In fact, block encoding is allowed, so that the whole of this description refers to the nth tensor degree of $\mathcal{H}_{A'B}$. We are interested in the classical capacity of this protocol, which is called the entanglement-assisted classical capacity of the channel Φ.

The maximum over measurements of B can be evaluated using the coding theorem, Theorem 5.4, for the classical capacity. First, we introduce the quantity

$$C_{ea}^{(1)}(\Phi) = \sup_{\pi_i, \mathcal{E}_A^i, S_{AB}^i} \chi\left(\{\pi_i\}; \left(\Phi \otimes \mathrm{Id}_B\right)\left[S_{AB}^i\right]\right), \tag{9.1}$$

which takes into account measurements in the system $A'B$. Using the channel n times and allowing arbitrary collective (entangled) measurement on B 's side, one gets

$$C_{ea}^{(n)}(\Phi) = C_{ea}^{(1)}\left(\Phi^{\otimes n}\right) \tag{9.2}$$

Now, the full entanglement-assisted classical capacity is

$$C_{ea}(\Phi) = \lim_{n\to\infty} \frac{1}{n} C_{ea}^{(1)}\left(\Phi^{\otimes n}\right). \tag{9.3}$$

The following theorem gives a simple "one-letter" expression for $C_{ea}(\Phi)$ in terms of quantum mutual information.

Theorem 9.1 (Bennett, Shor, Smolin, and Thapliyal [28]). The entanglement-assisted classical capacity of the channel Φ is equal to

$$C_{ea}(\Phi) = \max_{S_A} I\left(S_A, \Phi\right) = \max_{S_A} \left[H\left(S_A\right) + H\left(\Phi\left[S_A\right]\right) - H\left(S_A; \Phi\right)\right]. \tag{9.4}$$

The proof of this theorem will be given in the following sections. Here, we wish to compare entanglement-assisted and (unassisted) classical capacities.

Example 9.2. Consider the quantum erasure channel Φ_p. We have

$$H\left(\Phi_p\left[S_A\right]\right) = (1-p)H\left(S_A\right) + h_2(p)$$

Using the fact that the complementary channel $\tilde{\Phi}_p = \Phi_{1-p}$ (see Exercise 6.35) together with Definition 7.28 of the entropy exchange, we have $H\left(S_A; \Phi\right) = H\left(\tilde{\Phi}\left[S_A\right]\right) = pH\left(S_A\right) + h_2(p)$. Hence,

$$I\left(S_A, \Phi_p\right) = H\left(S_A\right) + (1-p)H\left(S_A\right) - pH\left(S_A\right) = 2(1-p)H\left(S_A\right)$$

whence $C_{ea}\left(\Phi_p\right) = 2(1-p)\log d$, which is twice as large as the classical capacity of the erasure channel.

Proposition 9.3. If the channel Φ is covariant, the maximum in (9.4) is attained for an invariant state S_A. In particular, if Φ is irreducibly covariant, it is attained on the chaotic state.

Proof. Let the channel Φ satisfy the covariance condition (6.48). In this case,

$$I\left(V_g^A S_A V_g^{A*}, \Phi\right) = I\left(S_A, \Phi\right) \tag{9.5}$$

This follows from the expression (7.52) for the mutual information, unitary covariance of the input and output entropies, and the corresponding property of the entropy exchange,

$$H\left(V_g^A S_A V_g^{A*}, \Phi\right) = H\left(S_A, \Phi\right) \tag{9.6}$$

To prove this last property, consider formula (7.47) for the entropy exchange and note that purification of the state $V_g^A S_A V_g^{A*}$ is given by the vector $\left(V_g^A \otimes I_R\right)|\psi_{AR}\rangle$. Substituting this into (7.47) and again using the covariance of Φ and the unitary invariance of the entropy gives (9.6).

Now, let S_A be an optimal state for the channel Φ. Consider the V_g^A-invariant state

$$\bar{S} = \frac{1}{|G|}\sum_{g\in G} V_g^A S_A V_g^{A*}$$

By Proposition 7.31, the function $S \to I(S, \Phi)$ is concave, and therefore

$$I(\bar{S}, \Phi) \geq \frac{1}{|G|}\sum_{g\in G} I\left(V_g^A S_A V_g^{A*}, \Phi\right) = I\left(S_A, \Phi\right)$$

where the last equality follows from (9.5).

Example 9.4. Consider the depolarizing channel (6.49). By using unitary covariance, one sees that $I(S, \Phi)$ achieves its maximum at the chaotic state $\bar{S} = \frac{I}{d}$, for which $H(\bar{S}) = H(\Phi[\bar{S}]) = \log d$. The entropy exchange $H(\bar{S}, \Phi)$ is given by the relation (7.51), whence

$$C_{ea}(\Phi) = \log d^2 + \left(1 - p\frac{d^2-1}{d^2}\right)\log\left(1 - p\frac{d^2-1}{d^2}\right) + p\frac{d^2-1}{d^2}\log\frac{p}{d^2}. \tag{9.7}$$

This should be compared with the unassisted classical capacity C, which is equal to C_X, given by formula (8.19).

One can see, in particular, that the gain of entanglement assistance $C_{\rm ea}\,/C \to d+1$ in the limit of strong noise $p \to 1$ (note that both capacities tend to zero!). Moreover, taking the maximal possible value $p = \frac{d^2}{d^2-1}$, we obtain

$$\begin{aligned} C_{ea} &= \log \frac{d^2}{d^2-1} \\ C = C_\chi &= \frac{1}{d+1}\log\frac{d}{d+1} + \frac{d}{d+1}\log\frac{d^2}{d^2-1} \end{aligned} .$$

The ratio C_{ea}/C increases monotonically from the value 5.08 for $d=2$, tightly approaching the asymptotic line $2(d+1)$ as d grows. Recall (Proposition 6.40) that the depolarizing channel is entanglement-breaking for all $p \geq d/(d+1)$. Nevertheless, $C_{ea} > C$ also in this case. In the next section we will show that this inequality holds generically even for q-c channels.

Here, entanglement again appears as a "catalyst" of the transmission of classical information through the quantum channel - it may indefinitely increase the classical capacity of noisy channels, while being unable to transmit the information on its own.

Exercise 9.5 Show that for a qubit unital channel of the form (6.59) with Λ given by (6.64),

$$C_{ea}(\Phi) = I(\bar{S},\Phi) = 2\log 2 + \sum_{\gamma=0,x,y,z} \mu_\gamma \log \mu_\gamma$$

Hint: the entropy exchange $H(\bar{S},\Phi)$ can be computed by using Proposition 7.29 and the Kraus representation (6.64), resulting in

$$H(\bar{S},\Phi) = -\sum_{\gamma=0,x,y,z} \mu_\gamma \log \mu_\gamma$$

Compare this with the capacity $C_X(\Phi)$, given by formula (8.21).

In general, there are simple inequalities relating entanglement-assisted and unassisted classical capacities, i. e.,

$$C_\chi(\Phi) \leq C_{ea}(\Phi) \leq \log d + C_\chi(\Phi) \tag{9.8}$$

Take S_A to be a mixture of arbitrary pure states S_j with probabilities p_j. In this case, (7.50) implies

$$I\left(S_A,\Phi\right) \leq H\left(\sum_j p_j S_j\right) + H\left(\sum_j p_j \Phi\left(S_j\right)\right) - \sum_j p_j H\left(\Phi\left(S_j\right)\right)$$

Taking the maxima in both sides and using (9.4), we obtain the second inequality in (9.8).

Although the entanglement-assisted protocol uses additional resources compared to unassisted transmission of classical information, the first inequality in (9.8) is not quite obvious, because of the special nature of the encoding procedure used by A. To avoid this, let us show that the definition of $C_{ea}^{(1)}(\Phi)$, and hence of $C_{ea}(\Phi)$, can be formulated without explicit introduction of the encoding operations $\mathcal{E}_A^i$, namely,

$$\begin{aligned} C_{ea}^{(1)}(\Phi) = \sup_{\pi_i,\left\{S_{AB}^i\right\}\in\Sigma_B} \Big[& H\left(\sum_i \pi_i \left(\Phi\otimes \mathrm{Id}_B\right)\left[S_{AB}^i\right]\right) \\ & - \sum_i p i_i H\left(\left(\Phi\otimes\mathrm{Id}_B\right)\left[S_{AB}^i\right]\right)\Big] \end{aligned} \tag{9.9}$$

where Σ_B is the collection of families of the states $\{S^i_{AB}\}$ that satisfy the condition that their partial states S^i_B do not depend on $i, S^i_B = S_B$.

The first inequality in (9.8) then follows by taking $S^i_{AB} = S^i_A \otimes S_B$. To prove (9.9), it is sufficient to establish the following fact.

Lemma 9.6. Let $\{S^i_{AB}\}$ be a family of the states satisfying the condition $S^i_B = S_B$. Then there exist a pure state S_{AB} and encodings $\mathcal{E}^i_A$ such that

$$S^i_{AB} = \left(\mathcal{E}^i_A \otimes \mathrm{Id}_B\right)[S_{AB}]\,. \tag{9.10}$$

Proof. For simplicity assume first that S_B is nondegenerate. In this case,

$$S_B = \sum_{k=1}^{d} \lambda_k \left|e^B_k\right\rangle \left\langle e^B_k\right|,$$

where $\lambda_k > 0$ and $\left\{\left|e^B_k\right\rangle\right\}$ is an orthonormal basis in $\mathcal{H}_B$. Let $\left\{\left|e^A_k\right\rangle\right\}$ be an orthonormal basis in $\mathcal{H}_A$. For a vector $\left|\psi^A\right\rangle = \sum_{k=1}^d c_k \left|e^A_k\right\rangle$ we denote $\left|\bar{\psi}^B\right\rangle = \sum_{k=1}^d \bar{c}_k \left|e^B_k\right\rangle$. The map $\left|\psi^A\right\rangle \to \left|\bar{\psi}^B\right\rangle$ is an antiisomorphism of $\mathcal{H}_A$ and $\mathcal{H}_B$. Set

$$|\psi_{AB}\rangle = \sum_{k=1}^{d} \sqrt{\lambda_k}\left|e^A_k\right\rangle \otimes \left|e^B_k\right\rangle,$$

so that $S_{AB} = |\psi_{AB}\rangle\langle\psi_{AB}|$, and define encodings by the relation

$$\mathcal{E}^i_A\left[\left|\psi^A\right\rangle\left\langle\phi^A\right|\right] = \left\langle\bar{\psi}^B\right| S_B^{-1/2} S^i_{AB} S_B^{-1/2} \left|\bar{\phi}^B\right\rangle, \quad \left|\psi^A\right\rangle, \left|\phi^A\right\rangle \in \mathcal{H}_A.$$

Then one can check that $\mathcal{E}^i_A$ are indeed channels fulfilling formula (9.10).
In the case where S_B is degenerate, the above construction should be modified by replacing $S_B^{-1/2} S^i_{AB} S_B^{-1/2}$ in the above formula with $\sqrt{S_B^-} S^i_{AB} \sqrt{S_B^-} + P^0_B$, where $S_B^-$is the generalized inverse of S_B and P^0_B is the projection onto the null subspace of S_B. □

10.9.2 9.2 The Classical Capacities of Quantum Observables

In this section, we wish to compare the classical capacities C, C_{ea} for the special class of q-c channels, when it is possible to establish a necessary and sufficient condition for their coincidence. Let $M = \{M_y; y \in \mathcal{Y}\}$ be a quantum observable in a Hilbert space $\mathcal{H}$. Consider the measurement channel

$$\mathcal{M}[S] = \sum_y |e_y\rangle\langle e_y| \operatorname{Tr} S M_y. \tag{9.11}$$

Since any q − c channel is entanglement-breaking, its classical capacity is given by the one-letter expression

$$C(\mathcal{M}) = C_\chi(\mathcal{M}) = \max_\pi \mathcal{I}(\pi; M),$$

where $\pi = \{\pi_x, S_x\}$ is an ensemble that assigns the probabilities π_x to states S_x and

$$\mathcal{I}(\pi; M) = H\left(P_{\bar{S}_\pi}\right) - \sum_x \pi_x H\left(P_{S_x}\right)$$

is the Shannon information between the input x and the output y. Here, $\bar{S}_\pi = \sum_x \pi_x S_x$, $P_S = \{\operatorname{Tr} S M_y\}$ is the probability distribution of the measurement outcomes and $H(P)$ is the Shannon entropy of a probability distribution P. This can be rewritten as

$$C(\mathcal{M}) = \max_S \left[H(P_S) - \min_{\pi:\bar{S}_\pi = S} \sum_x \pi_x H(P_{S_x}) \right], \tag{9.12}$$

where the minimum is over input ensembles π with the fixed average state $\bar{S}_\pi = S$.
Next, consider the entanglement-assisted capacity which, according to Theorem 9.1, is given by the formula

$$C_{ea}(\mathcal{M}) = \max_S I(S; \mathcal{M}), \tag{9.13}$$

where

$$I(S; \mathcal{M}) = H(S) + H(\mathcal{M}[S]) - H(S, \mathcal{M})$$

is the quantum mutual information. Here, $H(\cdot)$ is the von Neumann entropy and $H(S, \mathcal{M})$ is the entropy exchange. Let $p_y = \operatorname{Tr} SM_y$ and let V_y be an operator satisfying $M_y = V_y^* V_y$, for example, $V_y = M_y^{1/2}$. Then the density operator $\frac{V_y S V_y^*}{p_y} = S(y \mid M)$ can be interpreted as posterior state of the measurement of observable M with instrument $S \to \left\{V_y S V_y^*\right\}$ in state S. We use the following formula [211]:

$$I(S; \mathcal{M}) = H(S) - \sum_y (\operatorname{Tr} SM_y) H(S(y \mid M)). \tag{9.14}$$

Indeed, writing the Kraus decomposition

$$\mathcal{M}[S] = \sum_{y,j} |e_y\rangle \langle h_j| V_y S V_y^* |h_j\rangle \langle e_y|$$

and applying Proposition 7.29, we obtain

$$\begin{aligned} H(S, \mathcal{M}) &= H\left(\sum_y V_y S V_y^* \otimes |e_y\rangle \langle e_y| \right) \\ &= H\left(\sum_y p_y S(y \mid M) \otimes |e_y\rangle \langle e_y| \right) \\ &= H(P_S) + \sum_y p_y H(S(y \mid M)), \end{aligned}$$

while $H(\mathcal{M}[S]) = H(P_S)$, hence (9.14). The entanglement-assisted classical capacity of the channel $\mathcal{M}$ follows by substituting this expression into (9.13).

Let us now describe the ensemble-observable duality. If $M = \{M_y; y \in \mathcal{Y}\}$ is a quantum observable and $\pi = \{p_x, S_x; x \in \mathcal{X}\}$ an ensemble of quantum states, then

$$p_{xy} = p_x \operatorname{Tr} S_x M_y$$

is a probability distribution on $\mathcal{X} \times \mathcal{Y}$. On the other hand,

$$p_{xy} = p'_y \operatorname{Tr} S'_y M'_x,$$

where, denoting $\bar{S}_\pi = \sum_x p_x S_x$, we have $p'_y S'_y = {\bar{S}_\pi}^{1/2} M_y {\bar{S}_\pi}^{1/2}$ so that $p'_y = \operatorname{Tr} \bar{S}_\pi M_y$ and $M'_x = p_x {\bar{S}_\pi}^{-1/2} S_x {\bar{S}_\pi}^{-1/2}$. Here $M'_\pi = \{M'_x; x \in \mathcal{X}\}$ is the new observable, and $\pi' = \left\{p'_y, S'_y; y \in \mathcal{Y}\right\}$ is the new ensemble. Therefore, the Shannon information between x, y is

$$\mathcal{I}(\pi, M) = \mathcal{I}(\pi', M'_\pi).$$

Introducing the ensemble $\pi'_S = \left\{\operatorname{Tr} SM_y, \frac{S^{1/2}M_yS^{1/2}}{\operatorname{Tr} SM_y}\right\}$, for a given state S, we have the following duality relations.

Proposition 9.7. Denoting $A(\pi'_S) = \max_{M''} \mathcal{I}(\pi'_S, M'')$ the accessible information and $\chi(\pi'_S) = H\left(\sum_y p'_y S'_y\right) - \sum_y p'_y H\left(S'_y\right)$ the χ-quantity of the dual ensemble π'_S, we have

$$C(\mathcal{M}) \equiv \max_{\pi} \mathcal{I}(\pi, M) = \max_{S} A(\pi'_S) \tag{9.15}$$

$$C_{ea}(\mathcal{M}) \equiv \max_{S} I(S; \mathcal{M}) = \max_{S} \chi(\pi'_S) \tag{9.16}$$

Proof. Relation (9.15) follows from

$$\begin{aligned}
\max_{\pi} \mathcal{I}(\pi, M) &= \max_{S} \max_{\pi:\bar{S}_\pi = S} \mathcal{I}(\pi, M) \\
&= \max_{S} \max_{M'_\pi \cdot \bar{S}_\pi = S} \mathcal{I}(\pi'_S, M'_\pi) \\
&= \max_{S} \max_{M''} \mathcal{I}(\pi'_S, M'') \\
&= \max_{S} A(\pi'_S),
\end{aligned}$$

where in the third equality we used the fact that for any observable $M'' = \{M_y\}$ there is an ensemble $\pi = \left\{\frac{\operatorname{Tr} SM_y}{d}, \frac{M_y}{\operatorname{Tr} SM_y}\right\}$ such that $M'' = M'_\pi$ for this ensemble.

Note that $\sum_y p'_y S'_y = S$, and $H\left(S'_y\right) = H\left(\frac{V_y S V_y^*}{p'_y}\right)$, where V_y is an arbitrary operator that satisfies $M_y = V_y^* V_y$, because the operators $V_y S V_y^* = V_y S^{1/2} S^{1/2} V_y^*$ and $S^{1/2} V_y^* V_y S^{1/2} = S^{1/2} M_y S^{1/2} = p'_y S'_y$ are unitarily equivalent via polar decomposition and hence have the same spectrum. The density operator $\frac{V_y S V_y^*}{p'_y} = S(y \mid M)$ is the posterior state of the measurement of the observable M with the instrument $\{V_y\}$ in the state S. Thus, the χ-quantity of the dual ensemble is

$$\chi(\pi'_S) = H(S) - \sum_y p'_y H(S(y \mid M)) = I(S; \mathcal{M}) \tag{9.17}$$

and hence, in addition to (9.15), we have, via (9.14), the duality relation (9.16). □

Let us now recall the bound of Theorem 5.9,

$$A(\pi) \leq H\left(\sum_y p_y S_y\right) - \sum_y p_y H(S_y) \equiv \chi(\pi), \tag{9.18}$$

with equality attained if and only if the operators $p_y S_y$ all commute. Applying this to the dual situation, we obtain

$$A(\pi'_S) \leq H\left(\sum_y p'_y S'_y\right) - \sum_y p'_y H\left(S'_y\right) = \chi(\pi'_S).$$

Then the necessary and sufficient condition for the equality becomes

$$S^{1/2} M_y S M_{y'} S^{1/2} = S^{1/2} M_{y'} S M_y S^{1/2} \tag{9.19}$$

for all y, y'. Therefore, by (9.15), (9.16), the necessary and sufficient condition for the equality $C_{ea}(\mathcal{M}) = C(\mathcal{M})$ is that condition (9.19) is fulfilled for a density operator S maximizing the quantity (9.17). In particular, in the case of a covariant observable $M_g = V_g M_0 V_g^*$, where V_g is an irreducible representation of a symmetry group G, Proposition 9.3 implies $S = I/d$

and condition (9.19) reduces to the fact that all components of the observable commute, i. e., it is essentially a classically randomized observable.

Consider the case of an overcomplete system $M_y = |\psi_y\rangle\langle\psi_y|$ in d-dimensional Hilbert space $\mathcal{H}$, where $S = I/d$. The corresponding ensemble of pure states is $\pi'_S \equiv \bar{\pi} = \left\{\frac{\langle\psi_y|\psi_y\rangle}{d}, \frac{|\psi_y\rangle\langle\psi_y|}{\langle\psi_y|\psi_y\rangle}\right\}$ and $\chi(\bar{\pi}) = \log d = C_{ea}(\mathcal{M})$ (note that this is also equal to the classical capacity of the c-q channel $y \longrightarrow \frac{|\psi_y\rangle\langle\psi_y|}{\langle\psi_y|\psi_y\rangle}$, since this is the maximal possible value). Condition (9.19) amounts to

$$|\psi_y\rangle\langle\psi_y \mid \psi_{y'}\rangle\langle\psi_{y'}| = |\psi_{y'}\rangle\langle\psi_{y'} \mid \psi_y\rangle\langle\psi_y|.$$

We can always assume that the vectors $|\psi_y\rangle$ are all pairwise linearly independent. In this case, the last condition is equivalent to the fact that they form an orthonormal basis.

Thus we conclude that $C_{ea}(\mathcal{M}) > C(\mathcal{M})$, unless $\{\psi_y\}$ is an orthonormal basis.
Now, let Θ be the unit sphere in $\mathcal{H}$ and let $v(d\theta)$ be the uniform distribution on Θ. To avoid notational confusion with the differential, we denote in the argument below the dimensionality with $d_A = \dim \mathcal{H}$. According to relation (6.55), the family of unit vectors $\{|\theta\rangle; \theta \in \Theta\}$ can be considered a continuous overcomplete system. The corresponding measurement channel $\mathcal{M}$ maps the density operator S to the probability distribution on Θ, i. e.,

$$\mathcal{M} : S \longrightarrow d_A\langle\theta|S|\theta\rangle v(d\theta). \tag{9.20}$$

It can be shown that, similar to the discrete overcomplete systems considered above, $C_{ea}(\mathcal{M}) = \log d_A$. Let us show that

$$C(\mathcal{M}) = \log d_A - \log e \sum_{k=2}^{d_A} \frac{1}{k}. \tag{9.21}$$

Thus, for $d_A \to \infty$ we have $C(\mathcal{M}) \to \log e(1-\gamma)$, where $\gamma \approx 0.577$ is Euler's constant. At the same time, $C_{ea}(\mathcal{M}) = \log d_A \to \infty$.

All outcome probability distributions (9.20) are absolutely continuous with respect to $v(d\theta)$, and hence we can use the differential entropy

$$h(p_S) = -\int_\Theta p_S(\theta) \log p_S(\theta) v(d\theta),$$

where $p_S(\theta) = d_A\langle\theta|S|\theta\rangle$, to get the continuous analog of formula (9.12)

$$C(\mathcal{M}) = C_\chi(\mathcal{M}) = \max_S \left[h(p_S) - \min_{\pi: S_\pi = S} \sum_x \pi_x h(p_{S_x}) \right]. \tag{9.22}$$

The channel $\mathcal{M}$ is covariant with respect to the irreducible action of the unitary group, in the sense that

$$\mathcal{M}(USU^*) = d_A \langle U^*\theta| S |U^*\theta\rangle v(d\theta).$$

Therefore, similar to (8.15)

$$C_\chi(\mathcal{M}) = h\left(\mathcal{M}\left(\frac{I}{d_A}\right)\right) - \min_{\theta'} h\left(\mathcal{M}\left(|\theta'\rangle\langle\theta'|\right)\right). \tag{9.23}$$

But $\mathcal{M}\left(\frac{I}{d_A}\right)$ is the uniform distribution over Θ, with density $p(\theta) \equiv 1$. Hence, $h\left(\mathcal{M}\left(\frac{I}{d_A}\right)\right) = 0$. On the other hand,

$$-h\left(\mathcal{M}\left(|\theta'\rangle\langle\theta'|\right)\right)=\int_{\Theta}d_A\left|\langle\theta\mid\theta'\rangle\right|^2\log\left[d_A\left|\langle\theta\mid\theta'\rangle\right|^2\right]v(d\theta). \tag{9.24}$$

By the unitary invariance of v, this quantity is the same for all θ'. Hence, there is no need for minimization in (9.23). For its computation, we use relation (6.57). With this, (9.24) becomes

$$-\int_0^1\left(d_Ar^2\right)\log\left(d_Ar^2\right)d\left(1-r^2\right)^{d_A-1}=\int_0^1\left[d_A(1-u)\right]\log\left[d_A(1-u)\right]d\left(u^{d_A-1}\right),$$

where $u=1-r^2$, which, after integrations by parts, gives (9.21).

10.9.3 9.3 Proof of the Converse Coding Theorem

Now, we finally come to the proof of Theorem 9.1.
To prove the inequality

$$C_{ea}(\Phi)\leq\max_{S_A}I\left(S_A,\Phi\right), \tag{9.25}$$

we first prove that

$$C_{ea}^{(1)}(\Phi)\leq\max_{S_A}I\left(S_A,\Phi\right) \tag{9.26}$$

Let us denote by $\mathcal{E}_A^i$ the encodings used by A. Let S_{AB} be the pure state, initially shared between A and B. Then the state of the system AB (resp. A) after the encoding is

$$S_{AB}^i=\left(\mathcal{E}_A^i\otimes\mathrm{Id}_B\right)\left[S_{AB}\right],\quad S_A^i=\mathcal{E}_A^i\left[S_A\right]. \tag{9.27}$$

Note that the partial state of B does not change after the encoding, i.e., $S_B^i=S_B$. We will prove that

$$H\left(\sum_i\pi_i\left(\Phi\otimes\mathrm{Id}_B\right)\left[S_{AB}^i\right]\right)-\sum_i\pi_iH\left(\left(\Phi\otimes\mathrm{Id}_B\right)\left[S_{AB}^i\right]\right)\leq I\left(\sum_i\pi_iS_A^i,\Phi\right). \tag{9.28}$$

The maximum of the left-hand side with respect to all possible $\pi_i,\mathcal{E}_A^i$ is just $C_{ea}^{(1)}(\Phi)$, from which (9.26) follows.

By using the subadditivity of the quantum entropy, we can upperbound the first term in the left-hand side of (9.28) as

$$H\left(\sum_i\pi_i\Phi\left[S_A^i\right]\right)+H\left(S_B\right)=H\left(\Phi\left[\sum_i\pi_iS_A^i\right]\right)+\sum_i\pi_iH\left(S_B\right).$$

Here, the first term already provides us with the output entropy from $I\left(\sum_i\pi_iS_A^i;\Phi\right)$. Let us proceed with the evaluation of the remainder

$$\sum_i\pi_i\left[H\left(S_B\right)-H\left(\left(\Phi\otimes\mathrm{Id}_B\right)\left[S_{AB}^i\right]\right)\right].$$

We first show that the term in squared brackets does not exceed $H\left(S_A^i\right)-H((\Phi\otimes\mathrm{Id}_{R^i})\left[S_{AR^i}^i\right]$, where R^i is the purifying (reference) system for S_A^i, and $S_{AR^i}^i$ is the purified state. To this end consider the unitary extension of the encoding $\mathcal{E}_A^i$ with the environment E_i, which is initially in a pure state, according to Theorem 6.18. From (9.27) we

see that we can take $R^i = BE_i$ (after the unitary interaction, which involves only AE_i). Then again denoting by primes states after the application of the channel Φ, we have

$$H(S_B) - H\left((\Phi \otimes \mathrm{Id}_B)\left[S^i_{AB}\right]\right) = H(S_B) - H\left(S^i_{A'B}\right) = -H_i(A' \mid B), \tag{9.29}$$

where the lower index i of the conditional entropy refers to the joint state $S^i_{A'B'}$. Similarly,

$$\begin{aligned} H\left(S^i_A\right) - H\left((\Phi \otimes \mathrm{Id}_{R^i})\left[S^i_{AR^i}\right]\right) &= H\left(S^i_{R^i}\right) - H\left(S^i_{A'R^i}\right) \\ &= -H_i\left(A' \mid R^i\right) = -H_i(A' \mid BE_i), \end{aligned}$$

which is greater than or equal to (9.29), by the monotonicity of the conditional entropy (Exercise 7.26).

Using the concavity of the function $S_A \to H(S_A) - H((\Phi \otimes \mathrm{Id}_R)[S_{AR}])$, to be shown below, we get

$$\begin{aligned} \sum_i \pi_i \left[H\left(S^i_A\right) - H\left((\Phi \otimes \mathrm{Id}_{R^i})\left[S^i_{AR^i}\right]\right)\right] \leq & H\left(\sum_i \pi_i S^i_A\right) \\ & - H\left((\Phi \otimes \mathrm{Id}_R)\left[\hat{S}_{AR}\right]\right) \end{aligned}$$

where $\hat{S}_{AR}$ is the state purifying $\sum_i \pi_i S^i_A$ with a reference system R, thus arriving to (9.28).

To complete this proof, it remains to show the above concavity. By introducing the environment E for the channel Φ, we have

$$\begin{aligned} H(S_A) - H((\Phi \otimes \mathrm{Id}_R)[S_{AR}]) &= H(S_R) - H(S_{A'R}) \\ &= H(S_{A'E'}) - H(S_{E'}) = H(A' \mid E'). \end{aligned}$$

Now, $H(A' \mid E')$ is a concave function of $S_{A'E'}$ by Corollary 7.27. The map $S_A \to S_{A'E'}$ is affine and therefore $H(A' \mid E')$ is a concave function of S_A.

Applying the same argument to the channel $\Phi^{\otimes n}$ gives

$$C^{(n)}_{ea}(\Phi) \leq \max_{S_A} I\left(S_A, \Phi^{\otimes n}\right) \tag{9.30}$$

Then, from the subadditivity of the quantum mutual information (property iii in Proposition 7.31) we have

$$\max_{S_{12}} I(S_{12}, \Phi_1 \otimes \Phi_2) = \max_{S_1} I(S_1, \Phi_1) + \max_{S_2} I(S_2, \Phi_2),$$

whence the remarkable additivity follows, and we have

$$\max_{S_{A^n}} I\left(S_{A^n}, \Phi^{\otimes n}\right) = n \max_{S_A} I(S_A, \Phi).$$

Therefore, we finally obtain (9.25). □

10.9.4 9.4 Proof of the Direct Coding Theorem

Here, we prove the inequality

$$C_{ea}(\Phi) \geq \max_{S_A} I(S_A, \Phi). \tag{9.31}$$

First, let us show by generalizing the dense coding protocol that

$$C^{(1)}_{ea}\left(\Phi^{\otimes n}\right) \geq I\left(\frac{P}{\dim P}, \Phi^{\otimes n}\right) \tag{9.32}$$

for an arbitrary projection P in $\mathcal{H}_A^{\otimes n}$.
Indeed, let $P = \sum_{k=1}^m |e_k\rangle\langle e_k|$, where $\{e_k; k = 1, \ldots, m = \dim P\}$ is an orthonormal system. Consider the discrete Weyl system $\{W_{\alpha\beta}; \alpha, \beta = 0, \ldots, m-1\}$, defined by the relations (6.50) on the subspace $\mathcal{H}_P = P\mathcal{H}_A^{\otimes n}$.

Since $\dim \mathcal{H}_A \leq \dim \mathcal{H}_B$, we can assume that $\mathcal{H}_A \subseteq \mathcal{H}_B$. Let

$$|\psi_{AB}\rangle = \frac{1}{\sqrt{m}} \sum_{k=1}^m |e_k\rangle \otimes |e_k\rangle .$$

Exercise 9.8 Show that the system $\{(W_{\alpha\beta} \otimes I_B) |\psi_{AB}\rangle ; \alpha, \beta = 0, \ldots, m-1\}$ is an orthonormal basis in $\mathcal{H}_p \otimes \mathcal{H}_p$. In particular,

$$\sum_{\alpha,\beta=0}^{m-1} (W_{\alpha\beta} \otimes I_B) |\psi_{AB}\rangle \langle\psi_{AB}| (W_{\alpha\beta} \otimes I_B)^* = P \otimes P. \tag{9.33}$$

The operators $W_{\alpha\beta}$ will play a role similar to the Pauli matrices in the dense coding protocol for qubits. Take the classical signal to be transmitted as $i = (\alpha, \beta)$, with equal probabilities $1/m^2$, the entangled state $|\psi_{AB}\rangle\langle\psi_{AB}|$, and the unitary encodings $\mathcal{E}_A^i[S] = W_{\alpha\beta} S W_{\alpha\beta}^*$. Now, we have

$$C_{ea}^{(1)}\left(\Phi^{\otimes n}\right) \geq H\left(\frac{1}{m^2}\sum_{\alpha,\beta} (\Phi \otimes \mathrm{Id}_B)^{\otimes n}\left[S_{AB}^{\alpha\beta}\right]\right) - \frac{1}{m^2}\sum_{\alpha,\beta} H\left((\Phi \otimes \mathrm{Id}_B)^{\otimes n}\left[S_{AB}^{\alpha\beta}\right]\right),$$

where $S_{AB}^{\alpha\beta} = \left(W_{\alpha\beta} \otimes I_B^{\otimes n}\right) |\psi_{AB}\rangle\langle\psi_{AB}| \left(W_{\alpha\beta} \otimes I_B^{\otimes n}\right)^*$. By (9.33) the first term in the right-hand side is equal to $H\left((\Phi \otimes \mathrm{Id}_B)\left[\frac{P}{m} \otimes \frac{P}{m}\right]\right) = H\left(\frac{P}{m}\right) + H\left(\Phi\left[\frac{P}{m}\right]\right)$. Since $S_{AB}^{\alpha\beta}$ is a purification of $\frac{P}{m}$, the entropies in the second term are all equal to $H\left(\frac{P}{m}, \Phi\right)$. By the expression for the quantum mutual information

$$I(S_A, \Phi) = H(S_A) + H(\Phi[S_A]) - H(S_A; \Phi)$$

with $S_A = \frac{P}{m}$, this proves (9.32). For future use, note that the last term in the quantum mutual information - the entropy exchange - is equal to the final environment entropy $H(S'_E) = H\left(\tilde{\Phi}[S_A]\right)$, where $\tilde{\Phi}$ is the complementary channel from the system to the environment.

Now let $S_A = S$ be an arbitrary state in $\mathcal{H}_A$ and let $\hat{P}^{n,\delta}$ be the strongly typical projector of the state $S^{\otimes n}$ in the space $\mathcal{H}_A^{\otimes n}$, defined below. We shall prove that for an arbitrary channel Ψ from $\mathcal{H}_A$ to a possibly other Hilbert space $\tilde{\mathcal{H}}$ the following relation holds:

$$\lim_{\delta\to 0}\lim_{n\to\infty} \frac{1}{n} H\left(\Psi^{\otimes n}\left[\frac{\hat{P}^{n,\delta}}{\dim \hat{P}^{n,\delta}}\right]\right) = H(\Psi[S]).$$

This would imply, by the above expressions for the mutual information and the entropy exchange, that

$$\lim_{\delta\to 0}\lim_{n\to\infty} \frac{1}{n} I\left(\frac{\hat{P}^{n,\delta}}{\dim \hat{P}^{n,\delta}}, \Phi^{\otimes n}\right) = I(S, \Phi), \tag{9.34}$$

and hence, by (9.32), the required inequality (9.31).
Definition 9.9. Let us fix small positive δ, and let λ_j be the eigenvalues and $|e_j\rangle$ the eigenvectors of the density operator S. Then the eigenvalues and eigenvectors of $S^{\otimes n}$ are $\lambda_J = \lambda_{j_1} \cdots \lambda_{j_n}, |e_J\rangle = |e_{j_1}\rangle \otimes \cdots \otimes |e_{j_n}\rangle$, where $J = (j_1, \ldots, j_n)$. The sequence J is called strongly typical if the numbers $N(j \mid J)$ of times that the symbol j appears in J satisfy the condition

$$\left|\frac{N(j \mid J)}{n} - \lambda_j\right| < \delta, \quad j = 1, \ldots, d,$$

and $N(j \mid J) = 0$ if $\lambda_j = 0$. Let us denote the collection of all strongly typical sequences as $\hat{T}^{n,\delta}$. The strongly typical projector is defined as the following spectral projector of the density operator $S^{\otimes n}$:

$$\hat{P}^{n,\delta} = \sum_{J \in \hat{T}^{n,\delta}} |e_J\rangle \langle e_J| .$$

Let P^n be the probability distribution given by the eigenvalues λ_J. Then, by the law of large numbers, $\mathrm{P}^n\left(\hat{T}^{n,\delta}\right) \to 1$ as $n \to \infty$. For an arbitrary function $f(j), j = 1, \ldots, d$, and a sequence $J = (j_1, \ldots, j_n) \in \hat{T}^{n,\delta}$,

$$\left|\frac{f(j_1) + \cdots + f(j_n)}{n} - \sum_{j=1}^{d} \lambda_j f(j)\right| < \delta d \max f. \tag{9.35}$$

In particular, any strongly typical sequence is typical: taking $f(j) = -\log \lambda_j$ gives

$$n\left[H(S) - \delta_1\right] < -\log \lambda_J < n\left[H(S) + \delta_1\right], \tag{9.36}$$

where $\delta_1 = \delta d \max_{\lambda_j > 0}(-\log \lambda_j)$ (the converse is not true - not every typical sequence is strongly typical).

We shall need the following combinatorial result, the proof of which can be found in [50].

Exercise 9.10 Show that the size of the set $\hat{T}^{n,\delta}$ is estimated as

$$2^{n[H(S) - \Delta_n(\delta)]} < \left|\hat{T}^{n,\delta}\right| < 2^{n[H(S) + \Delta_n(\delta)]}, \tag{9.37}$$

where $H(S) = -\sum_{j=1}^{d} \lambda_j \log \lambda_j$, and $\lim_{\delta \to 0} \lim_{n \to \infty} \Delta_n(\delta) = 0$.

Proof of the relation (9.34). Denote $d_{n,\delta} = \dim \hat{P}^{n,\delta} = \left|\hat{T}^{n,\delta}\right|$ and $\bar{S}^{n,\delta} = \frac{\hat{P}^{n,\delta}}{d_{n,\delta}}$. We will prove that

$$\lim_{\delta \to 0} \lim_{n \to \infty} \frac{1}{n} H\left(\Psi^{\otimes n}\left[\bar{S}^{n,\delta}\right]\right) = H(\Psi[S]) \tag{9.38}$$

for an arbitrary channel Ψ. We have

$$\begin{aligned} nH(\Psi[S]) - H\left(\Psi^{\otimes n}\left[\bar{S}^{n,\delta}\right]\right) =& H\left(\Psi[S]^{\otimes n}\right) - H\left(\Psi^{\otimes n}\left[\bar{S}^{n,\delta}\right]\right) \\ =& H\left(\Psi^{\otimes n}\left[\bar{S}^{n,\delta}\right]; \Psi^{\otimes n}\left[S^{\otimes n}\right]\right) \\ &+ \operatorname{Tr} \log \Psi[S]^{\otimes n}\left(\Psi^{\otimes n}\left[\bar{S}^{n,\delta}\right] - \Psi[S]^{\otimes n}\right). \end{aligned} \tag{9.39}$$

Strictly speaking, this formula is correct if the density operator $\Psi[S]^{\otimes n}$ is nondegenerate, which we will assume for the moment. Later we shall show how the argument can be modified to the general case.

For the first term, by the monotonicity of the relative entropy, we have the estimate

$$H\left(\Psi^{\otimes n}\left[\bar{S}^{n,\delta}\right]; \Psi^{\otimes n}\left[S^{\otimes n}\right]\right) \leq H\left(\bar{S}^{n,\delta}; S^{\otimes n}\right),$$

with the right-hand side computed explicitly as

$$H\left(\bar{S}^{n,\delta}; S^{\otimes n}\right) = \sum_{J \in \hat{T}^{n,\delta}} \frac{1}{d_{n,\delta}} \log \frac{1}{d_{n,\delta} \lambda_J} = -\log d_{n,\delta} - \sum_{J \in \hat{T}^{n,\delta}} \frac{1}{d_{n,\delta}} \log \lambda_J,$$

which, divided by n, by (9.36), (9.37) is less than or equal to the quantity ($\delta_1 + \Delta_n(\delta)$), converging to zero as $n \to \infty, \delta \to 0$.

By using the identity

$$\log \Psi[S]^{\otimes n} = \log \Psi[S] \otimes I \otimes \cdots \otimes I + \cdots + I \otimes \cdots \otimes I \otimes \log \Psi[S]$$

and introducing the operator $F = \Psi^*[\log \Psi[S]]$, where Ψ^* is the dual channel, we can rewrite the second term as

$$\begin{aligned} & n \operatorname{Tr} \frac{(F \otimes I \otimes \cdots \otimes I + \cdots + I \otimes \cdots \otimes I \otimes F)}{n} \left(\bar{S}^{n,\delta} - S^{\otimes n}\right) \\ & = \frac{n}{d_{n,\delta}} \sum_{J \in \hat{T}^{n,\delta}} \left[\frac{f(j_1) + \cdots + f(j_n)}{n} - \sum_{j=1}^{d} \lambda_j f(j) \right] \end{aligned} \tag{9.40}$$

where $f(j) = \langle e_j | F | e_j \rangle$, which is evaluated by $n\delta d \max f$ via (9.35). This establishes (9.38) in the case of a nondegenerate $\Psi[S]$.

Coming back to the general case, let us denote by P_Ψ the supporting projector of $\Psi[S]$. Then the supporting projector of $\Psi[S]^{\otimes n}$ is $P_\Psi^{\otimes n}$, and the support of $\Psi^{\otimes n}\left(\bar{S}^{n,\delta}\right)$ is contained in the support of $\Psi[S]^{\otimes n} = \Psi^{\otimes n}\left[S^{\otimes n}\right]$, because the support of $\bar{S}^{n,\delta}$ is contained in that of $S^{\otimes n}$. Thus, the second term in (9.39) can be understood as

$$\operatorname{Tr} P_\Psi^{\otimes n} \log \left[P_\Psi^{\otimes n} \Psi[S]^{\otimes n} P_\Psi^{\otimes n}\right] P_\Psi^{\otimes n} \left(\Psi^{\otimes n}\left[\bar{S}^{n,\delta}\right] - \Psi[S]^{\otimes n}\right),$$

where now we have the logarithm of a nondegenerate operator in $P_\Psi^{\otimes n} \mathcal{H}_{A'}^{\otimes n}$. We can then repeat the argument, with F defined as $\Psi^*\left[P_\Psi \log\left(P_\Psi \Psi[S] P_\Psi\right) P_\Psi\right]$. This completes the proof of (9.34), from which (9.31) follows. □

10.9.5 9.5 Notes and References

1. Theorem 9.1 was announced by Bennett, Shor, Smolin, and Thapliyal in [28] and was proved in the paper [29] by the same authors. The case of limited amount of entanglement was studied by Shor [219].

2. Information capacities of quantum observables were studied by Dall'Arno, D'Ariano, and Sacchi [53] and by Holevo [123]. The identity (9.15) was obtained in [53] and (9.16) was obtained in [123]. Relation (9.14) is due to Shirokov [211], who also obtained a general criterion for the coincidence $C_{ea} = C_\chi$, saying that the essential part of the channel should be the c-q channel [212]. The duality between quantum observables and ensembles was introduced by Hall [89]. The value (9.21) was obtained in the paper of Jozsa, Robb, and Wootters [145] as the "subentropy" of the chaotic state $S = I/d$.

3. We here provide a simplified proof, following [116]. Concerning strongly typical projectors and the solution of Exercise 9.10, see [50].

10.10 10 Transmission of Quantum Information

As was already stressed, a quantum state is itself a special kind of information resource, insofar as it contains statistical uncertainty. Statistical mechanics studies irreversible state changes of a physical system that result from its interaction with the environment (and are accompanied by loss of information). Information theory in a sense solves a reverse problem, namely, that of how to reduce these losses to a negligible quantity by using a special processing

of the system state - encoding before and decoding after the irreversible evolution described by a noisy channel. This chapter is devoted to this kind of problems.

We shall start with a brief review of the methods of encoding the quantum information resilient to a certain specific kind of errors (e.g., an arbitrary error in one arbitrary qubit), when complete error correction is possible. We then pass to an approximate setting, where some measure of fidelity for the processing of a quantum state is introduced. In this situation, the aim is to asymptotically achieve an exact transmission of the quantum state through the composite channel $\Phi^{\otimes n}$ with maximal possible rate as $n \to \infty$. In this way, another analog of the Shannon coding theorem emerges, concerning the transmission of quantum information. This leads to the notion of the quantum capacity, expressed in terms of an entropic quantity called coherent information. On the other hand, the quantum capacity of a channel turns out to be closely related to its cryptographic characteristics, such as the capacity for the secret transmission of classical information (the private classical capacity). The role of the eavesdropper in such scenarios is played by the environment of the quantum system.

10.10.1 10.1 Quantum Error-Correcting Codes

10.10.2 10.1.1 Error Correction by Repetition

When transmitting information, one would like to have a code that is robust against errors. In the classical case, the existence of such codes for rates below the capacity follows from the Shannon coding theorem. However, this theorem does not provide a constructive method for the design of such codes, and a practical solution to this problem is the subject of extensive research in classical information theory.

A straightforward method of reducing errors is repetition of messages, which, of course, reduces the rate of transmission. Take the binary alphabet 0,1 and assume that the probability p of a bit flip in the process of transmission is small, so that the probability of a change in more than one bit is negligible. Consider the code $0 \to 00$, $1 \to 11$. In this case, having received 00 or 11 , one can conclude with a high degree of certitude that the encoded symbol was 0 or, correspondingly, 1 . However, if 01 or

10 was received, one can only ascertain an error but not recover the encoded symbol. However, this defect is easily remedied by adding one more bit to the code, $0 \to 000$ and $1 \to 111$. The last code corrects the error in one arbitrary bit of the received message.

A direct generalization of this recipe to the quantum case is impossible, because quantum information cannot be copied. By the very nature of quantum information, one should be able to transmit robustly not only the basis states but also their superposition. Although at first glance this seems not feasible, the problem has an ingenious solution. Let us consider an example of solving such a problem in an important model case.

Assume that one wants to transmit an arbitrary pure state of a qubit $\psi = a|0\rangle + b|1\rangle$, provided that encoding by states of several qubits is allowed. The encoding in the quantum case is just an isometric mapping. Following the classical analogy, consider first the code that maps the basis vectors as follows:

$$|0\rangle \to |000\rangle, \quad |1\rangle \to |111\rangle. \tag{10.1}$$

Such a code corrects the "bit flip," i.e., the change $|0\rangle \leftrightarrow |1\rangle$ in any one of the qubits. We are interested in the arbitrary state $a|0\rangle + b|1\rangle$, which is now encoded into $a|000\rangle + b|111\rangle$. Let, for example, the bit flip occur in the first qubit, i.e.,

$$a|0\rangle + b|1\rangle \to a|100\rangle + b|011\rangle,$$

In this case, the states $a|000\rangle + b|111\rangle, a|100\rangle + b|011\rangle$ are orthogonal, and hence can be perfectly distinguished to correct the error.

However, such a code does not correct a "phase flip" $|0\rangle \leftrightarrow |0\rangle, |1\rangle \leftrightarrow -|1\rangle$. Indeed, after such a phase error in one bit, we have $a|000\rangle - b|111\rangle$ instead of $a|000\rangle + b|111\rangle$, and in general these states are not orthogonal, and hence not perfectly distinguishable.

Now remark that the Hadamard transform

$$|0\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |1\rangle \to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

maps a phase flip into a bit flip and vice versa. By converting the code (10.1), we obtain another code,

$$\begin{aligned} |0\rangle &\to \frac{1}{2^{3/2}}(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)(|0\rangle + |1\rangle), \\ |1\rangle &\to \frac{1}{2^{3/2}}(|0\rangle - |1\rangle)(|0\rangle - |1\rangle)(|0\rangle - |1\rangle), \end{aligned} \tag{10.2}$$

which corrects a phase flip in one arbitrary qubit, but does not correct bit flips.
The Shor code, which corrects both phase and bit flips in one qubit, is obtained by concatenation of the codes (10.1), (10.2), and requires nine qubits, i.e.,

$$\begin{aligned} |0\rangle &\to \frac{1}{2^{3/2}}(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle), \\ |1\rangle &\to \frac{1}{2^{3/2}}(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle). \end{aligned} \tag{10.3}$$

Remarkably, it turns out that this code corrects not only bit and phase errors but also an arbitrary error in one of the nine qubits, since it can be represented as a combination of these two basic errors. This follows from the fact that the general conditions for error correction discussed in Section 10.1.3 are satisfied.

10.10.3 10.1.2 General Formulation

Let S be an arbitrary state in a Hilbert space $\mathcal{M}$. A quantum code is an isometric map $V : \mathcal{M} \to \mathcal{N}$, transforming states S into encoded states VSV^* in another Hilbert space $\mathcal{N}$. The system $\mathcal{N}$ is subject to errors, the effect of which is described by completely positive maps Φ in $\mathfrak{T}(\mathcal{N})$, that belong to a certain class $\mathcal{E}$. As we know, irreversible evolutions are described by CP maps that satisfy the normalization $\Phi(I) \leqslant I$ (see Section 6.5), but in the present situation this restriction is not essential, since the effect of an error is determined up to a constant factor.

Thus, transformations of the quantum information are given by the diagram

$$S \longrightarrow VSV^* \longrightarrow \Phi\left(VSV^*\right), \quad \Phi \in \mathcal{E}.$$

Definition 10.1. The code V is correcting errors from $\mathcal{E}$, if there exists a reverse channel $\mathcal{D}$ such that

$$\mathcal{D}\left[\Phi\left(VSV^*\right)\right] = c(\Phi)S \tag{10.4}$$

for an arbitrary state S and an arbitrary $\Phi \in \mathcal{E}$, where $c(\Phi)$ is a constant depending only on Φ.

In fact, the code is determined by the subspace $\mathcal{L} = V\mathcal{M} \subset \mathcal{N}$ and can be defined as such, without introducing $\mathcal{M}$ and V.

Example 10.2. Storage of quantum information in the memory of a quantum computer. Let $\mathcal{N} = \mathcal{H}_2^{\otimes n}$ be the quantum register in which the quantum information from the subspace $\mathcal{M}$ is to be stored. Consider errors involving no more than m qubits of the register. The corresponding class $\mathcal{E}(n,m)$ consists of the maps $\Phi = \Phi_1 \otimes \cdots \otimes \Phi_n$, where the number of $\Phi_k \neq \mathrm{Id}$ is not greater than m, while the error Φ_k in the k th qubit can be an arbitrary completely positive map. Operators of elementary errors in each qubit are usually given by the Pauli matrices, with σ_x describing the bit flip, σ_z the phase flip, and $\sigma_y = i\sigma_x\sigma_z$ their combination. Together with the unit operator $\sigma_0 = I$, corresponding to absence of error, they form a basis in the algebra of observables of the qubit.

The Shor code demonstrates the possibility of error-correction for the class $\mathcal{E}(n,1)$, if n is large enough (one can show that the smallest possible value of n for a code that corrects one error is 5). Restriction to the correction of only one error is, of course, essential here. However, it can be shown that there exist codes that correct errors from $\mathcal{E}(n,m)$, where the ratio m/n is greater than a certain positive number for large enough n.

10.10.4 10.1.3 Necessary and Sufficient Conditions for Error Correction

The class $\mathcal{E}$ of errors usually has the following structure. It consists of mappings of the form $\Phi(S) = \sum_j V_j S V_j^*$, where $V_j \in \mathrm{Lin}\,(B_1, \ldots, B_p)$, and B_j are the fixed, linearly independent operators of elementary errors.

Theorem 10.3 (Knill and Laflamme [153]). The following statements are equivalent:
i. the code $\mathcal{L}$ corrects errors from $\mathcal{E}$;
ii. the code $\mathcal{L}$ corrects the error $\Phi[S] = \sum_{j=1}^p B_j S B_j^*$;
iii. for all $\phi, \psi \in \mathcal{L}$ such that $\langle \phi \mid \psi \rangle = 0$, one has $\langle \phi | B_i^* B_j | \psi \rangle = 0$ for all $i, j = 1, \ldots p$;
iv. for an orthonormal basis $\{|k\rangle\}$ in $\mathcal{L}$ one has

$$\langle k|B_i^* B_j|k\rangle = \langle l|B_i^* B_j|l\rangle, \quad \text{for all } i,j;k,l,$$
$$\langle k|B_i^* B_j|l\rangle = 0, \quad \text{for } k \neq l;$$

v. $P_{\mathcal{L}} B_i^* B_j P_{\mathcal{L}} = b_{ij} P_{\mathcal{L}}$, where $P_{\mathcal{L}}$ is the projector onto $\mathcal{L}$.

Proof.
i. $\Rightarrow$ ii. This is obvious.
ii. $\Rightarrow$ iii. Let there exist a reverse channel $\mathcal{D}[S] = \sum_r R_r S R_r^*$ for the error Φ. Consider a pure input state $S = |\psi\rangle\langle\psi|, |\psi\rangle \in \mathcal{L}$. In this case,

$$\sum_r \sum_j R_r B_j |\psi\rangle\langle\psi| B_j^* R_r^* = c|\psi\rangle\langle\psi|.$$

But this is possible only if $R_r B_j |\psi\rangle = c_{jr}|\psi\rangle$, in which case $c = \sum_r \sum_j |c_{jr}|^2$.
Let $|\phi\rangle, |\psi\rangle \in \mathcal{L}$ be two orthogonal vectors. Since the reverse channel is tracepreserving, we have $I = \sum_r R_r^* R_r$. Therefore,

$$\langle \phi | B_i^* B_j | \psi \rangle = \sum_r \langle \phi | B_i^* R_r^* R_r B_j | \psi \rangle = \left(\sum_r \overline{c_{ir}} c_{jr} \right) \langle \phi \mid \psi \rangle = 0.$$

iii. $\Rightarrow$ iv. The second equality follows trivially, while the first one is obtained by letting $|\phi\rangle = |k+l\rangle, |\psi\rangle = |k-l\rangle$.
iv. $\Rightarrow$ v. Denoting $b_{ij} = \langle k|B_i^* B_j|k\rangle$, we can write condition iv as

$$\langle k|B_i^* B_j|l\rangle = \delta_{kl} b_{ij}$$

which is equivalent to v .

v. $\Rightarrow$ i. The matrix $[b_{ij}]$ is Hermitian positive, hence there exists a unitary matrix $[u_{ij}]$ such that

$$\sum_{ij} \bar{u}_{ir} b_{ij} u_{js} = \delta_{rs} \lambda_r,$$

where $\lambda_r \geq 0$. Introducing $\tilde{B}_s = \sum_j u_{js} B_j$, we have $\Phi[S] = \sum_{s=1}^{p} \tilde{B}_s S \tilde{B}_s^*$ and

$$P_{\mathcal{L}} \tilde{B}_r^* \tilde{B}_s P_{\mathcal{L}} = \delta_{rs} \lambda_r P_{\mathcal{L}}.$$

Thus, for $\lambda_s > 0$ we have

$$\lambda_s^{-1/2} \tilde{B}_s P_{\mathcal{L}} = U_s P_{\mathcal{L}},$$

where U_s are the partially isometric operators that map $\mathcal{L}$ onto mutually orthogonal subspaces $\mathcal{L}_s \subset \mathcal{H}$. It follows that

$$\Phi[S] = \sum_S \lambda_s U_S S U_s^* \tag{10.5}$$

for any state S with $\operatorname{supp} S \subset \mathcal{L}$.

Let P_s be the projectors onto the subspaces $\mathcal{L}_s$, and denote $P_0 = I - \sum_s P_s$. We define the channel

$$\mathcal{D}[S] = \sum_s U_s^* P_s S P_s U_s + P_0 S P_0$$

and wish to show that it is the reverse for all errors in $\mathcal{E}$. However, a linear combination of elementary errors B_j is also a linear combination of $\tilde{B}_r$ and, taking into account that $U_s^* P_s \tilde{B}_r P_{\mathcal{L}} = \lambda_r^{1/2} \delta_{sr} P_{\mathcal{L}}$, we obtain (10.4) for arbitrary $\Phi \in \mathcal{E}$. $\square$

Exercise 10.4 Check condition iv for the Shor code (10.3) and the elementary error operators given by the Pauli matrices in arbitrary one qubit.

10.10.5 10.1.4 Coherent Information and Perfect Error Correction

We now consider an arbitrary channel Φ from A to B. Let $S = S_A$ be an input state of the channel. Introduce the reference system R so that $S_{AR} = |\psi_{AR}\rangle \langle \psi_{AR}|$ is a purification of S_A. Let $V : \mathcal{H}_A \to \mathcal{H}_B \otimes \mathcal{H}_E$ be the Stinespring isometry (6.7) for the channel Φ, where E is the environment.

An important component of the mutual information $I(S, \Phi)$ is the coherent information

$$\begin{aligned} I_c(S, \Phi) &= H(\Phi[S]) - H(S; \Phi) \\ &= H(B) - H(E) \\ &= H(B) - H(RB) \\ &= -H(R \mid B). \end{aligned}$$

As we shall see later, it is closely related to the quantum capacity of the channel Φ. Somewhat disappointingly, the coherent information does not have several "natural" information properties, such as concavity in S, subadditivity, or the second chain rule. Moreover, it can take negative values. Its classical analog is never positive, $H(Y) - H(XY) = -H(X \mid Y) \leq 0$. However, $I_c(S, \Phi)$ is convex in Φ and satisfies the first chain rule, i.e.,

$$I_c(S, \Phi_2 \circ \Phi_1) \leq I_c(S, \Phi_1) \tag{10.6}$$

as can be seen from the relation $I_c(S,\Phi) = I(S,\Phi) - H(S)$ and from the corresponding properties for the quantum mutual information $I(S,\Phi)$. Let us see why one should not expect the second chain rule, $I_c(S, \Phi_2 \circ \Phi_1) \leq I_c(\Phi_1[S], \Phi_2)$. Assuming that this holds, we would have

$$H(\Phi_2 \circ \Phi_1[S]) - H(S, \Phi_2 \circ \Phi_1) \leq H(\Phi_2 \circ \Phi_1[S]) - H(\Phi_1[S], \Phi_2)$$

i. e., $H(S, \Phi_2 \circ \Phi_1) \geq H(\Phi_1[S], \Phi_2)$. But this is the same as $H(E_1E_2) \geq H(E_2)$, where E_j is the environment for the j th channel. However, such a monotonicity does not hold in general for quantum entropy, as we have noted in Section 7.5.

Exercise 10.5 Show that subadditivity of $I_c(S,\Phi)$ is equivalent to the following inequality:

$$H(B_1B_2) - H(B_1) - H(B_2) \leq H(E_1E_2) - H(E_1) - H(E_2),$$

which need not hold in general.

There is a close relationship between the perfect transmission of quantum information, error correction, and the coherent information.

Definition 10.6. The channel Φ is called perfectly reversible on the state $S = S_A$ if there is a reverse channel $\mathcal{D}$ from B to A, such that

$$(\mathcal{D} \circ \Phi \otimes \mathrm{Id}_R)[S_{AR}] = S_{AR}$$

Proposition 10.7. The following conditions are equivalent:
i. the channel Φ is perfectly reversible on the state S;
ii. $I(R;E) = 0$, i.e., $S_{RE} = S_R \otimes S_E$ (where $S_{RE} = \mathrm{Tr}_B S_{BRE}$);
iii. $I_c(S,\Phi) = H(S)$;
iv. the channel Φ admits a representation (10.5) on the support of the state S.

The meaning of condition ii is that no information goes to the environment, i.e., the channel is "private." Thus, the perfect reversibility of the channel and its perfect privacy are equivalent. Condition iii means that for perfect transmission by the channel Φ of the state S, the coherent information $I_c(S,\Phi)$ should reach its maximal possible value $H(S)$. In particular, by taking $S = \bar{S}_A = I_A/d_A$ - the chaotic state - we obtain the condition $\log d_A = I_C\left(\bar{S}_A, \Phi\right)$. This indicates that the coherent information is the quantity relevant to the quantum capacity of the channel Φ, i.e., the capacity for perfect transmission of quantum states. In the next sections, we shall see that for approximately perfect transmission by the memoryless channel $\Phi^{\otimes n}$, an appropriate analog of these conditions should hold asymptotically, with $n \to \infty$.

Proof.
i. $\Rightarrow$ ii. The vector $|\psi_{BRE}\rangle = (V \otimes I_R)|\psi_{AR}\rangle$ is a vector of the pure state S_{BRE} of the composite system BRE. The perfect reversibility implies

$$(\mathcal{D} \otimes \mathrm{Id}_{RE})[S_{BRE}] = S_{ARE}.$$

Since the partial state S_{AR} is pure, by Corollary 3.12 $S_{ARE} = S_{AR} \otimes S_E$. Taking the partial trace with respect to A, we obtain

$$S_{RE} = S_R \otimes S_E, \tag{10.7}$$

that is, ii.
ii. $\Rightarrow$ iii. We have

$$H(S) - I_c(S,\Phi) = H(A) + H(E) - H(B) \tag{10.8}$$
$$= H(R) + H(E) - H(RE) = I(R;E) \geq 0, \tag{10.9}$$

with equality if and only if $I(R;E)=0$, i. e., $S_{RE}=S_R\otimes S_E$.
ii. $\Rightarrow$ i. The vector $|\psi_{BRE}\rangle=(V\otimes I_R)\,|\psi_{AR}\rangle$ is the vector of joint pure state S_{BRE} of the system BRE, which is a purification of the state S_{RE}. Starting from the right-hand side of (10.7), we obtain another purification $|\psi_{AR}\rangle\otimes|\psi_{EE'}\rangle$, where E' is a purifying system for S_E. By choice of E' we can always assume that this second purification has dimensionality not less than that of the first. Hence, by the remark after Theorem 3.10, there is an isometric operator $W:\mathcal{H}_B\to\mathcal{H}_A\otimes\mathcal{H}_{E'}$ such that

$$(I_{RE}\otimes W)\,|\psi_{BRE}\rangle=|\psi_{AR}\rangle\otimes|\psi_{EE'}\rangle\,. \tag{10.10}$$

Taking the partial trace with respect to E,E' of the corresponding density operator, we obtain the perfect reversibility

$$(\mathrm{Id}_R\otimes\mathcal{D}\circ\Phi)\,[S_{AR}]=S_{AR} \tag{10.11}$$

where the reverse channel is defined as

$$\mathcal{D}\,[S_B]=\mathrm{Tr}_{E'}\,WS_BW^*. \tag{10.12}$$

i. $\Rightarrow$ iv. Later, we shall prove Corollary 10.14, the statement i. $\Leftrightarrow$ iii. of which, with the replacement of Φ by $\mathcal{D}\circ\Phi$, implies that the channel Φ is perfectly reversible on the state S if and only if

$$\mathcal{D}\circ\Phi[\tilde{S}]=\tilde{S}$$

for all $\tilde{S}$ with $\mathrm{supp}\,\tilde{S}\subset\mathcal{L}\equiv\mathrm{supp}\,S$, where $\mathrm{supp}\,S$ is the support of the density operator S (see Section 1.3). We can reformulate this property by saying that Φ is perfectly reversible on the subspace $\mathcal{L}$. In other words, the subspace $\mathcal{L}$ is a quantum code that corrects the error Φ (and hence, all errors of the associated class $\mathcal{E}$). The statement then follows from the proof of Theorem 10.3.

The following proposition provides yet another characterization in terms of complementary channels (see Section 6.6), which prepares the ground for the coding theorem for the private classical capacity of a quantum channel, in Section 10.4.1.

Proposition 10.8. For a given Stinespring dilation of the channel Φ the following conditions are equivalent:
i. the channel Φ is perfectly reversible on the subspace $\mathcal{L}$;
ii. the complementary channel $\tilde{\Phi}$ is completely depolarizing on $\mathcal{L}$, i.e.,

$$\tilde{\Phi}[\tilde{S}]=S_E, \tag{10.13}$$

for any state $\tilde{S}$ with $\mathrm{supp}\,\tilde{S}\subset\mathcal{L}$, where S_E is a fixed state.

Proof.

i. $\Rightarrow$ ii. Assuming Φ is perfectly reversible, the relation (10.10) holds, with an isometric W for all $|\psi_{RA}\rangle$ having a tensor decomposition with A-components in $\mathcal{L}$. Here, $|\psi_{EE'}\rangle$ cannot depend on the input $|\psi_{RA}\rangle$, since otherwise the right-hand side would be nonlinear in $|\psi_{RA}\rangle$. Taking the partial trace with respect to RAE' of the corresponding density operators, we obtain (10.13).
ii. $\Rightarrow$ i. We have a Stinespring dilation $\tilde{\Phi}[\tilde{S}]=\mathrm{Tr}_B\,V\tilde{S}V^*$, where B plays the role of an "environment" for the environment system. Let (10.13) hold and let $|\psi_{EE'}\rangle$ be a purification of S_E. Then there is another Stinespring dilation for the restriction of the channel
$\tilde{\Phi}$ to the states with support in $\mathcal{L}$, i. e.,

$$\tilde{\Phi}[\tilde{S}] = \mathrm{Tr}_{AE'}\, V'\tilde{S}V'^{*}, \tag{10.14}$$

where $V' = I_A \otimes |\psi_{EE'}\rangle$ is an isometric operator from $\mathcal{H}_A$ to $\mathcal{H}_{AEE'} = \mathcal{H}_E \otimes \mathcal{H}_{AE'}$, acting as $V'|\psi\rangle = |\psi\rangle \otimes |\psi_{EE'}\rangle$. In this dilation, the role of an "environment" for the environment E is now played by AE'. By Theorem 6.12, there is a partial isometry $W : \mathcal{H}_B \to \mathcal{H}_{AE'}$ such that

$$(W \otimes I_E)\, V = V' = I_A \otimes |\psi_{EE'}\rangle\,.$$

It follows that relation (10.10) holds for all $|\psi_{RA}\rangle$ having a tensor decomposition with A-components in $\mathcal{L}$. By possibly extending the space $\mathcal{H}_{E'}$ we can replace W with an isometry that preserves relation (10.10). Following a similar argument as in the proof of the previous proposition, we take the partial trace of the corresponding density operator with respect to REE' and obtain the perfect reversibility on $\mathcal{L}$, i.e.,

$$\mathcal{D} \circ \Phi[\tilde{S}] = \tilde{S}, \tag{10.15}$$

where the reverse channel is defined by (10.12). □

10.10.6 10.2 Fidelities for Quantum Information

As a measure of exactness of the transmission of a quantum state S by the channel Φ one could take the trace norm $\|S - \Phi[S]\|_1$. However, in quantum information theory there are a number of other useful quantities playing the same role as the probability of a correct decision in the classical case. Let us first consider these quantities and study the relations between them.

10.10.7 10.2.1 Fidelities for Pure States

Lemma 10.9. Let ψ be a unit vector and S an arbitrary state. Then the following inequalities hold:

$$2[1 - \langle\psi|S|\psi\rangle] \leqslant \||\psi\rangle\langle\psi| - S\|_1 \leqslant 2\sqrt{1 - \langle\psi|S|\psi\rangle}. \tag{10.16}$$

If $S = |\phi\rangle\langle\phi|$ is a pure state, the second inequality turns into equality, i.e.,

$$\||\psi\rangle\langle\psi| - |\phi\rangle\langle\phi|\|_1 = 2\sqrt{1 - |\langle\psi \mid \phi\rangle|^2}. \tag{10.17}$$

Proof. By using (1.19) we have

$$\||\psi\rangle\langle\psi| - S\|_1 = \max_U |\,\mathrm{Tr}(|\psi\rangle\langle\psi| - S)U|,$$

where the maximum is over all unitary operators U. Taking $U = 2|\psi\rangle\langle\psi| - I$ produces the first inequality.

Equality (10.17) is obtained similar to relation (2.44). To compute the trace norm, it is sufficient to find the eigenvalues of the operator $|\psi\rangle\langle\psi| - |\phi\rangle\langle\phi|$, which has rank two (see Proposition 2.26).

Now, let S be an arbitrary density operator and consider its spectral decomposition $S = \sum \lambda_i S_i$. By using the convexity of the norm, the concavity of the square root, and relation (10.17), we obtain

$$\begin{aligned}\||\psi\rangle\langle\psi| - S\|_1 &\leq \sum_i \lambda_i \||\psi\rangle\langle\psi| - S_i\|_1 \\ &= 2\sum_i \lambda_i \sqrt{1 - \langle\psi|S_i|\psi\rangle} \leq 2\sqrt{1 - \langle\psi|S|\psi\rangle}.\end{aligned}$$

□

For a pure state $|\psi\rangle\langle\psi|$ and an arbitrary state S, the quantity

$$F(|\psi\rangle\langle\psi|, S) = \langle\psi|S|\psi\rangle \tag{10.18}$$

is called the fidelity between the pure state $|\psi\rangle\langle\psi|$ and the state S. Clearly, $F \leq 1$, with equality if and only if $S = |\psi\rangle\langle\psi|$. Note that in quantum data compression (Section 5.5) we in fact used the fidelity (10.18). There, the state $|\psi_i\rangle\langle\psi_i|$ appeared with probability p_i. Hence, the average fidelity is just $\bar{F} = \sum_i p_i \langle\psi_i| S_i |\psi_i\rangle$.

In connection with error-correcting codes, a natural definition of fidelity is as follows. Let a subspace (quantum code) $\mathcal{L} \subset \mathcal{H}$ and a channel Φ in $\mathcal{H}$, for which the input and output spaces coincide $\mathcal{H}_B = \mathcal{H}_A = \mathcal{H}$, be given. The subspace fidelity is defined as

$$\begin{aligned} F_s(\mathcal{L}, \Phi) &= \min_{\psi\in\mathcal{L}, \|\psi\|=1} F(|\psi\rangle\langle\psi|, \Phi[|\psi\rangle\langle\psi|]) \\ &= \min_{\psi\in\mathcal{L}, \|\psi\|=1} \langle\psi|\Phi[|\psi\rangle\langle\psi|]|\psi\rangle. \end{aligned}$$

By Lemma 10.9,

$$2\left[1 - F_s(\mathcal{L}, \Phi)\right] \leq \max_{\psi\in\mathcal{L}, \|\psi\|=1} \| |\psi\rangle\langle\psi| - \Phi[|\psi\rangle\langle\psi|] \|_1 \leq 2\sqrt{1 - F_s(\mathcal{L}, \Phi)}. \tag{10.19}$$

Another important quantity is the entanglement fidelity $F_e(S, \Phi)$, defined as follows. Let us purify the state $S = S_A$ to $|\psi_{AR}\rangle\langle\psi_{AR}|$ in the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_R$ and consider the fidelity for this pure state under the action of the trivial extension of the channel

$$F_e(S, \Phi) = \langle\psi_{AR}| \left(\Phi \otimes \mathrm{Id}_R\right) \left(|\psi_{AR}\rangle\langle\psi_{AR}|\right) |\psi_{AR}\rangle .$$

There is another convenient expression for $F_e(S, \Phi)$, which also shows independence of this definition of the way of purification of the initial state.

Lemma 10.10. Let the channel have the Kraus representation

$$\Phi[S] = \sum_i V_i S V_i^* \tag{10.20}$$

Then

$$F_e(S, \Phi) = \sum_i |\mathrm{Tr}\, V_i S|^2 \tag{10.21}$$

Proof. Indeed,

$$\begin{aligned} \langle\psi_{AR}| \sum_i \left(V_i \otimes I_R\right) |\psi_{AR}\rangle\langle\psi_{AR}| \left(V_i \otimes I_R\right)^* |\psi_{AR}\rangle &= \sum_i \left| \langle\psi_{AR}| \left(V_i \otimes I_R\right) \right| \psi_{AR} \Big\rangle \Big|^2 \\ &= \sum_i |\mathrm{Tr}\, V_i S|^2 . \end{aligned}$$

□

Note that for a pure state $S = |\psi\rangle\langle\psi|$,

$$F_e(S, \Phi) = \langle\psi|\Phi[|\psi\rangle\langle\psi|]|\psi\rangle = F(|\psi\rangle\langle\psi|, \Phi[|\psi\rangle\langle\psi|]).$$

Exercise 10.11 Prove that $F_e(S, \Phi)$ is a convex function of S. Hint: by (10.21), $F_e(S, \Phi)$ is the sum of squares of affine functions of S.

10.10.8 10.2.2 Relations Between the Fidelity Measures

Lemma 10.12. For an arbitrary state S

$$1 - F_e(S, \Phi) \leq 4\sqrt{1 - F_S(\operatorname{supp} S, \Phi)}$$

Proof. We have

$$\begin{aligned} 1 - F_e(S, \Phi) &= 1 - \langle \psi_{AR}| \left(\Phi \otimes \mathrm{Id}_R\right) \left(|\psi_{AR}\rangle \langle \psi_{AR}|\right) |\psi_{AR}\rangle \\ &= \langle \psi_{AR}| \left((\mathrm{Id}_A - \Phi) \otimes \mathrm{Id}_R\right) \left[|\psi_{AR}\rangle \langle \psi_{AR}|\right] |\psi_{AR}\rangle \end{aligned}$$

Representing $|\psi_{AR}\rangle = \sum_j |\psi_j\rangle \otimes |e_j\rangle$, where $\{|e_j\rangle\}$ is an orthonormal basis in $\mathcal{H}_R$, $\sum_j \|\psi_j\|^2 = 1, \psi_j \in \operatorname{supp} S$, we obtain the equivalent relation

$$\sum_{jk} \langle \psi_j| \left(\mathrm{Id} - \Phi\right) \left[|\psi_j\rangle \langle \psi_k|\right] |\psi_k\rangle = \sum_{jk} \operatorname{Tr} |\psi_k\rangle \langle \psi_j| \left(|\psi_j\rangle \langle \psi_k| - \Phi\left[|\psi_j\rangle \langle \psi_k|\right]\right).$$

Taking into account inequality (1.18) and the fact that the operators $|\psi_j\rangle \langle \psi_k|$ all have both trace and operator norms equal to $\|\psi_j\| \, \|\psi_k\|$, we obtain that this does not exceed

$$\max_T \frac{\|T - \Phi[T]\|_1}{\|T\|_1},$$

where the maximum is taken over all nonzero operators T acting in $\mathcal{L} = \operatorname{supp} S$. By decomposing $T = T_1 + iT_2$, where $T_1^* = T_1, T_2^* = T_2$ again act in $\mathcal{L}$, and taking into account that $\|T_{1,2}\|_1 \leq \|T\|_1$, as well as the triangle inequality, we infer that this does not exceed the following quantity:

$$2 \max_{T^* = T} \frac{\|T - \Phi[T]\|_1}{\|T\|_1} = 2 \max_{S : \operatorname{supp} S \in \mathcal{L}} \|S - \Phi[S]\|_1. \tag{10.22}$$

Here, the inequality $\geq$ is obtained by restricting ourselves to positive T. On the other hand,

$$\max_{T^* = T} \frac{\|T - \Phi[T]\|_1}{\|T\|_1} \leq \|S_+ - \Phi\left[S_+\right]\|_1 \frac{p_+}{p_+ + p_-} + \|S_- - \Phi\left[S_-\right]\|_1 \frac{p_-}{p_+ + p_-}, \tag{10.23}$$

where we denoted $p_\pm = \operatorname{Tr} T_\pm; S_\pm = p_\pm^{-1} T_\pm$. Here, the right-hand side is less than or equal to the right-hand side in the relation (10.22), which is thus proved. Finally,

$$\max_{S : \operatorname{supp} S \in \mathcal{L}} \|S - \Phi[S]\|_1 = \max_{\psi : \psi \in \mathcal{L}, \|\psi\| = 1} \| |\psi\rangle\langle\psi| - \Phi[|\psi\rangle\langle\psi|]\|_1,$$

since the maximum of a convex function is attained at an extreme point of the convex set. By using the second inequality from (10.19), we obtain that the expression does not exceed $4\sqrt{1 - F_s(\mathcal{L}, \Phi)}$. $\square$

Exercise 10.13 By using the convexity property from Exercise 10.11, prove the inequality

$$1 - F_s(\mathcal{L}, \Phi) \leq 1 - \min_{S : \operatorname{supp} S \subset \mathcal{L}} F_e(S, \Phi). \tag{10.24}$$

Now, let $\mathcal{L} = \mathcal{H}$. In this case,

$$\max_T \frac{\|T - \Phi[T]\|_1}{\|T\|_1} = \|\mathrm{Id} - \Phi\|.$$

From the proof of Lemma 10.12, we have the chain of inequalities

$$1 - \min_S F_e(S,\Phi) \le \|\mathrm{Id} - \Phi\| \le 2 \max_{\|\psi\|=1} \| |\psi\rangle\langle\psi| - \Phi[|\psi\rangle\langle\psi|] \|_1 \le 2\| \mathrm{Id} - \Phi\|. \tag{10.25}$$

Together with relation (10.24) this means that a deviation of the channel Φ from the ideal channel Id is equivalently described by one of the quantities

$$\|\mathrm{Id} - \Phi\|, \quad \max_S \|S - \Phi[S]\|_1, \quad 1 - F_S(\mathcal{H},\Phi), \quad 1 - \min_S F_e(S,\Phi)$$

In the consideration of the quantum capacity we will need the following obvious corollary of Lemma 10.12:

$$1 - F_e(\bar{S},\Phi) \le 4\sqrt{1 - F_s(\mathcal{H},\Phi)}, \tag{10.26}$$

where $\bar{S}$ is the chaotic state in $\mathcal{H}$.

It is instructive to consider the "ideal" case of the unit fidelities.

Corollary 10.14. The following conditions are equivalent:

i. $F_e(S,\Phi) = 1$;

ii. $F_S(\mathrm{supp}\, S,\Phi) = 1$;

iii. $\Phi[\tilde{S}] = \tilde{S}$ for arbitrary state $\tilde{S}$ with $\mathrm{supp}\,\tilde{S} \subset \mathrm{supp}\, S$;

iv. $F_e(\tilde{S},\Phi) = 1$ for arbitrary state $\tilde{S}$ with $\mathrm{supp}\,\tilde{S} \subset \mathrm{supp}\, S$.

Proof. Let us prove i. $\Rightarrow$ ii. Let $|\psi\rangle \in \mathrm{supp}\, S$. In this case, we can write

$$S = p|\psi\rangle\langle\psi| + (1-p)S',$$

where $p > 0$ and S' is a density operator. By Exercise 10.11, the function $S \to F_e(S,\Phi)$ is convex. Therefore,

$$pF_e(|\psi\rangle\langle\psi|,\Phi) + (1-p)F_e\,(S',\Phi) \ge F_e(S,\Phi) = 1$$

and hence $F_e(|\psi\rangle\langle\psi|,\Phi) = 1$. But this means that

$$\langle\psi|\Phi[|\psi\rangle\langle\psi|]|\psi\rangle = 1$$

for all $|\psi\rangle \in \mathrm{supp}\, S$ and $F_s(\mathrm{supp}\, S,\Phi) = 1$.

Lemma 10.12 implies ii. $\Rightarrow$ i. Moreover, since ii obviously implies the same condition, with $\mathrm{supp}\,\tilde{S}$ instead of $\mathrm{supp}\, S$, it also implies iv, which is formally stronger than i.

By the definition of F_S, ii is equivalent to iii for pure, and, hence, for mixed states $\tilde{S}$.

10.10.9 10.2.3 Fidelity and the Bures Distance

Here, we discuss the fidelity between two arbitrary mixed states. This material will be needed only in Section 10.4.4.

For pure states $S = |\phi\rangle\langle\phi|, T = |\psi\rangle\langle\psi|$, the fidelity is equal to $F(T,S) = |\langle\phi \mid \psi\rangle|^2$, and formula (10.17) provides the relation between the fidelity and the trace norm distance between S, T. Now, let S, T be arbitrary density operators.

Definition 10.15. The fidelity between the density operators S, T is defined by the relation

$$F(T,S) = \max |\langle\psi_T \mid \psi_S\rangle|^2 \tag{10.27}$$

where the maximum is taken over all possible purifications ψ_S, ψ_T of the states S, T (in the same Hilbert space $\mathcal{H} \otimes \mathcal{H}'$).

By using Theorem 3.11, we see that

$$F(T,S) = \max_W |\langle \psi_T \mid (I \otimes W)\psi_S \rangle|^2 , \tag{10.28}$$

where now ψ_S, ψ_T are fixed purifications of the states S, T in a fixed Hilbert space $\mathcal{H} \otimes \mathcal{H}'$, and the maximum is taken over all unitary operators W in $\mathcal{H}'$. In particular, taking the purifications $\sqrt{S}, \sqrt{T}$ in $L^2(\mathcal{H}) \simeq \mathcal{H} \otimes \mathcal{H}^*$ we obtain

$$F(T,S) = \max_W |\operatorname{Tr} \sqrt{S}\sqrt{T}W|^2,$$

where the maximum is over all unitary operators W in $\mathcal{H}$. By using the polar decomposition of the operator $\sqrt{S}\sqrt{T} = U|\sqrt{S}\sqrt{T}|$, one sees that the maximum is achieved for $W = U^*$ and is equal to

$$F(T,S) = (\operatorname{Tr} |\sqrt{S}\sqrt{T}|)^2 = \|\sqrt{S}\sqrt{T}\|_1^2.$$

This coincides with (10.18) for $T = |\psi\rangle\langle\psi|$. Note that the above argument implies that in the definition (10.27) we can restrict ourselves to maximization with respect to all purifications of only one of the states, with a fixed purification of another.

Exercise 10.16 Show that $F(T,S) \leq 1$, with equality if and only if $T = S$.

Related to the fidelity (10.27), there is a metric on the set of all states, called the Bures distance, namely,

$$\beta(T,S) = \min \|\psi_T - \psi_S\| , \tag{10.29}$$

where the minimum is again taken over all possible purifications ψ_S, ψ_T of the states S, T. Taking the square of the norm and using the definition (10.27), one obtains

$$\beta(T,S) = \sqrt{2(1 - \sqrt{F(T,S)})} = \sqrt{2\left(1 - \|\sqrt{S}\sqrt{T}\|_1\right)}. \tag{10.30}$$

In particular, for pure states $T = |\psi\rangle\langle\psi|, S = |\phi\rangle\langle\phi|$,

$$\beta(T,S) = \sqrt{2(1 - |\langle\psi \mid \phi\rangle|)}.$$

It also follows that, just as in the definition of fidelity, in the definition (10.29) we can restrict ourselves to minimization with respect to all purifications of only one of the states, with a fixed purification of another.

The triangle inequality for $\beta(T,S)$ then follows from the definition (10.29) and the corresponding inequality for the norm. For pure states, it reduces to

$$\sqrt{1 - |\langle\varphi \mid \psi\rangle|} \leq \sqrt{1 - |\langle\varphi \mid \chi\rangle|} + \sqrt{1 - |\langle\chi \mid \psi\rangle|}, \tag{10.31}$$

where φ, χ, ψ are arbitrary unit vectors.

Lemma 10.17. For any two density operators S_1, S_2 in $\mathcal{H}$,

$$\beta\left(S_1, S_2\right)^2 \leq \|S_1 - S_2\|_1 \leq 2\beta\left(S_1, S_2\right), \tag{10.32}$$

The first inequality, combined with (10.30) and (10.28), implies the following.

Corollary 10.18. For any two density operators S_1, S_2 in $\mathcal{H}$ and their given purifications ψ_{S_1}, ψ_{S_2} in $\mathcal{H} \otimes \mathcal{H}'$,

$$\|S_1 - S_2\|_1 \geq 2\left(1 - \max_W |\langle\psi_{S_1} \mid (I \otimes W)\psi_{S_2}\rangle|\right), \tag{10.33}$$

where the maximum is taken over all unitary operators W in $\mathcal{H}'$.

Proof of Lemma 10.17. Since $\operatorname{Tr}\sqrt{S_1}\sqrt{S_2} \le \operatorname{Tr}\left|\sqrt{S_1}\sqrt{S_2}\right|$, to prove the first inequality in (10.32) it is sufficient to prove that

$$2\left(1 - \operatorname{Tr}\sqrt{S_1}\sqrt{S_2}\right) \le \|S_1 - S_2\|_1 .$$

This in turn follows from the more general inequality

$$\operatorname{Tr}\left(\sqrt{S_1} - \sqrt{S_2}\right)^2 \le \|S_1 - S_2\|_1 ,$$

valid for arbitrary positive S_1, S_2. To prove this, for a Hermitian operator K, we denote by $1_+(K)$ (resp. $1_-(K)$) the spectral projector corresponding to positive (resp. nonpositive) eigenvalues. In this case, $\sigma(K) = 1_+(K) - 1_-(K)$ is a unitary Hermitian operator that satisfies $\sigma(K)K = K\sigma(K) = |K|$. Denoting $K = \sqrt{S_1} - \sqrt{S_2}, L = \sqrt{S_1} + \sqrt{S_2}$, we have $S_1 - S_2 = \frac{1}{2}(KL + LK) \equiv K \circ L$. Hence,

$$\begin{aligned}\|S_1 - S_2\|_1 \ge |\operatorname{Tr}\sigma(K)K \circ L| &= \operatorname{Tr}|K|L \\ &= \operatorname{Tr}|K|\left(1_+(K)L1_+(K) + 1_-(K)L1_-(K)\right).\end{aligned}$$

Since $L \ge K \ge -L$, we have $1_+(K)L1_+(K) \ge 1_+(K)K$ and $1_-(K)L1_-(K) \ge -1_-(K)K$. Thus, $(1_+(K)L1_+(K) + 1_-(K)L1_-(K)) \ge |K|$, and therefore

$$\|S_1 - S_2\|_1 \ge \operatorname{Tr}|K|^2 = \operatorname{Tr}\left(\sqrt{S_1} - \sqrt{S_2}\right)^2 .$$

To prove the second inequality in (10.32), let $S_1 = T_1^*T_1, S_2 = T_2^*T_2$ for some not necessarily Hermitian T_1, T_2. Denoting $K = T_1 - T_2, L = T_1 + T_2$, we have

$$\begin{aligned}\|S_1 - S_2\|_1 &= \operatorname{Tr}\sigma\left(S_1 - S_2\right)\left(S_1 - S_2\right) \\ &= \frac{1}{2}\left[\operatorname{Tr}\sigma\left(S_1 - S_2\right)K^*L + \operatorname{Tr}\sigma\left(S_1 - S_2\right)L^*K\right]\end{aligned}$$

By using the Cauchy-Schwarz inequality for the trace, we obtain

$$\left|\operatorname{Tr}\sigma\left(S_1 - S_2\right)K^*L\right| \le \left[\operatorname{Tr}\sigma\left(S_1 - S_2\right)^2 K^*K \cdot \operatorname{Tr}L^*L\right]^{\frac{1}{2}} = \left[\operatorname{Tr}K^*K \cdot \operatorname{Tr}L^*L\right]^{\frac{1}{2}},$$

and similarly for the second term. Thus, $\|S_1 - S_2\|_1 \le \left[\operatorname{Tr}K^*K \cdot \operatorname{Tr}L^*L\right]^{\frac{1}{2}}$. Using the normalization of S_1, S_2, we obtain

$$\operatorname{Tr}K^*K = 2\left(1 - \operatorname{Re}\operatorname{Tr}T_1^*T_2\right), \quad \operatorname{Tr}L^*L = 2\left(1 + \operatorname{Re}\operatorname{Tr}T_1^*T_2\right).$$

Take $T_1 = \sqrt{S_1}, T_2 = U\sqrt{S_2}$, where U is the unitary from the polar decomposition of $\sqrt{S_1}\sqrt{S_2}$. Then $\operatorname{Re}\operatorname{Tr}T_1^*T_2 = \operatorname{Re}\operatorname{Tr}T_2^*T_1 = \operatorname{Tr}\left|\sqrt{S_1}\sqrt{S_2}\right|$. Thus,

$$\begin{aligned}\operatorname{Tr}K^*K &= 2\left(1 - \left\|\sqrt{S_1}\sqrt{S_2}\right\|_1\right) = \beta\left(S_1, S_2\right)^2 \\ \operatorname{Tr}L^*L &= 2\left(1 + \left\|\sqrt{S_1}\sqrt{S_2}\right\|_1\right) \le 4\end{aligned}$$

and the second inequality in (10.32) follows.

10.10.10 10.3 The Quantum Capacity

10.10.11 10.3.1 Achievable Rates

Let $\Phi : \mathfrak{T}(\mathcal{H}_A) \to \mathfrak{T}(\mathcal{H}_B)$ be a quantum channel. Consider the composite channel $\Phi^{\otimes n} : \mathfrak{T}\left(\mathcal{H}_A^{\otimes n}\right) \to \mathfrak{T}\left(\mathcal{H}_B^{\otimes n}\right)$.

Definition 10.19. A number $R \geq 0$ is called the achievable rate (for the transmission of quantum information) if there exist a sequence of spaces $\mathcal{H}^{(n)}$ such that

$$\overline{\lim_{n\to\infty}} \frac{1}{n} \log \dim \mathcal{H}^{(n)} = R$$

and sequences of channels $\mathcal{E}^{(n)} : \mathfrak{T}\left(\mathcal{H}^{(n)}\right) \to \mathfrak{T}\left(\mathcal{H}_A^{\otimes n}\right)$ (encodings) and $\mathcal{D}^{(n)} : \mathfrak{T}\left(\mathcal{H}_B^{\otimes n}\right) \to \mathfrak{T}\left(\mathcal{H}^{(n)}\right)$ (decodings) such that

$$\lim_{n\to\infty} F_s\left(\mathcal{H}^{(n)}, \mathcal{D}^{(n)} \circ \Phi^{\otimes n} \circ \mathcal{E}^{(n)}\right) = 1 \tag{10.34}$$

The least upper bound of achievable rates will be denoted $Q(\Phi)$ and called the quantum capacity of the channel Φ.

The following data-processing inequality is useful for obtaining bounds on the quantum capacity.

Proposition 10.20. For any two channels Φ_1, Φ_2

$$Q(\Phi_2 \circ \Phi_1) \leq \min\{Q(\Phi_1), Q(\Phi_2)\}. \tag{10.35}$$

In particular, if one of these channels has zero quantum capacity, so does their concatenation.

Proof. To show that $Q(\Phi_2 \circ \Phi_1) \leq Q(\Phi_2)$, it suffices to observe that $Q(\Phi_2 \circ \Phi_1)$ is equal to the supremum of the achievable rates for channel Φ_2 over the special class of encodings, including post-processing with channel Φ_1. Hence, it does not exceed $Q(\Phi_2)$. The inequality $Q(\Phi_2 \circ \Phi_1) \leq Q(\Phi_1)$ is proved similarly by considering decodings for Φ_1, including preprocessing with channel Φ_2. □

Note that essentially the same reasoning implies a similar inequality for the classical capacity,

$$C(\Phi_2 \circ \Phi_1) \leq \min\{C(\Phi_1), C(\Phi_2)\}, \tag{10.36}$$

while for the classical entanglement-assisted capacity C_{ea} this can be derived from the data-processing inequality for quantum mutual information (Proposition 7.31, property iv), taking into account expression (9.4).

In the proof of the classical coding theorem it was much more convenient to use the average error probability instead of the maximal error probability, as the two criteria were shown to be equivalent in Lemma 4.11. In the quantum case, the role of the average error is played by the quantity $1 - F_e\left(\bar{S}^{(n)}, \mathcal{D}^{(n)} \circ \Phi^{\otimes n} \circ \mathcal{E}^{(n)}\right)$, where $\bar{S}^{(n)} = \frac{1}{d_n} I_{\mathcal{H}^{(n)}}$ is the chaotic state in $\mathcal{H}^{(n)}$, while the analog of the maximal error is $1 - F_s\left(\mathcal{H}^{(n)}, \mathcal{D}^{(n)} \circ \Phi^{\otimes n} \circ \mathcal{E}^{(n)}\right)$. Indeed, $F_S\left(\mathcal{H}^{(n)}, \mathcal{D}^{(n)} \circ \Phi^{\otimes n} \circ \mathcal{E}^{(n)}\right) \to 1$ implies $F_e\left(\bar{S}^{(n)}, \mathcal{D}^{(n)} \circ \Phi^{\otimes n} \circ \mathcal{E}^{(n)}\right) \to 1$ (according to Lemma 10.12). In the reverse direction, there is the following noncommutative analog of Lemma 4.11.

Lemma 10.21. Let $\mathcal{H}$ be a Hilbert space of dimensionality $2d$ and Φ a channel in $\mathcal{H}$. There exists a subspace $\mathcal{H}'$ of dimensionality d such that

$$1 - F_S(\mathcal{H}', \mathcal{D}' \circ \Phi) \leq 2\left(1 - F_e(\bar{S}, \Phi)\right)$$

where $\bar{S} = \frac{1}{2d} I_{\mathcal{H}}$, and $\mathcal{D}'[S] = P'SP' + \frac{P'}{d} \operatorname{Tr}(I - P')S$ for all $S \in \mathfrak{S}(\mathcal{H})$ with P' being the projector onto $\mathcal{H}'$.

Proof. On the unit ball of $\mathcal{H}$, consider the continuous function $|\psi\rangle \to f(\psi) = \langle\psi|\Phi[|\psi\rangle\langle\psi|]|\psi\rangle = F_e(|\psi\rangle\langle\psi|, \Phi)$. Let $|\psi_1\rangle$ be a vector minimizing $f(\psi)$. Define

the orthonormal basis $\{|\psi_j\rangle\,; j = 1, \ldots, 2d\}$ in $\mathcal{H} \equiv \mathcal{H}_0$ by the following recurrent procedure: $|\psi_{j+1}\rangle$ is the vector in the subspace $\mathcal{H}_j = \{|\psi_1\rangle, \ldots, \psi_j\rangle\}^\perp$ that minimizes $f(\psi)$. Then $\mathcal{H}_j \supset \mathcal{H}_{j+1}$ and $\dim \mathcal{H}_j = 2d - j$. By the convexity of $F_e(S, \Phi)$ (see Exercise 10.11), we obtain

$$\begin{aligned} 1 - F_e(\bar{S}, \Phi) &\geq \frac{1}{2d} \sum_{j=1}^{2d} \left(1 - F_e\left(|\psi_j\rangle \langle\psi_j|, \Phi\right)\right) \\ &\geq \frac{1}{2d} \sum_{j=d+1}^{2d} \left(1 - f\left(\psi_j\right)\right) \\ &\geq \frac{1}{2} \left(1 - \min_{|\psi\rangle \in \mathcal{H}_d} f(\psi)\right) \\ &\geq \frac{1}{2} \left(1 - F_s\left(\mathcal{H}', \mathcal{D}' \circ \Phi\right)\right), \end{aligned}$$

where $\mathcal{H}' = \mathcal{H}_d$.

From this lemma, together with inequality (10.26), it follows that in the definition of achievable rates we can replace (10.34) by

$$\lim_{n\to\infty} F_e\left(\bar{S}^{(n)}, \mathcal{D}^{(n)} \circ \Phi^{\otimes n} \circ \mathcal{E}^{(n)}\right) = 1 \tag{10.37}$$

Corollary 10.22. Any PPT channel (in particular, an entanglement-breaking channel) has zero quantum capacity.

Proof. In this proof, we denote by T the operations of transposition in different spaces, which will be clear from the context. By using (6.31), we have

$$\begin{aligned} F_e\left(\bar{S}^{(n)}, \mathcal{D}^{(n)} \circ \Phi^{\otimes n} \circ \mathcal{E}^{(n)}\right) &= F_e\left(\bar{S}^{(n)}, \mathcal{D}^{(n)} \circ T \circ T \circ \Phi^{\otimes n} \circ \mathcal{E}^{(n)}\right) \\ &= F_e\left(\bar{S}^{(n)}, T \circ \Phi_n\right) \end{aligned}$$

where $\Phi_n = \left(\mathcal{D}^{(n)}\right)^\top \circ (T \circ \Phi^{\otimes n}) \circ \mathcal{E}^{(n)}$ is a channel, because by Proposition 6.27 $T \circ \Phi^{\otimes n}$ is a channel. Now,

$$\begin{aligned} F_e\left(\bar{S}^{(n)}, T \circ \Phi_n\right) &= \left\langle \Omega^{(n)} \right| \left(\mathrm{Id}_{\mathcal{H}^{(n)}} \otimes T \circ \Phi_n\right) \left[\left|\Omega^{(n)}\right\rangle \left\langle \Omega^{(n)}\right|\right] \left|\Omega^{(n)}\right\rangle \\ &= \mathrm{Tr} \left|\Omega^{(n)}\right\rangle \left\langle \Omega^{(n)}\right| \left(\mathrm{Id}_{\mathcal{H}^{(n)}} \otimes T \circ \Phi_n\right) \left[\left|\Omega^{(n)}\right\rangle \left\langle \Omega^{(n)}\right|\right] \\ &= \mathrm{Tr} \left(\mathrm{Id}_{\mathcal{H}^{(n)}} \otimes T\right) \left[\left|\Omega^{(n)}\right\rangle \left\langle \Omega^{(n)}\right|\right] \left(\mathrm{Id}_{\mathcal{H}^{(n)}} \otimes \Phi_n\right) \left[\left|\Omega^{(n)}\right\rangle \left\langle \Omega^{(n)}\right|\right], \end{aligned}$$

where

$$\left|\Omega^{(n)}\right\rangle = \frac{1}{\sqrt{d_n}} \sum_{m=1}^{d_n} |m\rangle \otimes |m\rangle \tag{10.38}$$

is the maximally entangled vector in $\mathcal{H}^{(n)} \otimes \mathcal{H}^{(n)}$.

Introducing the Kraus decomposition $\Phi_n[S] = \sum_k V_k S V_k^*$, we obtain, by using (10.38), that the last expression for F_e is evaluated as

$$\begin{aligned} \frac{1}{d_n^2} \sum_k \sum_{l,m=1}^{d_n} \langle m|V_k|l\rangle \langle m|V_k^*|l\rangle \leq \frac{1}{d_n^2} \sum_k \sum_{l,m=1}^{d_n} \left|\langle m|V_k|\, l\right\rangle|^2 &= \frac{1}{d_n^2} \sum_k \mathrm{Tr}\, V_k^* V_k \\ &= \frac{1}{d_n} \end{aligned}$$

Thus, for arbitrary encodings and decodings $F_e\left(\bar{S}^{(n)}, \mathcal{D}^{(n)} \circ \Phi^{\otimes n} \circ \mathcal{E}^{(n)}\right) = d_n^{-1} \leq 1/2$ implying $Q(\Phi) = 0$.

Now, let us show that in the definition of the quantum capacity we can restrict ourselves to isometric encodings, i.e., to those which have the form

$$\mathcal{E}[S] = \operatorname{Ad} V[S] \equiv VSV^*, \tag{10.39}$$

where V is an isometric mapping of the space $\mathcal{H}^{(n)}$ into the input space $\mathcal{H}^{\otimes n}$ of the channel. We shall prove that if there is an encoding of a general form which achieves high fidelity for a given state, there also is an isometric encoding with a similar property. To explain this on an intuitive level, consider the case of perfect transmission. If the concatenation encoding-channel-decoding perfectly reproduces some state S, the encoding channel $\mathcal{E}$ is perfectly reversible on S, with the concatenation channel-decoding as the reverse channel. In this case, according to Proposition 10.7 the channel $\mathcal{E}$ on $\operatorname{supp} S$ can be represented in the form (10.5) as a convex combination of isometric encodings $\mathcal{U}_j = \operatorname{Ad} U_j$. Hence, any channel $\mathcal{U}_j$ is perfectly reversible on S with the same reverse channel.

Lemma 10.23. Let S be a state in a Hilbert space $\mathcal{L}, \mathcal{L} = \operatorname{supp} S$, let $\mathcal{E}$ be a completely positive map from $\mathfrak{T}(\mathcal{L})$ to $\mathfrak{T}(\mathcal{H})$, such that $\operatorname{Tr} \mathcal{E}[S] = 1$, and let $\mathcal{A}$ be a channel from $\mathfrak{T}(\mathcal{H})$ to $\mathfrak{T}(\mathcal{L})$. Assume that $\dim \mathcal{L} \leq \dim \mathcal{H}$. Then there exists an isometry V from $\mathcal{L}$ to $\mathcal{H}$ such that

$$F_e(S, \mathcal{A} \circ \operatorname{Ad} V) \geq F_e(S, \mathcal{A} \circ \mathcal{E})^2. \tag{10.40}$$

This lemma will be used in the situation where $\mathcal{E}$ is the encoding map, while $\mathcal{A}$ is the concatenation channel-decoding. For the proof, we need the following generalization of the polar decomposition. If X is an operator from $\mathcal{L}$ to $\mathcal{H}, \dim \mathcal{L} \leq \dim \mathcal{H}$, then $X = V|X|$, where $|X| = \sqrt{X^*X}$ is a positive operator in $\mathcal{L}$ and V is an isometry from $\mathcal{L}$ to $\mathcal{H}$. This implies the following representation for an arbitrary square matrix X : $X = VDU$, where D is a diagonal matrix with nonnegative elements, and V, U are unitary matrices.

Proof. Let $A_i : \mathcal{H} \to \mathcal{L}$ and $E_j : \mathcal{L} \to \mathcal{H}$ be the components of the Kraus decomposition for the maps $\mathcal{A}$ and $\mathcal{E}$, respectively. Denote by X the matrix with the elements $X_{ij} = \operatorname{Tr} A_i E_j S$. Then, by (10.21),

$$F_e(S, \mathcal{A} \circ \mathcal{E}) = \sum_{ij} |X_{ij}|^2 .$$

Complementing the Kraus decompositions, if necessary, with additional zero components, we may assume that X is a square matrix. The decomposition $X = VDU$ implies that by transforming the Kraus decompositions for $\mathcal{A}$ and $\mathcal{E}$, we can make the matrix X diagonal. Then again using (10.21), we obtain $F_e(S, \mathcal{A} \circ \mathcal{E}) = \sum_k |\operatorname{Tr} A_k E_k S|^2$. We denote $\lambda_k = \operatorname{Tr} S E_k^* E_k$, and we restrict ourselves to $\lambda_k > 0$. Then $\sum_k \lambda_k \left(|\operatorname{Tr} A_k E_k S|^2 / \lambda_k \right) =$
$F_e(S, \mathcal{A} \circ \mathcal{E})$ and $\sum_k \lambda_k = 1$, so that there exists a k such that $|\operatorname{Tr} A_k E_k S|^2 / \lambda_k \geq F_e(S, \mathcal{A} \circ \mathcal{E})$. Setting $E = E_k / \sqrt{\lambda_k} : \mathcal{L} \to \mathcal{H}, A = A_k : \mathcal{H} \to \mathcal{L}$, we have $A^*A \leq I_{\mathcal{H}}, \operatorname{Tr} S E^* E = 1$, and

$$F_e(S, \mathcal{A} \circ \mathcal{E}) \leq F_e(S, \operatorname{Ad} A \circ \operatorname{Ad} E) = |\operatorname{Tr} AES|^2.$$

Let $A^* = V |A^*|$ be the polar decomposition of the operator $A^* : \mathcal{L} \to \mathcal{H}$, where $V : \mathcal{L} \to \mathcal{H}$ is an isometry. According to the noncommutative Cauchy-Schwarz inequality (2.24)

$$|\operatorname{Tr} AES|^2 = |\operatorname{Tr} SAE|^2 \leq \operatorname{Tr} SAA^* \operatorname{Tr} SE^*E = \operatorname{Tr} S |A^*|^2 . \tag{10.41}$$

Since $A^*A \leq I_{\mathcal{H}}$, also $AA^* \leq I_{\mathcal{L}}$. Hence, $|A^*|^2 \leq |A^*|$ and therefore

$$\operatorname{Tr} S |A^*|^2 \leq \operatorname{Tr} S |A^*| = \operatorname{Tr} AVS.$$

Then

$$|\operatorname{Tr} AVS|^2 \le \sum_k |\operatorname{Tr} A_k VS|^2 = F_e(S, \mathcal{A}\circ \operatorname{Ad} V)$$

This chain of inequalities implies (10.40).
Now, let some sequences of subspaces $\mathcal{H}^{(n)}$, encodings $\mathcal{E}^{(n)}$, and decodings $\mathcal{D}^{(n)}$ be given, for which (10.37) holds. In this case, by Lemma 10.23, there exists a sequence of isometric encodings $\mathcal{V}^{(n)} = \operatorname{Ad} V^{(n)}$ such that

$$\lim_{n\to\infty} F_e\left(\bar{S}^{(n)}, \mathcal{D}^{(n)}\circ\Phi^{\otimes n}\circ\mathcal{V}^{(n)}\right) = 1 \tag{10.42}$$

It follows that in the definition of the quantum capacity we can restrict ourselves to the isometric encodings.

10.10.12 10.3.2 The Quantum Capacity and the Coherent Information

The following fundamental result is the coding theorem for the quantum capacity, which relates it to the coherent information.

Theorem 10.24 (Lloyd, Shor, Devetak). For any channel Φ, the quantum capacity is given by the expression

$$Q(\Phi) = \lim_{n\to\infty}\frac{1}{n}\max_S I_c\left(S, \Phi^{\otimes n}\right), \tag{10.43}$$

where $I_c(S,\Phi)$ is the coherent information.

Existence of the limit can be shown, just like in the case of the classical capacity, by using superadditivity of the sequence $\bar{Q}_n = \max_S I_c\left(S, \Phi^{\otimes n}\right)$. Let us check that (10.43) implies the inequality relating the quantum and the classical capacities of the channel

$$Q(\Phi) \le C(\Phi) \tag{10.44}$$

which is proved the same way as the second inequality in (9.8). Indeed, take S to be a mixture of arbitrary pure states S_j with probabilities p_j. Then (7.50) implies

$$I_c(S,\Phi) = H(\Phi[S]) - H(S,\Phi) \le H\left(\sum_j p_j \Phi\left[S_j\right]\right) - \sum_j p_j H\left(\Phi\left[S_j\right]\right) = \chi\left(\{p_j\}, \{\Phi\left[S_j\right]\}\right)$$

Taking the maximum gives $\max_S I_c(S,\Phi) \le C_\chi(\Phi)$. Applying this to $\Phi^{\otimes n}$ leads to (10.44).
Proof of the inequality $\le$. Denote by $\bar{Q}(\Phi)$ the right-hand side of (10.43). A simpler part of the theorem is the proof of the inequality

$$Q(\Phi) \le \bar{Q}(\Phi) \tag{10.45}$$

i. e., the weak converse of the coding theorem. Let $\mathcal{H}^{(n)}$ be the input space of dimensionality $d_n = \dim \mathcal{H}^{(n)} = 2^{nR}$ and let $\mathcal{E}^{(n)}, \mathcal{D}^{(n)}$ be an encoding and decoding such that

$$1 - F_e\left(\bar{S}^{(n)}, \mathcal{D}^{(n)}\circ\Phi^{\otimes n}\circ\mathcal{E}^{(n)}\right) \le \varepsilon$$

where $\bar{S}^{(n)} = \frac{1}{d_n} I_{\mathcal{H}^{(n)}}$ is the chaotic state in $\mathcal{H}^{(n)}$, with the entropy $H\left(\bar{S}^{(n)}\right) = \log d_n = nR$. Here, we are using the requirement (10.37) in the definition of the achievable rate. According to Lemma 10.23, we can assume that $\mathcal{E}^{(n)}$ are isometric encodings. Since

$$F_e\left(\bar{S}^{(n)}, \mathcal{D}^{(n)} \circ \Phi^{\otimes n} \circ \mathcal{E}^{(n)}\right)$$
$$= \left\langle \Omega^{(n)} \right| \left(\mathrm{Id}_{\mathcal{H}^{(n)}} \otimes \mathcal{D}^{(n)} \circ \Phi^{\otimes n} \circ \mathcal{E}^{(n)}\right) \left[\left|\Omega^{(n)}\right\rangle \left\langle \Omega^{(n)}\right|\right] \left|\Omega^{(n)}\right\rangle,$$

where $\left|\Omega^{(n)}\right\rangle$ is the maximally entangled vector, it follows by Lemma 10.9 that for the maximally entangled state $\left|\Omega^{(n)}\right\rangle \left\langle \Omega^{(n)}\right|$ in $\mathcal{H}^{(n)} \otimes \mathcal{H}^{(n)}$ the following holds:

$$\| \left|\Omega^{(n)}\right\rangle \left\langle \Omega^{(n)}\right| - \left(\mathrm{Id}_{\mathcal{H}^{(n)}} \otimes \mathcal{D}^{(n)} \circ \Phi^{\otimes n} \circ \mathcal{E}^{(n)}\right) \left[\left|\Omega^{(n)}\right\rangle \left\langle \Omega^{(n)}\right|\right] \|_1 \leq 2\sqrt{\varepsilon}. \tag{10.46}$$

This means that the rate R is achievable for asymptotically perfect transmission of the chaotic state in $\mathcal{H}^{(n)}$.

Denoting $S^{(n)} = \mathcal{E}^{(n)}\left[\bar{S}^{(n)}\right]$ and using the chain rule (10.6) for the coherent information, we have

$$I_c\left(S^{(n)}, \Phi^{\otimes n}\right) \geq I_c\left(S^{(n)}, \mathcal{D}^{(n)} \circ \Phi^{\otimes n}\right) = H\left(S_{B'}\right) - H\left(S_{B'R'}\right) \tag{10.47}$$

where $S_{B'R'} = \left(\mathrm{Id}_{\mathcal{H}^{(n)}} \otimes \left(\mathcal{D}^{(n)} \circ \Phi^{\otimes n} \circ \mathcal{E}^{(n)}\right)\right) \left[\left|\Omega^{(n)}\right\rangle \left\langle \Omega^{(n)}\right|\right]$, so that

$$S_{B'} = \left(\mathcal{D}^{(n)} \circ \Phi^{\otimes n} \circ \mathcal{E}^{(n)}\right) \left[\bar{S}^{(n)}\right].$$

The equality $H\left(S_{B'R'}\right) = H\left(S^{(n)}, \mathcal{D}^{(n)} \circ \Phi^{\otimes n}\right)$ follows from the fact that, due to the isometric nature of the encoding $\mathcal{E}^{(n)}$, the state $\left(\mathrm{Id}_{\mathcal{H}^{(n)}} \otimes \mathcal{E}^{(n)}\right) \left[\left|\Omega^{(n)}\right\rangle \left\langle \Omega^{(n)}\right|\right]$ is pure and can be regarded as a purification of $S^{(n)}$. According to (10.46)

$$\left\|\bar{S}^{(n)} - S_{B'}\right\|_1 \leq \| \left|\Omega^{(n)}\right\rangle \left\langle \Omega^{(n)}\right| - S_{B'R'} \|_1 \leq 2\sqrt{\varepsilon}.$$

Here the first inequality follows from a simple observation, to be proved in the following exercise.

Exercise 10.25 Prove the following statement: the trace norm does not increase under partial trace, i.e.,

$$\|\mathrm{Tr}_{\mathcal{H}_0} T\|_1 \leq \|T\|_1,$$

for any positive operator $T \in \mathcal{H} \otimes \mathcal{H}_0$. Hint: use expression (1.19) for the trace norm.

By using twice the estimate (7.26) for the continuity of the entropy, we have

$$\begin{aligned} H\left(S_{B'}\right) - H\left(S_{B'R'}\right) =& H\left(\bar{S}^{(n)}\right) + \left[H\left(S_{B'}\right) - H\left(\bar{S}^{(n)}\right)\right] \\ &+ \left[H\left(\left|\Omega^{(n)}\right\rangle \left\langle \Omega^{(n)}\right|\right) - H\left(S_{B'R'}\right)\right] \\ \geq& H\left(\bar{S}^{(n)}\right) - 6 \log \dim \mathcal{H}^{(n)} \sqrt{\varepsilon} - \frac{2 \log e}{e} \\ =& nR(1 - 6\sqrt{\varepsilon}) - \frac{2 \log e}{e}. \end{aligned}$$

Therefore, taking into account (10.47),

$$\bar{Q}_n = \max_{S^{(n)}} I_c\left(S^{(n)}, \Phi^{\otimes n}\right) \geq nR(1 - 6\sqrt{\varepsilon}) - \frac{2 \log e}{e},$$

whence $R \leq \lim_{n\to\infty} \frac{1}{n} \bar{Q}_n = \bar{Q}(\Phi)$.

This completes the proof of inequality (10.45), i.e., the weak converse for the quantum capacity. The proof of the direct coding theorem is postponed to Section 10.4.4. □

10.10.13 10.3.3 Degradable Channels

First of all, we obtain important relations between the coherent information and the quantity

$$\chi\left(\{\pi_x\},\{S_x\}\right)=H\left(\sum_x \pi_x S_x\right)-\sum_x \pi_x H\left(S_x\right),$$

giving the upper bound (5.16) for the amount of classical information and, as a consequence, a relation between the quantum and the classical capacities of a channel and its complementary.

Consider a channel $\Phi:\mathfrak{T}\left(\mathcal{H}_A\right)\to\mathfrak{T}\left(\mathcal{H}_B\right)$, its Stinespring dilation with the isometry $V:\mathcal{H}_A\to\mathcal{H}_B\otimes\mathcal{H}_E$, and the complementary channel (see Section 6.6)

$$\tilde{\Phi}[S]=\mathrm{Tr}_{\mathcal{H}_B} VSV^*,\quad S\in\mathfrak{T}\left(\mathcal{H}_A\right). \tag{10.48}$$

Let $S=\sum_x \pi_x S_x$ be an arbitrary decomposition of the state S into pure states. Then the following equalities hold:

$$\begin{aligned}
I_c(S,\Phi)&=H(\Phi[S])-H(\tilde{\Phi}[S])\\
&=\left[H(\Phi[S])-\sum_x \pi_x H\left(\Phi\left[S_x\right]\right)\right] &(10.49)\\
&-\left[H(\tilde{\Phi}[S])-\sum_x \pi_x H\left(\tilde{\Phi}\left[S_x\right]\right)\right]\\
&=\chi\left(\{\pi_x\},\{\Phi\left[S_x\right]\}\right)-\chi\left(\{\pi_x\},\left\{\tilde{\Phi}\left[S_x\right]\right\}\right) &(10.50)\\
&=\sum_x \pi_x\left[H\left(\Phi\left[S_x\right];\Phi[S]\right)-H\left(\tilde{\Phi}\left[S_x\right];\tilde{\Phi}[S]\right)\right] &(10.51)
\end{aligned}$$

Here, equality (10.49) follows from the fact that the state VS_xV^* is pure and hence

$$H\left(\Phi\left[S_x\right]\right)=H\left(\tilde{\Phi}\left[S_x\right]\right)$$

for all x, and (10.51) follows from identity (7.19). Taking the upper and the lower bounds in (10.50), with respect to all possible ensembles of pure states, we obtain

$$-Q_1(\tilde{\Phi})\le C_\chi(\Phi)-C_\chi(\tilde{\Phi})\le Q_1(\Phi), \tag{10.52}$$

where we introduced the notation

$$Q_1(\Phi)=\max_S I_c(S,\Phi). \tag{10.53}$$

Applying (10.52) to channel $\Phi^{\otimes n}$, taking the limit $n\to\infty$, and using the coding theorems, we obtain

$$-Q(\tilde{\Phi})\le C(\Phi)-C(\tilde{\Phi})\le Q(\Phi).$$

Now, we introduce an important class of channels for which the quantum capacity is given by the "one-letter" expression (10.53).

Definition 10.26. The channel Φ is called degradable if there exists a channel Γ such that $\tilde{\Phi}=\Gamma\circ\Phi$ (Fig. 10.1) and antidegradable if there exists a channel Γ' such that $\Phi=\Gamma'\circ\tilde{\Phi}$.

Obviously, Φ is degradable if and only if $\tilde{\Phi}$ is antidegradable. From relation (10.51), by using the monotonicity of the relative entropy, we deduce that if Φ is an antidegradable channel, then

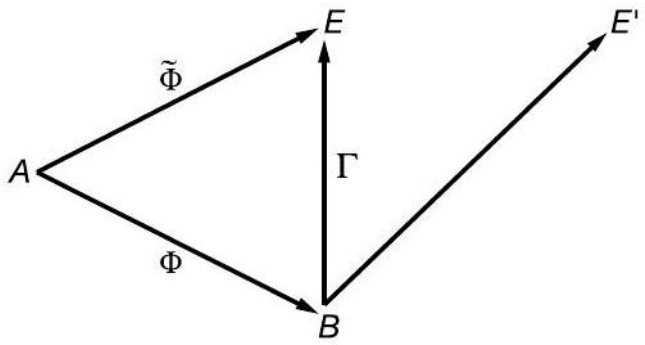


Figure 10.1: Degradable channel.

$$I_c(S,\Phi) \le 0 \quad \text{for all states } S \tag{10.54}$$

(correspondingly, $I_c(S,\Phi) \ge 0$ for a degradable channel).

Proposition 10.27. If Φ is an antidegradable channel, then $Q(\Phi) = 0$. If Φ is degradable, then

$$Q(\Phi) = Q_1(\Phi) = \max_S I_c(S,\Phi). \tag{10.55}$$

Proof. The first statement follows from (10.54) and the weak converse (10.45).

Let Φ be a degradable channel and $W : \mathcal{H}_B \to \mathcal{H}_E \otimes \mathcal{H}_{E'}$ be the Stinespring isometry for the channel $\Gamma : \mathfrak{T}(\mathcal{H}_B) \to \mathfrak{T}(\mathcal{H}_E)$. Then $I_c(S,\Phi) = H(B) - H(E) = H(EE') - H(E)$, so that

$$I_c(S,\Phi) = H(E' \mid E).$$

For two degradable channels Φ_1, Φ_2 and for an arbitrary state S_{12} in $\mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2}$, we have

$$I_c(S_{12}, \Phi_1 \otimes \Phi_2) = H(E_1' E_2' \mid E_1 E_2).$$

Hence, by subadditivity (7.43) of the conditional entropy

$$I_c(S_{12}, \Phi_1 \otimes \Phi_2) \le I_c(S_1, \Phi_1) + I_c(S_2, \Phi_2)$$

implying

$$I_c\left(S^{(n)}, \Phi^{\otimes n}\right) \le n \max_S I_c(S,\Phi) \tag{10.56}$$

and hence, by the weak converse, (10.55). □

Consider an entanglement-breaking channel

$$\Phi[S] = \sum_{k=1}^{\tilde{d}} |\varphi_k\rangle \langle\psi_k| S |\psi_k\rangle \langle\varphi_k|,$$

where $\{\psi_k\}$ is an overcomplete system in $\mathcal{H}$ and $\{\varphi_k\}$ is a system of unit vectors in the output space $\mathcal{H}'$. The complementary channel is

$$\tilde{\Phi}[S] = \sum_{k,l=1}^{\tilde{d}} c_{kl} |e_k\rangle \langle\psi_k| S |\psi_l\rangle \langle e_l|,$$

where $c_{kl} = \langle\varphi_l \mid \varphi_k\rangle$, while $\{e_k\}$ is the standard basis in $\tilde{\mathbb{C}}^{\tilde{d}}$. We have $\Phi = \Gamma' \circ \tilde{\Phi}$, where

$$\Gamma'[S] = \sum_{k=1}^{\tilde{d}} |\varphi_k\rangle \langle e_k| S |e_k\rangle \langle \varphi_k| .$$

This proves the following.

Corollary 10.28. Any entanglement-breaking channel Φ is antidegradable.

The first statement of Proposition 10.27 again implies $Q(\Phi) = 0$, thus reconfirming Corollary 10.22.

Example 10.29. Consider the quantum erasure channels Φ_p. For $q \geq p$,

$$\Phi_q = \Gamma_{(1-q)/(1-p)} \circ \Phi_p,$$

where $\Gamma_\alpha : \mathfrak{T}(\mathcal{H} \oplus \mathbb{C}) \to \mathfrak{T}(\mathcal{H} \oplus \mathbb{C})$ is the channel acting as

$$\Gamma_\alpha \left[\begin{bmatrix} S & 0 \\ 0 & S \end{bmatrix} \right] = \alpha \begin{bmatrix} S & 0 \\ 0 & S \end{bmatrix} + (1-\alpha) \begin{bmatrix} 0 & 0 \\ 0 & \operatorname{Tr} S + s \end{bmatrix}.$$

Combining this with the fact that $\tilde{\Phi}_p = \Phi_{1-p}$ (see Exercise 6.35), we find that Φ_p is degradable for $p \in [0, 1/2]$ and antidegradable for $p \in [1/2, 1]$. Therefore, by Theorem 10.27, we obtain

$$Q(\Phi_p) = \begin{cases} (1-2p) \log d, & p \in [0, 1/2], \\ 0, & p \in [1/2, 1]. \end{cases} \tag{10.57}$$

Here, the first line follows from (10.55) together with the fact that $H(\Phi_p[S]) = (1-p)H(S) + h_2(p)$. Hence, $I_c(S, \Phi_p) = H(\Phi_p[S]) - H\left(\tilde{\Phi}_p[S]\right) = (1-p)H(S) - pH(S) = (1-2p)H(S)$. Maximizing over S gives (10.57).

10.10.14 10.4 The Private Classical Capacity and the Quantum Capacity

10.10.15 10.4.1 The Quantum Wiretap Channel

Consider the situation where the quantum communication channel is accessed by three parties, i. e., a sender A, a receiver B, and an eavesdropper E. The mathematical model of the quantum wiretap channel consists of three Hilbert spaces $\mathcal{H}_A, \mathcal{H}_B, \mathcal{H}_E$
and an isometric map $V : \mathcal{H}_A \to \mathcal{H}_B \otimes \mathcal{H}_E$, so that the input state S_A is mapped to the state $S_{BE} = \Phi_{BE}[S_A] \equiv V S_A V^*$ of the system BE, with the partial states

$$S_B = \Phi_B[S_A] = \operatorname{Tr}_E V S_A V^*, \quad S_E = \Phi_E[S_A] = \operatorname{Tr}_B V S_A V^*$$

Recall that the notation E was used previously for the environment. This is a consistent change, if we regard the whole environment as accessible to the eavesdropper.

Assume that the party A chooses an ensemble of states $\left\{S_A^X\right\}$ with probabilities $\{\pi_\chi\}$, so that B and E receive states $\{S_B^\chi\}$ and $\{S_E^\chi\}$, respectively. In this case, the upper bounds for the Shannon informations of B and E are, correspondingly, $\chi\left(\{\pi_x\}, \left\{S_B^X\right\}\right)$ and $\chi(\{\pi_x\}, \{S_E^x\})$. By analogy with the classical wiretap channel (see Section 4.5), the "quantum privacy" can be characterized by the quantity $\chi(\{\pi_x\}, \{S_B^x\}) - \chi(\{\pi_x\}, \{S_E^x\})$. Assuming that the input states S_A^X are pure and denoting by $\bar{S}_A = \sum_x \pi_x S_A^X$ the average of the input ensemble, we obtain, from (10.50), a key relation (Schumacher and Westmoreland [201]),

$$I_c\left(\bar{S}_A, \Phi_B\right) = \chi(\{\pi_\chi\}, \{S_B^x\}) - \chi(\{\pi_\chi\}, \{S_E^x\}) \tag{10.58}$$

This points to the profound connection between the quantum capacity and the private classical capacity, which provides a hint to a proof of the direct coding theorem.

To define the private classical capacity, let us consider block coding for the quantum wiretap channel. The goal is to transmit the maximum amount of classical information from A to B in a private way, so that E can receive only an asymptotically negligible amount of information. A code $\left(\Sigma^{(n)}, M^{(n)}\right)$ of length n and of size N is defined as in Definition 8.1, i. e., as a collection of states $\Sigma^{(n)} = \left\{S^i_{A^{(n)}}; i = 1, \ldots, N\right\}$ in $\mathcal{H}_A^{\otimes n}$, together with an observable $M^{(n)} = \{M_j; j = 0, 1, \ldots, N\}$ in $\mathcal{H}_B^{\otimes n}$. Along with its error probability $P_e\left(\Sigma^{(n)}, M^{(n)}\right)$, defined by (8.1), we consider the new quantity

$$v_E\left(\Sigma^{(n)}\right) = \max_{i,k=1,\ldots,N} \left\|S^i_{E^{(n)}} - S^k_{E^{(n)}}\right\|_1$$

which characterizes the variability, and hence the information content of the output states for the eavesdropper E. Note that, by the triangle inequality for the norm, we have

$$\left\|\bar{S}_{E^{(n)}} - S^i_{E^{(n)}}\right\|_1 \leq v_E\left(\Sigma^{(n)}\right) \qquad \text{for all } i$$

where $\bar{S}_{E^{(n)}} = \frac{1}{N}\sum_{i=1}^N S^i_{E^{(n)}}$. Applying inequality (7.25), we obtain

$$\begin{aligned} \frac{1}{n}\chi\left(\left\{\frac{1}{N}\right\}, \left\{S^i_{E^{(n)}}\right\}\right) &= \frac{1}{nN}\sum_{i=1}^N \left[H\left(\bar{S}_{E^{(n)}}\right) - H\left(S^i_{E^{(n)}}\right)\right] \\ &\leq \log\dim\mathcal{H}_E \cdot v_E\left(\Sigma^{(n)}\right) + \frac{1}{n}\eta\left(v_E\left(\Sigma^{(n)}\right)\right) \end{aligned} \tag{10.59}$$

provided that $v_E\left(\Sigma^{(n)}\right)$ is small enough. Therefore, if the variability is small, the Shannon mutual information between A and E, with equiprobable encoding, is also small.

We call R the achievable rate for the wiretap channel if there exists a sequence of codes $\left(\Sigma^{(n)}, M^{(n)}\right)$ of sizes $N = 2^{nR}$, such that

$$\lim_{n\to\infty} P_e\left(\Sigma^{(n)}, M^{(n)}\right) = 0$$

and

$$\lim_{n\to\infty} v_E\left(\Sigma^{(n)}\right) = 0. \tag{10.60}$$

The least upper bound of the achievable rates is called the private classical capacity $C_p\left(\Phi_{BE}\right)$ of the wiretap channel. By (10.59), condition (10.60) implies asymptotic vanishing of the mutual information between A and E. It is possible to show that these conditions are, in fact, equivalent, but condition (10.60) is more convenient technically and is also more useful for later application to the quantum capacity.

Theorem 10.30 (Devetak [62] and Cai, Winter, and Yeung [38]). We have

$$C_p\left(\Phi_{BE}\right) = \lim_{n\to\infty}\frac{1}{n}\max_{\pi^{(n)},\Sigma^{(n)}}\left[\chi\left(\left\{\pi^{(n)}_i\right\}, \left\{S^i_{B^{(n)}}\right\}\right) - \chi\left(\left\{\pi^{(n)}_i\right\}, \left\{S^i_{E^{(n)}}\right\}\right)\right], \tag{10.61}$$

where the maximization is over all ensembles, i. e., finite collections of states $\Sigma^{(n)} = \left\{S^i_{A^{(n)}}\right\}$ in $\mathcal{H}_A^{\otimes n}$ with probability distributions $\pi^{(n)} = \left\{\pi^{(n)}_i\right\}$ (we use the notations $S^i_{B^{(n)}} = \Phi_B^{\otimes n}\left[S^i_{A^{(n)}}\right]$, $S^i_{E^{(n)}} = \Phi_E^{\otimes n}\left[S^i_{A^{(n)}}\right]$).

Formulas (10.43), (10.58), and (10.61) imply an important relation between the quantum and the private classical capacities

$$Q\left(\Phi_B\right) \leq C_p\left(\Phi_{BE}\right) \tag{10.62}$$

following from the fact that $C_p\left(\Phi_{BE}\right)$ involves arbitrary state ensembles for A, while $Q\left(\Phi_B\right)$ involves only pure ones. In general, the inequality can be strict. Therefore, the following statement is of special interest.

Proposition 10.31. If the channel Φ_B is degradable,

$$C_p\left(\Phi_{BE}\right) = Q\left(\Phi_B\right) = Q_1\left(\Phi_B\right). \tag{10.63}$$

Proof. By using equality (10.50), we have

$$\begin{aligned}
&\chi\left(\left\{\pi_i^{(n)}\right\}, \left\{S_{B^{(n)}}^i\right\}\right) - \chi\left(\left\{\pi_i^{(n)}\right\}, \left\{S_{E^{(n)}}^i\right\}\right) \\
&= H\left(\sum_i \pi_i^{(n)} S_{B^{(n)}}^i\right) - H\left(\sum_i \pi_i^{(n)} S_{E^{(n)}}^i\right) \\
&\quad - \sum_i \pi_i^{(n)}\left[H\left(S_{B^{(n)}}^i\right) - H\left(S_{E^{(n)}}^i\right)\right] \\
&= I_c\left(\sum_i \pi_i^{(n)} S_{A^{(n)}}^i, \Phi_B^{\otimes n}\right) - \sum_i \pi_i^{(n)} I_c\left(S_{A^{(n)}}^i, \Phi_B^{\otimes n}\right) \\
&\leq I_c\left(\sum_i \pi_i^{(n)} S_{A^{(n)}}^i, \Phi_B^{\otimes n}\right)
\end{aligned}$$

since channel $\Phi_B^{\otimes n}$, along with Φ_B, is degradable and hence, $I_c\left(S_{A^{(n)}}^i, \Phi_B^{\otimes n}\right) \geq 0$. Therefore, by using (10.62)

$$\max_{\pi^{(n)}, \Sigma^{(n)}}\left[\chi\left(\left\{\pi_i^{(n)}\right\}, \left\{S_B^i\right\}\right) - \chi\left(\left\{\pi_i^{(n)}\right\}, \left\{S_{E^{(n)}}^i\right\}\right)\right] = \max_{S^{(n)}} I_c\left(S^{(n)}, \Phi_B^{\otimes n}\right)$$

which is equal to $nQ_1\left(\Phi_B\right)$ due to (10.56). Substituting this into (10.61) we obtain (10.63). □

10.10.16 10.4.2 Proof of the Private Capacity Theorem

We first prove inequality $\leq$ i. e., the weak converse. Let R be an achievable rate. In this case, by (5.32) and the information bound (5.16),

$$\begin{aligned}
\bar{P}_e\left(\Sigma^{(n)}, M^{(n)}\right) &\geq 1 - \frac{\chi\left(\left\{1/N\right\}, \left\{S_{B^{(n)}}^i\right\}\right)}{nR} - \frac{1}{nR} \\
&= 1 - \frac{\chi\left(\left\{1/N\right\}, \left\{S_{B^{(n)}}^i\right\}\right) - \chi\left(\left\{1/N\right\}, \left\{S_{E^{(n)}}^i\right\}\right)}{nR} \\
&\quad - \frac{1 + \chi\left(\left\{1/N\right\}, \left\{S_{E^{(n)}}^i\right\}\right)}{nR}.
\end{aligned} \tag{10.64}$$

According to (10.59),

$$\chi\left(\left\{1/N\right\}, \left\{S_{E^{(n)}}^i\right\}\right) \leq v_E\left(\Sigma^{(n)}\right)\left[n \log d_E - \log v_E\left(\Sigma^{(n)}\right)\right]$$

where $d_E = \dim \mathcal{H}_E$. Therefore, the last term in the right-hand side of (10.64) tends to zero as $n \to \infty$, along with the left-hand side. From this follows $0 \geq 1 - \bar{C}_p/R$, where $\bar{C}_p$ is the right-hand side of (10.61), and hence $C_p\left(\Phi_{BE}\right) \leq \bar{C}_p$.

To prove the direct statement it is sufficient to show that for an arbitrary ensemble $\{\pi_\chi, S_A^\chi\}$ and $\delta > 0$ the rate $\chi\left(\{\pi_\chi\}, \{S_B^\chi\}\right) - \chi\left(\{\pi_\chi\}, \{S_E^\chi\}\right) - \delta$ is achievable. Achievability of the rate $\bar{C}_p - \delta$ then follows by additional blocking. Consider the c-q channel $x \to S_B^x$ and the random codebook $W^{(n)}$ of size $N = 2^{n\left[\chi\left(\{\pi_\chi\},\left\{S_B^X\right\}\right)-c\delta\right]}$, with independent words having the probability distribution

$$\mathrm{P}\left\{w = (x_1, \ldots, x_n)\right\} = \pi_{x_1} \cdots \pi_{x_n}. \tag{10.65}$$

The constant c in the definition of N will be fixed later. To simplify the notation, we will denote all constants that appear below by the same letter c. In fact, we can always take the maximum of them. By the remark that follows the proof of the direct quantum coding theorem at the end of Section 5.6, for sufficiently large n, there exist decision rules $M^{(n)}$ for the system B such that

$$E\bar{P}_e\left(W^{(n)}, M^{(n)}\right) \le 2^{-n\beta}, \quad \beta > 0.$$

Now, consider the new random code with independent words having the uniform distribution on the set $\hat{T}^{n,\delta}$ of δ-strongly typical words,

$$\tilde{\mathrm{P}}(w) = \begin{cases} \frac{1}{\left|\hat{T}^{n,\delta}\right|}, & w \in \hat{T}^{n,\delta} \\ 0, & w \notin \hat{T}^{n,\delta} \end{cases}$$

By Exercise 9.10, $\left|\hat{T}^{n,\delta}\right| \ge 2^{n[H(\pi)-\Delta_n(\delta)]}$, where $\lim_{\delta\to 0}\lim_{n\to\infty}\Delta_n(\delta) = 0$. Since $\mathrm{P}(w) \ge 2^{-n[H(\pi)+c\delta]}$ for $w \in \hat{T}^{n,\delta}$, where c is a constant (depending on $\{\pi_x\}$), we have $\tilde{\mathrm{P}}(w) \le 2^{n[c\delta+\Delta_n(\delta)]}\mathrm{P}(w)$ for all w, and hence

$$\tilde{\mathrm{E}}\bar{P}_e\left(W^{(n)}, M^{(n)}\right) \le 4^{n[c\delta+\Delta_n(\delta)]}2^{-n\beta} \le \varepsilon$$

for n large enough, because the estimate (5.51) for $\bar{P}_e\left(W^{(n)}, M^{(n)}\right)$ involves at most two independent words. Hence, by the Markov inequality,

$$\tilde{\mathrm{P}}\left\{\bar{P}_e\left(W^{(n)}, M^{(n)}\right) \ge \sqrt{\varepsilon}\right\} \le \sqrt{\varepsilon}. \tag{10.66}$$

So far, this was just a slight modification of the random code for the classical information transmission from A to B. To make it secure against eavesdropping, A has to sacrifice $n\left[\chi\left(\{\pi_\chi\}, \left\{S_E^X\right\}\right) + c\delta/2\right]$ bits of information, by additional randomization of the input. Assuming $\chi\left(\{\pi_\chi\}, \left\{S_B^X\right\}\right) - \chi\left(\{\pi_\chi\}, \left\{S_E^X\right\}\right) > 0$, set

$$N_E = 2^{n\left[\chi\left(\{\pi_x\},\left\{S_E^x\right\}\right)+c\delta/2\right]}, \quad N_B = 2^{n\left[\chi\left(\{\pi_x\},\left\{S_B^x\right\}\right)-\chi\left(\{\pi_x\},\left\{S_E^x\right\}\right)-3c\delta/2\right]},$$

so that $N_E N_B = N$, and arrange the codebook $W^{(n)}$ in a rectangular array with N_B rows and N_E columns. Then

$$W^{(n)} = \left\{w^{mj}; m = 1, \ldots, N_B; j = 1, \ldots, N_E\right\},$$
$$M^{(n)} = \left\{M_{mj}; m = 1, \ldots, N_B; j = 1, \ldots, N_E\right\}.$$

(For brevity of notation we omit the zero component of $M^{(n)}$ which corresponds to "no decision.")

For each m, A will take the value j at random, with equal probabilities, which results in the input states

$$m \to S_{A^{(n)}}^m = \frac{1}{N_E}\sum_{j=1}^{N_E} S_{A^{(n)}}^{w^{mj}}$$

with the corresponding outputs $S^m_{B^{(n)}}$ for B and $S^m_{E^{(n)}}$ for E. (Let us recall here that $S^W_{A^{(n)}} = S^{x_1}_A \otimes \cdots \otimes S^{x_n}_A$ for a word $w = (x_1, \ldots, x_n)$.) Such a randomization will make the transmitted information almost secret to E, because from the viewpoint of the eavesdropper, for every m the codebook

$$\left\{w^{mj}; j = 1, \ldots, N_E\right\}$$

with a high probability is a "good" codebook, that carries almost the maximum possible information from A to E, provided an optimal strategy is applied by E. Therefore, the mutual information between the codebooks with different m must be close to zero. Hence, randomizing inside each of these codebooks discards almost all information carried from A to E.

The crucial step in the rigorous justification of this scenario is the application of the following estimate, based on a quantum version of the Bernstein inequality to be established in the next section.

Proposition 10.32. Let $S^{w^{mj}}_{E^{(n)}}, m = 1, \ldots, N_B, j = 1, \ldots, N_E$, be the random i.i.d. density operators, with N_B, N_E chosen as above. There exists a $\beta_1 > 0$ such that, for n large enough,

$$\tilde{\mathrm{P}}\left\{\left\|\frac{1}{N_E}\sum_{j=1}^{N_E} S^{w^{mj}}_{E^{(n)}} - \theta\right\|_1 \geq \varepsilon\right\} \leq 2^{-2^{n\beta_1}}, \tag{10.67}$$

for each $m = 1, \ldots, N_B$, where θ is a nonrandom operator (in fact, one can take $\theta = \tilde{\mathrm{E}} S^{w^{mj}}_{E^{(n)}}$, but we do not need this).

This estimate implies that the probability

$$\begin{aligned}\tilde{\mathrm{P}}\left\{\left\|S^m_{E^{(n)}} - \theta\right\|_1 < \varepsilon; m = 1, \ldots, N_B\right\} &\geq 1 - N_B 2^{-2^{n\beta_1}} \\ &= 1 - 2^{n\left[X\left(\{\pi_x\},\left\{S^x_B\right\}\right) - \chi\left(\{\pi_x\},\left\{S^x_E\right\}\right) - 3c\delta/2\right] - 2^{n\beta_1}}\end{aligned}$$

can be made arbitrarily close to 1 for n large enough. Together with (10.66) this implies that there exists a realization of the codebook $W^{(n)} = \{W^{mj}\}$, for which

$$\bar{P}_e\left(W^{(n)}, M^{(n)}\right) < \sqrt{\varepsilon},$$

and

$$\left\|S^m_{E^{(n)}} - S^l_{E^{(n)}}\right\|_1 < 2\varepsilon, \quad m, l = 1, \ldots, N_B. \tag{10.68}$$

Defining $\Sigma^{(n)} = \left\{S^m_{A^{(n)}}; m = 1, \ldots, N_B\right\}, \tilde{M}^{(n)} = \left\{\tilde{M}_m; m = 0, 1, \ldots, N_B\right\}$, where $\tilde{M}_m = \sum_{j=1}^{N_E} M_{mj}$, we have $\bar{P}_e\left(\Sigma^{(n)}, \tilde{M}^{(n)}\right) \leq \bar{P}_e\left(W^{(n)}, M^{(n)}\right) < \sqrt{\varepsilon}$. An argument similar to Lemma 4.11 shows that we can choose a subcode for which the maximal error $P_e\left(W^{(n)},\ M^{(n)}\right) < 2\sqrt{\varepsilon}$ while $v_E\left(\Sigma^{(n)}\right) < \varepsilon'$, where $\varepsilon' \to 0$ if $\varepsilon \to 0$, which proves the theorem. □

Proof of Proposition 10.32. As in Section 5.6, we introduce the density operator

$$\bar{S}_\pi = \sum_x \pi_x S^X_E,$$

and we write for brevity

$$H\left(\bar{S}_\pi\right) = H(E), \quad \sum_x \pi_x H\left(S^x_E\right) = H(E \mid A),$$

with $\chi\left(\{\pi_\chi\},\{S_E^\chi\}\right) = H(E) - H(E \mid A)$.
Denote by λ_j the eigenvalues of $\bar{S}_\pi$. Let us fix a small positive δ, and let $P = P^{n,\delta}$ be the strongly typical projector of the density operator $\bar{S}_\pi^{\otimes n}$, corresponding to the eigenvalues $\lambda_J = \lambda_{j_1}\cdots\lambda_{j_n}$ for which the sequence $J = (j_1,\ldots,j_n)$ is strongly typical, i.e., the numbers $N(j \mid J)$ of times the symbol j appears in J satisfy the condition

$$\left|\frac{N(j \mid J)}{n} - \lambda_j\right| < \delta, \quad j = 1,\ldots,d_E,$$

and $N(j \mid J) = 0$ if $\lambda_j = 0$ (see Definition 9.9). Denote by $\lambda_j(x)$ the eigenvalues of the density operator S_E^X. For a codeword $w = (x_1,\ldots,x_n)$ of length n, let $S_w = S_E^{x_1} \otimes \cdots \otimes S_E^{x_n}$ and denote by P_w the typical projector of S_w, corresponding to the eigenvalues $\lambda_J(w) = \lambda_{j_1}(x_1)\cdots\lambda_{j_n}(x_n)$, for which

$$\left|\frac{N(j,x \mid J,w)}{n} - \frac{N(x \mid w)}{n}\lambda_j(x)\right| < \delta, \quad j = 1,\ldots,d_E,$$

and $N(j,x \mid J,w) = 0$ if $\lambda_j(x) = 0$. We shall need the following properties, which are just a reformulation of the corresponding properties for strongly typical sequences in the classical information theory (see [50]):
i. For $w \in \hat{T}^{n,\delta}$, the eigenvalues of the operator $P_w S_w P_w$ lie in the interval $\left(2^{-n[H(E|A)+c\delta]}, 2^{-n[H(E|A)-c\delta]}\right)$, where c is another constant, depending on $\{\lambda_j(x)\}$ (to simplify the notation we use the same c as before; in fact, we can choose the maximum of the two constants). In particular, $P_w S_w P_w \le 2^{-n[H(E|A)-c\delta]} P_w$.
ii. For $\varepsilon_1 > 0$ and sufficiently large n, $\operatorname{Tr} P_w S_w \ge 1 - \varepsilon_1$ (this is a corollary of the law of large numbers for the probability distribution given by the eigenvalues of S_w).

The following property is less straightforward.
iii. For given $\varepsilon_1, \delta > 0$, there is a $\delta_1 > 0$ such that for $w \in \hat{T}^{n,\delta_1}$ and sufficiently large n, $\operatorname{Tr} P S_w \ge 1 - \varepsilon_1$, where $P = P^{n,\delta}$ is the strongly typical projector of $\bar{S}_\pi^{\otimes n}$.

Proof. Denote by $p^{(k)}(j) = \langle e_j| S_E^{x_k} |e_j\rangle$, where $|e_j\rangle$ are the eigenvectors of $\bar{S}_\pi$, and note that $p^{(k)}(j) = 0$ if $\lambda_j = 0$, because $\operatorname{supp} S_E^{x_k} \subset \operatorname{supp} \bar{S}_\pi$. Then

$$\begin{aligned}\operatorname{Tr} P^{n,\delta} S_w &= \sum_{J \in B^{n,\delta}} p^{(1)}(j_1)\cdots p^{(n)}(j_n) \\ &= \mathrm{P}\left\{\left|\frac{N(j \mid J)}{n} - \lambda_j\right| < \delta, \text{ if } \lambda_j > 0\right\}, \end{aligned} \tag{10.69}$$

where P is the probability distribution, ascribing the probability $p^{(1)}(j_1)\cdots p^{(n)}(j_n)$ to the sequence $J = (j_1,\ldots,j_n)$, and $B^{n,\delta}$ is the set of strongly typical sequences. The fact that $w \in \hat{T}^{n,\delta_1}$ is expressed by similar inequalities

$$\left|\frac{N(x \mid w)}{n} - \pi_x\right| < \delta_1, \quad \text{if } \pi_x > 0,$$

and $N(x \mid w) = 0$ if $\pi_x = 0$, which implies for $\bar{\lambda}_j = \frac{1}{n}\sum_{k=1}^n p^{(k)}(j)$,

$$\begin{aligned}\left|\bar{\lambda}_j - \lambda_j\right| &= \left|\langle e_j| \left[\frac{1}{n}\sum_{k=1}^n S_E^{x_k} - \bar{S}_\pi\right] \middle| e_j\right\rangle| \\ &= \left|\sum_x \left[\frac{N(x \mid w)}{n} - \pi_x\right] \langle e_j| S_E^x \middle| e_j\right\rangle| < \delta_1 K, \end{aligned}$$

where K is the number of symbols x. Therefore, by choosing $\delta_1 = \delta/2K$, we have

$$\begin{aligned}
&\mathrm{P}\left\{\left|\frac{N(j\mid J)}{n}-\lambda_j\right|<\delta;\ \text{for all } j:\lambda_j>0\right\}\\
&\quad\geq \mathrm{P}\left\{\left|\frac{N(j\mid J)}{n}-\bar{\lambda}_j\right|<\delta/2;\ \text{for all } j:\lambda_j>0\right\}\\
&\quad\geq 1-\sum_{j:\lambda_j>0}\mathrm{P}\left\{\left|\frac{N(j\mid J)}{n}-\bar{\lambda}_j\right|\geq\delta/2\right\}
\end{aligned}$$

But under the probability distribution P , the random variable $N(j \mid J)$ has mean value $\sum_{k=1}^{n} p^{(k)}(j) = n\bar{\lambda}_j$ and variance $\sum_{k=1}^{n} p^{(k)}(j)\left(1-p^{(k)}(j)\right) \leq n/4$. Applying the Chebyshev inequality and taking into account (10.69), we obtain iii. □

We proceed with the proof of Proposition 10.32, for which we also need the following lemma.

Lemma 10.33. For a positive operator X and a projector P

$$\|X-PXP\|_1 \leq 3\sqrt{\operatorname{Tr} X \operatorname{Tr}(I-P)X}$$

Proof. By the triangle inequality and the properties of the trace norm

$$\|X-PXP\|_1 \leq \|(I-P)X(I-P)\|_1 + 2\|PX(I-P)\|_1 \leq 3\|X(I-P)\|_1.$$

There is a unitary U such that $\|X(I-P)\|_1 = \operatorname{Tr} X(I-P)U$. By the Cauchy-Schwarz inequality for the trace (take $S = I/d$ in (2.24))

$$[\operatorname{Tr}\sqrt{X}\sqrt{X}(I-P)U]^2 \leq \operatorname{Tr} X \operatorname{Tr} U^*(I-P)X(I-P)U = \operatorname{Tr} X \operatorname{Tr}(I-P)X.$$

Hence, the result follows. □

To simplify notation in (10.67), we shall denote $S_{E^{(n)}}^{W^{mj}} = S_{w^j}$, where the codewords $w^j, j = 1,\ldots,N_E$, are i. i. d. uniformly on the set T^{n,δ_1}. We shall obtain (10.67) by applying the operator Bernstein inequality (10.76), to be established in the next section, to the random operators

$$X_j = 2^{n[H(E|A)-\delta]}\Pi P P_{w^i} S_{w^i} P_{w^i} P \Pi,$$

where Π is the projector onto the eigenspace of the operator

$$\theta' = \tilde{\mathrm{E}} P P_{w^j} S_{w^j} P_{w^j} P$$

corresponding to eigenvalues $\geq 2^{-n[H(E)+3c\delta/2]}$. By construction, $0 \leq X_j \leq I$,

$$M = \tilde{\mathrm{E}} X_j = 2^{n[H(E|A)-c\delta]}\tilde{\mathrm{E}}\left(\Pi P P_{w^j} S_{w^j} P_{w^j} P \Pi\right) = 2^{n[H(E|A)-c\delta]}\Pi\theta'\Pi$$

and $\mu = 2^{n[H(E|A)-H(E)-5c\delta/2]} = 2^{-n\left[x\left(\{\pi_x\},\left\{S_E^x\right\}\right)+5c\delta/2\right]}$, so that $N_E\mu = 2^{-2nc\delta}$ and (10.76) imply

$$\begin{aligned}
\tilde{\mathrm{P}}\left\{\omega : \left\|\frac{1}{N_E}\sum_{j=1}^{N_E} X_j(\omega) - M\right\|_1 \geq \varepsilon_2 2^{n[H(E|A)-c\delta]}\right\} &\leq 2d_E^n \exp\left(-2^{-2nc\delta}\varepsilon_2^2/4\right)\\
&\leq 2^{-2^{-n\beta_1}} \qquad (10.70)
\end{aligned}$$

for some $\beta_1 > 0$ and n large enough. Here, we used the fact that $\operatorname{Tr} M \leq 2^{n[H(E|A)-c\delta]}$. It remains for us to derive (10.67) from (10.70).

Denoting $\theta = \Pi\theta'\Pi$, we have

$$\left\| \frac{1}{N_E} \sum_{j=1}^{N_E} S_{w^j} - \theta \right\|_1 \leq \frac{1}{N_E} \sum_{j=1}^{N_E} \| S_{w^j} - P S'_{w^j} P \|_1 \tag{10.71}$$

$$+ \left\| \frac{1}{N_E} \sum_{j=1}^{N_E} P S'_{w^j} P - \frac{1}{N_E} \sum_{j=1}^{N_E} \Pi P S'_{w^j} P \Pi \right\|_1 \tag{10.72}$$

$$+ \left\| \frac{1}{N_E} \sum_{j=1}^{N_E} \Pi P S'_{w^j} P \Pi - \theta \right\|_1 . \tag{10.73}$$

The estimate (10.70) implies

$$\tilde{\mathrm{P}} \left\{ \left\| \frac{1}{N_E} \sum_{j=1}^{N_E} \Pi P S'_{w^j} P \Pi - \theta \right\|_1 \leq \varepsilon_2 \right\} > 1 - 2^{-2^{-n\beta_1}} .$$

The inequality

$$\left\| \frac{1}{N_E} \sum_{j=1}^{N_E} \Pi P S'_{w^j} P \Pi - \theta \right\|_1 \leq \varepsilon_2 \tag{10.74}$$

gives the estimate for the term (10.73).

For the term (10.71), we use the triangle inequality

$$\| S_{w^j} - P S'_{w^j} P \|_1 \leq \| S_{w^j} - P_{w^j} S'_{w^j} P_{w^j} \|_1 + \| S'_{w^j} - P S'_{w^j} P \|_1 .$$

The first term on the right can be made small for sufficiently large n by property ii and Lemma 10.33. Further, note that for $w^j \in \hat{T}^{n,\delta_1}$

$$\operatorname{Tr} P S'_{w^j} = \operatorname{Tr} S'_{w^j} - \operatorname{Tr}(I - P) S'_{w^j} \geq \operatorname{Tr} P_{w^j} S_{w^j} - \operatorname{Tr}(I - P) S_{w^j} \geq 1 - 2\varepsilon_1 \tag{10.75}$$

by ii and iii. Applying the lemma, we can also make the second term on the right small for sufficiently large n.

The term (10.72) has the form $\| S - \Pi S \Pi \|_1$. Therefore, to show that it is close to zero, by Lemma 10.33 it is sufficient to show that

$$\operatorname{Tr} \Pi S = \operatorname{Tr} \frac{1}{N_E} \sum_{j=1}^{N_E} \Pi P S'_{w^j} P \Pi$$

is close to 1 . But, according to (10.74), this is not less than $\operatorname{Tr} \theta - \varepsilon_2 = \operatorname{Tr} \Pi \theta' - \varepsilon_2$. Now, $\operatorname{Tr} \Pi \theta' = \operatorname{Tr} \theta' - \operatorname{Tr}(I - \Pi) \theta' \geq \operatorname{Tr} \theta' - 2^{-nc\delta/2}$, because $\operatorname{Tr}(I - \Pi)\theta'$ is the sum of eigenvalues of θ' that are less than $2^{-n[H(E)+3c\delta/2]}$, while the total number of positive eigenvalues is less than or equal to $\dim\operatorname{supp} \theta' \leq \dim\operatorname{supp} P = 2^{n[H(E)+c\delta]}$. It remains for us to prove that $\operatorname{Tr} \theta'$ is close to 1 . However, $\theta' = \tilde{\mathrm{E}} P S'_{w^j} P$ and $\operatorname{Tr} \theta' = \tilde{\mathrm{E}} \operatorname{Tr} P S'_{w^j} \geq 1 - 2\varepsilon_1$ by (10.75). This implies that, given ε, we can choose $\varepsilon_1, \varepsilon_2$ such that (10.67) holds for n large enough. □

10.10.17 10.4.3 Large Deviations for Random Operators

Theorem 10.34 (Ahlswede and Winter [5]). Let $X_1(\omega), \ldots, X_N(\omega)$ be i.i.d. operatorvalued random variables in $\mathcal{H}, \dim \mathcal{H} = d$, such that $0 \leq X_i(\omega) \leq I, M = \mathrm{E} X_i \geq \mu I$. Then, for $0 \leq \varepsilon \leq 1$,

$$\mathrm{P}\left\{\omega : \left\| \frac{1}{N}\sum_{j=1}^{N} X_j(\omega) - M \right\|_1 \geq \varepsilon \operatorname{Tr} M \right\} \leq 2d \exp\left(-\frac{N\mu\varepsilon^2}{4}\right). \tag{10.76}$$

Proof. The proof consists of several steps. First, we prove the operator Markov inequality. Let X be a Hermitian operator-valued random variable, $t > 0$. In this case,

$$\mathrm{P}\{\omega : X(\omega) \not\leq 0\} \leq \operatorname{Tr} E \exp tX,$$

where $\{\omega : X(\omega) \not\leq 0\} = \overline{\{\omega : X(\omega) \leq 0\}}$. Indeed,

$$\begin{aligned}\mathrm{P}\{\omega : X(\omega) \not\leq 0\} &= \mathrm{P}\{\omega : \exp tX(\omega) \not\leq I\} \\ &\leq \mathrm{E}1_{\{\exp tX \not\leq I\}} \operatorname{Tr} \exp tX \\ &\leq \operatorname{Tr} \mathrm{E} \exp tX,\end{aligned}$$

where the first inequality follows from the fact that $0 \leq Y \not\leq I$ implies $1 \leq \operatorname{Tr} Y$.

Second, by letting $X(\omega) = \sum_{i=1}^{N} X_i(\omega)$, where X_i are i.i.d. Hermitian operatorvalued random variables, we obtain

$$\begin{aligned}\mathrm{P}\left\{\omega : \sum_{i=1}^{N} X_i(\omega) \not\leq 0\right\} &\leq \operatorname{Tr} \mathrm{E} \exp\left(t \sum_{i=1}^{N} X_i\right) \\ &\leq \mathrm{E} \operatorname{Tr} \exp\left(t \sum_{i=1}^{N-1} X_i\right) \exp tX_N \\ &= \operatorname{Tr} \mathrm{E} \exp\left(t \sum_{i=1}^{N-1} X_i\right) \mathrm{E} \exp tX_N\end{aligned}$$

where the Golden-Thompson inequality ([31], Theorem IX.3.7) was used, i.e.,

$$\operatorname{Tr} \exp(A + B) \leq \operatorname{Tr} \exp A \exp B.$$

By inequality (1.18) this is less than or equal to

$$\operatorname{Tr} E \exp\left(t \sum_{i=1}^{N-1} X_i\right) \|E \exp tX_N\|.$$

Applying the estimate iteratively, we get

$$\mathrm{P}\left\{\omega : \sum_{i=1}^{N} X_i(\omega) \not\leq 0\right\} \leq d \left\|\mathrm{E} \exp tX_i\right\|^N. \tag{10.77}$$

Third, let $X_1(\omega), \ldots, X_N(\omega)$ be i. i. d. operator-valued random variables, such that $0 \leq X_i(\omega) \leq I, \mathrm{E}X_i = \mu I$, and $0 \leq \mu \leq a \leq 1$. Then

$$\mathrm{P}\left\{\omega : \frac{1}{N}\sum_{i=1}^{N} X_i(\omega) \not\leq aI\right\} \leq d \exp(-Nh(a;\mu)), \tag{10.78}$$

where $h(a;\mu) = a \ln \frac{a}{\mu} + (1-a) \ln \frac{1-a}{1-\mu}$. Indeed, by using (10.77) for $X_i(\omega) - aI$, we obtain

$$\mathrm{P}\left\{\omega : \frac{1}{N}\sum_{i=1}^{N} X_i(\omega) \not\leq aI\right\} \leq d \left\|\mathrm{E} \exp tX_i\right\|^N \exp(-atN).$$

But $\exp tx \leq 1 + x(\exp t - 1)$ for $x \in [0,1]$; hence

$$\exp tX_i \le I + X_i(\exp t - 1),$$

and the right-hand side is less than or equal to

$$d[1 + \mu(\exp t - 1)]^N \exp(-atN).$$

Taking $\exp t = \frac{a}{\mu}\frac{1-\mu}{1-a} \ge 1$ provides the right-hand side of (10.78). Similarly, for $0 \le a \le \mu \le 1$,

$$\mathrm{P}\left\{\omega : \frac{1}{N}\sum_{i=1}^{N} X_i(\omega) \not\ge aI\right\} \le d\exp(-Nh(a;\mu)). \tag{10.79}$$

Note that $h(\mu;\mu) = 0$, $\frac{\partial}{\partial a}h(a;\mu)\big|_{\mu=a} = 0$, $\frac{\partial^2}{\partial^2 a}h(a;\mu) = \frac{1}{a(1-a)}$. It follows that

$$\frac{\partial^2}{\partial^2 \varepsilon}h(\mu(1\pm\varepsilon);\mu) = \frac{\mu}{(1\pm\varepsilon)(1-\mu(1\pm\varepsilon))} \ge \frac{\mu}{2},$$

if $\mu \le \frac{1}{2}, |\varepsilon| \le 1$. Hence,

$$h(\mu(1\pm\varepsilon);\mu) \ge \frac{\mu\varepsilon^2}{4}. \tag{10.80}$$

Finally, let $X_i(\omega)$ satisfy the conditions of Theorem 10.34. Consider the operator random variables $Y_i(\omega) = \mu M^{-1/2} X_i(\omega) M^{-1/2}$, such that $0 \le Y_i(\omega) \le I$ and $EY_i = \mu I$. We have

$$\begin{aligned}
&\left\{\omega : \left\|\frac{1}{N}\sum_{i=1}^{N} X_i(\omega) - M\right\|_1 < \varepsilon \operatorname{Tr} M\right\} \\
&\quad\supseteq \left\{\omega : (1-\varepsilon)M \le \frac{1}{N}\sum_{i=1}^{N} X_i(\omega) \le (1+\varepsilon)M\right\} \\
&\quad= \left\{\omega : (1-\varepsilon)\mu \le \frac{1}{N}\sum_{i=1}^{N} Y_i(\omega) \le (1+\varepsilon)\mu\right\} \\
&\quad= \left\{\omega : (1-\varepsilon)\mu \le \frac{1}{N}\sum_{i=1}^{N} Y_i(\omega)\right\} \\
&\quad\cap \left\{\omega : \frac{1}{N}\sum_{i=1}^{N} Y_i(\omega) \le (1+\varepsilon)\mu\right\}
\end{aligned}$$

By taking the complements and applying the estimates (10.78) and (10.79), together with (10.80), we get (10.76). □

10.10.18 10.4.4 The Direct Coding Theorem for the Quantum Capacity

The proof of inequality $Q(\Phi) \ge \bar{Q}(\Phi)$ will be based on a "coherent" version of the proof for the private classical capacity, i.e., a version that uses the same random coding, but where the mixtures of states are replaced with superpositions. It is sufficient to prove that for a given input state S the quantity $R = I_c(S,\Phi) - \delta$ is an achievable rate. Achievability of $\bar{Q}(\Phi) - \delta$ is then shown by applying the argument to $\Phi^{\otimes n}$ and taking the
limit $n \to \infty$. In this section, we will show how to construct an encoding and decoding such that

$$F_e\left(\bar{S}^{(n)}, \mathcal{D}^{(n)} \circ \Phi^{\otimes n} \circ \mathcal{E}^{(n)}\right) \to 1, \tag{10.81}$$

where $\bar{S}^{(n)}$ is the chaotic state in $\mathcal{H}^{(n)}, d_n = \dim \mathcal{H}^{(n)} = 2^{nR}$. By the argument following Definition 10.19 this means that the rate R is achievable for asymptotically perfect transmission of quantum information.

For channel Φ, we consider representation (6.7) (Theorem 6.9), namely,

$$\Phi[S] = \mathrm{Tr}_E\, VSV^*,$$

where V is an isometric map from the input space $\mathcal{H}_A$ to the tensor product $\mathcal{H}_B \otimes \mathcal{H}_E$ of the output and the environment spaces.

Consider a spectral decomposition $S = \sum_x \pi_x S_A^x$, where $S_A^x = |\phi_x\rangle_A \langle\phi_x|$, and $\{|\phi_x\rangle_A\}$ form an orthonormal basis. Denote by $|\phi'_x\rangle_{BE} = V|\phi_x\rangle_A$ the joint output states of BE. In this case, the states of B and E, correspondingly, will be $S_B^X = \mathrm{Tr}_E |\phi'_x\rangle_{BE} \langle\phi'_x|$ and $S_E^X = \mathrm{Tr}_B |\phi'_x\rangle_{BE} \langle\phi'_x|$. Let us recall that, according to (10.58),

$$I_c(S, \Phi) = \chi\left(\{\pi_\chi\}, \left\{S_B^X\right\}\right) - \chi\left(\{\pi_\chi\}, \left\{S_E^X\right\}\right). \tag{10.82}$$

Our aim is to construct a sequence of subspaces $\mathcal{H}^{(n)}$ such that $\dim \mathcal{H}^{(n)} = 2^{nR}, R = I_c(S, \Phi) - \delta$, and corresponding encodings and decodings for which (10.81) holds.

Now, consider the block channel $\Phi^{\otimes n}$ and the codebook

$$W^{(n)} = \left\{w^{mj}; m = 1, \ldots, N_B; j = 1, \ldots, N_E\right\},$$

used in the construction of the privacy code, with the corresponding resolution of the identity $M^{(n)} = \{M_{mj}\}$ in $\mathcal{H}_B^{\otimes n}$, such that

$$P_e\left(W^{(n)}, M^{(n)}\right) \equiv \max_{mj}\left(1 - \mathrm{Tr}\, S_{B^{(n)}}^{mj} M_{mj}\right) < \varepsilon, \tag{10.83}$$

where $S_{B^{(n)}}^{mj} = S_B^{x_1} \otimes \cdots \otimes S_B^{x_n}$ if $w^{mj} = (x_1, \ldots, x_n)$,

$$\left\| \frac{1}{N_E} \sum_{j=1}^{N_E} S_{E^{(n)}}^{mj} - \theta \right\|_1 < \sqrt{\varepsilon}, \quad m = 1, \ldots, N_B. \tag{10.84}$$

Consider the space $\mathcal{H}^{(n)}$ with the orthonormal basis $\{|m\rangle; m = 1, \ldots, N_B\}$, where

$$N_B = 2^{n\left[\chi\left(\{\pi_x\}, \left\{S_B^x\right\}\right) - \chi\left(\{\pi_x\}, \left\{S_E^x\right\}\right) - \delta\right]} = 2^{n[I_c(S,\Phi) - \delta]},$$

and the encoding $\mathcal{E}^{(n)}$ given by the following isometric map from $\mathcal{H}^{(n)}$ to $\mathcal{H}_A^{\otimes n}$:

$$|m\rangle \to \frac{1}{\sqrt{N_E}} \sum_{j=1}^{N_E} e^{i\alpha_{mj}} |\phi_{mj}\rangle_A$$

where $|\phi_{mj}\rangle_A = |\phi_{x_1}\rangle_A \otimes \cdots \otimes |\phi_{x_n}\rangle_A$ if $w^{mj} = (x_1, \ldots, x_n)$, and $\{\alpha_{mj}\} = \alpha$ is a collection of phases to be chosen later. Isometry of this map follows from the fact that $\left\{|\phi_{mj}\rangle_A\right\}$ is an orthonormal system, because it is built from the orthonormal vectors $|\phi_x\rangle_A$.

This is what was called the coherent version of the private code for the classical information. The action of the encoding on the maximally entangled vector (10.38) produces the vector

$$\frac{1}{\sqrt{N_B}} \sum_{m=1}^{N_B} |m\rangle \otimes \left[\frac{1}{\sqrt{N_E}} \sum_{j=1}^{N_E} e^{i\alpha_{mj}} |\phi_{mj}\rangle_A\right]$$

The encoding followed by the channel $\Phi^{\otimes n}$ gives

$$\frac{1}{\sqrt{N_B}}\sum_{m=1}^{N_B}|m\rangle\otimes\left[\frac{1}{\sqrt{N_E}}\sum_{j=1}^{N_E}e^{i\alpha_{mj}}\left|\phi'_{mj}\right\rangle_{BE}\right] \tag{10.85}$$

where the vectors $\left|\phi'_{mj}\right\rangle_{BE} = V\left|\phi_{mj}\right\rangle_A$ are again orthonormal. Note that $S^{mj}_{B^{(n)}} = \mathrm{Tr}_E\left|\phi'_{mj}\right\rangle_{BE}\left\langle\phi'_{mj}\right|, S^{mj}_{E^{(n)}} = \mathrm{Tr}_B\left|\phi'_{mj}\right\rangle_{BE}\left\langle\phi'_{mj}\right|$, where, in order to simplify notations, we denote by Tr_E the partial trace with respect to $\mathcal{H}_E^{\otimes n}$, etc.

To construct the decoding $\mathcal{D}^{(n)}$, we first use the observable $M^{(n)} = \{M_{mj}\}$, which provides a measurement of mj with asymptotically vanishing error. By the discussion of the measurement process leading to relation (6.37), there are an auxiliary system $\mathcal{H}_0^{(n)} = \mathcal{H}^{(n)}\otimes\mathcal{H}_1^{(n)}$ with the basis $\{|m\rangle\otimes|j\rangle_1\}$, a unit vector $|\psi_0\rangle\in\mathcal{H}_0^{(n)}$, and a unitary operator U in $\mathcal{H}_B^{\otimes n}\otimes\mathcal{H}_0^{(n)}$, such that

$$M_{mj} = \mathrm{Tr}_0\left(I_{B^{(n)}}\otimes|\psi_0\rangle\langle\psi_0|\right)U^*\left(I_{B^{(n)}}\otimes|mj\rangle_0\langle mj|\right)U,$$

where we denoted $|mj\rangle_0 = |m\rangle\otimes|j\rangle_1$. Defining

$$|\psi_{mj}\rangle_{BE0} = \left(I_{E^{(n)}}\otimes U\right)\left(\left|\phi'_{mj}\right\rangle_{BE}\otimes|\psi_0\rangle\right),$$

we have the following state vector of the system $\mathcal{H}^{(n)}\otimes\mathcal{H}_B^{\otimes n}\otimes\mathcal{H}_E^{\otimes n}\otimes\mathcal{H}_0^{(n)}$:

$$|Y(\alpha)\rangle = \frac{1}{\sqrt{N_B}}\sum_{m=1}^{N_B}|m\rangle\otimes\left[\frac{1}{\sqrt{N_E}}\sum_{j=1}^{N_E}e^{i\alpha_{mj}}\left|\psi_{mj}\right\rangle_{BE0}\right]$$

as the result of the action of the encoding, followed by the channel, and further followed by the measurement, on the maximally entangled vector. Here, $\left\{\left|\psi_{mj}\right\rangle_{BE0}\right\}$ is again an orthonormal system. Relation (10.83) means that the "projection" of this system onto $\mathcal{H}_0^{(n)}$ is close to $\{|mj\rangle_0\}$. More precisely,

$${}_0\langle mj|\left(\mathrm{Tr}_{BE}\left|\psi_{mj}\right\rangle_{BE0}\left\langle\psi_{mj}\right|\right)|mj\rangle_0 > 1-\varepsilon \quad \text{for all } mj$$

The following lemma implies that there exist unit vectors $\left|\chi_{mj}\right\rangle_{BE}\in\mathcal{H}_B^{\otimes n}\otimes\mathcal{H}_E^{\otimes n}$ such that, for $\left|\tilde{\psi}_{mj}\right\rangle_{BE0} = \left|\chi_{mj}\right\rangle_{BE}\otimes|mj\rangle_0$, one has

$$\left|{}_{BE0}\left\langle\psi_{mj}\mid\tilde{\psi}_{mj}\right\rangle_{BE0}\right|^2 > 1-\varepsilon. \tag{10.86}$$

Lemma 10.35. Let $|\varphi\rangle_0\in\mathcal{H}_0, |\psi\rangle\in\mathcal{H}_0\otimes\mathcal{H}$ be two unit vectors. In this case,

$${}_0\langle\varphi|\left(\mathrm{Tr}_{\mathcal{H}}\left|\psi\right\rangle\langle\psi|\right)|\varphi\rangle_0 = \max_{\chi}\mid\langle\psi|\left(|\varphi\rangle_0\otimes|\chi\rangle\right)|^2, \tag{10.87}$$

where the maximum is taken over all unit vectors $|\chi\rangle\in\mathcal{H}$.

Proof. By fixing an orthonormal basis $\{|e_j\rangle\}$ in $\mathcal{H}$, we have $|\chi\rangle = \sum_j c_j|e_j\rangle$, with $\sum_j|c_j|^2 = 1$ and

$$\mid\langle\psi|\left(|\varphi\rangle_0\otimes|\chi\rangle\right)|^2 = \mid\sum_j c_j\langle\psi|\left(|\varphi\rangle_0\otimes|e_j\rangle\right)\Bigg|^2.$$

Maximizing with respect to c_j we obtain (10.87). □

Note that $\left\{\left|\tilde{\psi}_{mj}\right\rangle_{BE0}\right\}$ is again an orthonormal system, approximating $\left\{\left|\psi_{mj}\right\rangle_{BE0}\right\}$ in the sense (10.86). Defining

$$|\Gamma(\alpha)\rangle = \frac{1}{\sqrt{N_B}} \sum_{m=1}^{N_B} |m\rangle \otimes \left[\frac{1}{\sqrt{N_E}} \sum_{j=1}^{N_E} e^{i\alpha_{mj}} \left| \tilde{\psi}_{mj} \right\rangle_{BE0} \right]$$

we have

$$\int \cdots \int \langle \Upsilon(\alpha) \mid \Gamma(\alpha + \alpha') \rangle \, d\mu(\alpha) = \frac{1}{N_B N_E} \sum_{m=1}^{N_B} \sum_{j=1}^{N_E} e^{i\alpha'_{mj}} {}_{BE0} \left\langle \psi_{mj} \mid \tilde{\psi}_{mj} \right\rangle_{BE0}$$

where $d\mu(\alpha)$ is the uniform distribution. Here, the integration eliminates the inner products with $j \neq j'$. One can always pick $\alpha' = \left\{ \alpha'_{mj} \right\}$ such that the right-hand side will be

$$\frac{1}{N_B N_E} \sum_{m=1}^{N_B} \sum_{j=1}^{N_E} \left| {}_{BE0} \left\langle \psi_{mj} \mid \tilde{\psi}_{mj} \right\rangle_{BE0} \right| > \sqrt{1-\varepsilon}$$

by (10.86). Hence, there is an α such that $\operatorname{Re} \langle Y(\alpha) \mid \Gamma(\alpha + \alpha') \rangle > \sqrt{1-\varepsilon}$. By introducing an additional common phase to α'_{mj} we can always make the inner product positive. Hence,

$$\langle \Upsilon(\alpha) \mid \Gamma(\alpha + \alpha') \rangle > \sqrt{1-\varepsilon}. \tag{10.88}$$

There is one more transformation to incorporate into the decoding $\mathcal{D}^{(n)}$, which will leave the system E in the state almost independent of m. To achieve this, note that combining (10.86) with (10.17) gives

$$\| \, |\psi_{mj}\rangle_{BE0} \langle \psi_{mj}| - \left| \tilde{\psi}_{mj} \right\rangle_{BE0} \left\langle \tilde{\psi}_{mj} \right| \, \|_1 < 2\sqrt{\varepsilon} \tag{10.89}$$

Now note that $S^{mj}_{E^{(n)}} = \operatorname{Tr}_{B0} |\psi_{mj}\rangle_{BE0} \langle \psi_{mj}|$ and denote

$$\tilde{S}^{mj}_{E^{(n)}} = \operatorname{Tr}_{B0} \left| \tilde{\psi}_{mj} \right\rangle_{BE0} \left\langle \tilde{\psi}_{mj} \right| = \operatorname{Tr}_B |\chi_{mj}\rangle_{BE} \langle \chi_{mj}| \, .$$

Then (10.89) and Exercise 10.25 imply

$$\left\| S^{mj}_{E^{(n)}} - \tilde{S}^{mj}_{E^{(n)}} \right\|_1 < 2\sqrt{\varepsilon}, \tag{10.90}$$

which, combined with (10.84), implies

$$\left\| \frac{1}{N_E} \sum_{j=1}^{N_E} \tilde{S}^{mj}_{E^{(n)}} - \theta \right\|_1 < O(\sqrt{\varepsilon}), \quad m = 1, \ldots, N_B. \tag{10.91}$$

Consider the vectors

$$|\varphi_m\rangle_{BE1} = \frac{1}{\sqrt{N_E}} \sum_{j=1}^{N_E} e^{i\left(\alpha_{mj} + \alpha'_{mj}\right)} |\chi_{mj}\rangle_{BE} \otimes |j\rangle_1,$$

which are purifications of $\frac{1}{N_E} \sum_{j=1}^{N_E} \tilde{S}^{mj}_{E^{(n)}}$. Let $|\phi_\theta\rangle \in \mathcal{H}_B^{\otimes n} \otimes \mathcal{H}_E^{\otimes n} \otimes \mathcal{H}_1^{(n)}$ be a purification of θ. Then (10.91) implies that there are unitary operators W_m in $\mathcal{H}_B^{\otimes n} \otimes \mathcal{H}_1^{(n)}$ such that

$$\left| {}_{BE1} \left\langle \phi_\theta \mid \left(I_{\mathcal{H}_E^{\otimes n}} \otimes W_m \right) \varphi_m \right\rangle_{BE1} \right| > 1 - O(\sqrt{\varepsilon}) \quad \text{for all } m. \tag{10.92}$$

This follows from inequality (10.33), which says that if two states are close in trace norm, there exist purifications of these states with fidelity close to 1 .

Defining a "controlled unitary" operator $W = \sum_{m=1}^{N_B} e^{i\beta_m} W_m \otimes |m\rangle\langle m|$ in $\mathcal{H}_B^{\otimes n} \otimes \mathcal{H}_0^{(n)}$, where β_m are phases to be adjusted later, we have

$$\left(I_{\mathcal{H}_E^{\otimes n}} \otimes W\right) \left(|\varphi_m\rangle_{BE1} \otimes |m\rangle\right) = e^{i\beta_m} \left(I_{\mathcal{H}_E^{\otimes n}} \otimes W_m\right) |\varphi_m\rangle_{BE1} \otimes |m\rangle.$$

Hence,

$$\begin{aligned} &\left(I_{\mathcal{H}^{(n)}} \otimes I_{\mathcal{H}_E^{\otimes n}} \otimes W\right) |\Gamma\left(\alpha + \alpha'\right)\rangle \\ &\quad = \frac{1}{\sqrt{N_B}} \sum_{m=1}^{N_B} |m\rangle \otimes |m\rangle \otimes e^{i\beta_m} \left(I_{\mathcal{H}_E^{\otimes n}} \otimes W_m\right) |\varphi_m\rangle_{BE1}. \end{aligned}$$

Denoting $\left|\Omega^{(n)}\right\rangle = \frac{1}{\sqrt{N_B}} \sum_{m=1}^{N_B} |m\rangle \otimes |m\rangle$ the maximally entangled vector in $\mathcal{H}^{(n)} \otimes \mathcal{H}^{(n)}$, we have

$$\begin{aligned} &\left(\left\langle\Omega^{(n)}\right| \otimes \langle\phi_\theta|\right) \left(I_{\mathcal{H}^{(n)}} \otimes I_{\mathcal{H}_E^{\otimes n}} \otimes W\right) |\Gamma\left(\alpha + \alpha'\right)\rangle \\ &\quad = \frac{1}{N_B} \sum_{m=1}^{N_B} e^{i\beta_m} \langle\phi_\theta| \left(I_{\mathcal{H}_E^{\otimes}} \otimes W_m\right) |\varphi_m\rangle_{BE1}. \end{aligned}$$

This can be made equal to

$$\frac{1}{N_B} \sum_{m=1}^{N_B} \left| \langle\phi_\theta| \left(I_{\mathcal{H}_E^{\otimes n}} \otimes W_m\right) \right| \varphi_m \Bigg\rangle_{BE1} |$$

by an appropriate choice of phases β_m, which is greater than $1 - O(\sqrt{\varepsilon})$ by the estimate (10.92). Comparing this with (10.88), we have

$$\left(\left\langle\Omega^{(n)}\right| \otimes \langle\phi_\theta|\right) \left(I_{\mathcal{H}^{(n)}} \otimes I_{\mathcal{H}_E^{\otimes n}} \otimes W\right) |\Upsilon(\alpha)\rangle > 1 - O(\sqrt{\varepsilon}),$$

as follows from the triangle inequality (10.31).
Introducing the density operator

$$S' = \mathrm{Tr}_{BE1} \left(I_{\mathcal{H}^{(n)}} \otimes I_{\mathcal{H}_E^{\otimes n}} \otimes W\right) |\mathrm{Y}(\alpha)\rangle\langle\Upsilon(\alpha)| \left(I_{\mathcal{H}^{(n)}} \otimes I_{\mathcal{H}_E^{\otimes n}} \otimes W\right)$$

in $\mathcal{H}^{(n)} \otimes \mathcal{H}^{(n)}$, we have

$$\begin{aligned} F\left(\left|\Omega^{(n)}\right\rangle \left\langle\Omega^{(n)}\right|, S'\right) &\equiv \left\langle\Omega^{(n)}\right| S' \left|\Omega^{(n)}\right\rangle \\ &\geq \left| \left(\left\langle\Omega^{(n)}\right| \otimes \langle\phi_\theta|\right) \left(I_{\mathcal{H}^{(n)}} \otimes I_{\mathcal{H}_E^{\otimes n}} \otimes W\right) |Y(\alpha)\rangle \right|^2 \\ &> 1 - O(\sqrt{\varepsilon}) \end{aligned} \tag{10.93}$$

On the other hand,

$$S' = \left(\mathrm{Id}_{\mathcal{H}^{(n)}} \otimes \mathcal{D}^{(n)} \circ \Phi^{\otimes n} \circ \mathcal{E}^{(n)}\right) \left[\left|\Omega^{(n)}\right\rangle \left\langle\Omega^{(n)}\right|\right]$$

where the decoding $\mathcal{D}^{(n)}$ is defined as

$$\mathcal{D}^{(n)}\left[S_{B^{(n)}}\right] = \mathrm{Tr}_{B1}\, WU \left(S_{B^{(n)}} \otimes |\psi_0\rangle\langle\psi_0|\right) U^* W^*$$

(remember that $|\psi_0\rangle \in \mathcal{H}_0^{(n)} = \mathcal{H}^{(n)} \otimes \mathcal{H}_1^{(n)}$). Then (10.93) is the same as

$$F_e\left(\bar{S}^{(n)}, \mathcal{D}^{(n)} \circ \Phi^{\otimes n} \circ \mathcal{E}^{(n)}\right) > 1 - O(\sqrt{\varepsilon})$$

and (10.81) is established.

10.10.19 10.5 Notes and References

1. The first examples of quantum error-correcting codes were constructed by Shor [39] and by Steane [225]. Many authors contributed to the subsequent development of the subject, sketched in this chapter (see a survey in Nielsen and Chuang [179] and Gottesman [87]). Necessary and sufficient conditions for error correction of Theorem 10.3 were proposed by Knill and Laflamme [153]. For the solution of Exercise 10.4, see [179], n. 10.2. The possibility of error correction is of basic importance to the problem of
the realization of a quantum computer; see, e. g., Nielsen and Chuang [179] and Valiev [235]. An architecture of a fault-tolerant quantum computer was proposed, correcting errors not only in the quantum register, but also in the error-correcting modules; see Kitaev [154] and Steane [225].

The importance of coherent information to perfect error correction was pointed out by Barnum, Nielsen, and Schumacher [18].

2. The relations between the fidelity measures were studied by Fuchs [74], Barnum, Nielsen, and Schumacher [18] and Werner and Kretschmann [158]. Fidelity for mixed states was investigated by Uhlmann [233]. Lemma 10.17 goes back to Powers and Størmer [191]; see also [109].

3. The coding theorem for the quantum capacity was first conjectured by Lloyd [168] as $Q(\Phi) = \max_\rho I_c(\rho, \Phi)$, but it was soon recognized by Di Vincenzo, Shor, and Smolin [65] that $\bar{Q}_n$ is strictly superadditive; see also Smith and Yard [224]. Hence, taking the limit in (10.43) is indeed required. Additional evidence in favor of a heuristic random subspace coding argument was given by Shor [216]. See also the discussion in Horodeckis' paper [138]. The proof based on this approach was given later by Hayden [98].

The inequality $Q(\Phi) \leq \bar{Q}(\Phi)$ (the converse coding theorem), as well as lemmas in Section 10.3.1, were established by Barnum, Nielsen, and Schumacher [18] and Barnum, Knill, and Nielsen [17]. Corollary 10.22 is inspired by an observation of Smith and Smolin [222].

Relation (10.58) was obtained by Schumacher and Westmoreland [201], who used the ideas of classical information theory [3] to relate the "privacy" of information transmission via quantum channel Φ to the quantity

$$\chi\left(\{\pi_\chi\}, \{S_B^X\}\right) - \chi\left(\{\pi_\chi\}, \{S_E^X\}\right).$$

The notion of a degradable channel was introduced by Devetak and Shor [63], who showed that the quantum capacity of a degradable channel is given by the oneletter expression (10.53). This resembles the notion of a "stochastically degraded" channel [47] for classical broadcast channels, with the role of second receiver played by the environment. For such channels, there is a one-letter expression for the capacity region. Antidegradable channels were considered by Caruso, Giovannetti, and Holevo [41]. Corollary 10.28 is obtained in the work of Cubitt, Ruskai, and Smith [49].

Smith and Yard [224] provided an explicit example of a remarkable phenomenon named superactivation. There exist cases in which, given two quantum channels Φ_1, Φ_2 with zero quantum capacity, it is possible to have $Q(\Phi_1 \otimes \Phi_2) > 0$. The example in [224] is built by joining an antidegradable channel Φ_1 with an entanglementbinding channel Φ_2. Further results in this direction were obtained by Cubitt et al. [48]. Shirokov and Shulman [213], Shirokov [214] demonstrated superactivation phenomena for zero-error quantum capacity.

4. A complete proof of the direct coding theorem ($Q(\Phi) \geq \bar{Q}(\Phi)$) was given by Devetak [62]. It is based on an idea that reveals a profound relation between the quantum and the private classical capacities; see(10.58). It is this proof (as well as a simpler proof of the converse) which we follow here. The large deviation estimates for random operators of the Bernstein type using the operator version (10.78) of Hoeffding's inequality ([105], Theorem 1) are due to Ahlswede and Winter [5]. Another proof, based on random subspaces, which is closer to the

initial argument of Lloyd, was given by Hayden, Shor, and Winter [101]. Proposition 10.31 is due to Smith [221]. For more recent results concerning tail bounds for sums of i. i. d. Hermitian matrices, including an improvement of the Ahlswede-Winter inequality using Lieb's theorem on convex trace functions in place of the Golden-Thompson inequality, see Tropp [232].

It was already stressed that a quantum channel is characterized by a whole spectrum of capacities. Apart from the capacities $C, C_\chi, C_{ea}, C_p, Q$, treated in detail in this book, there are classical and quantum feedback capacities (denoted by C_b, Q_b correspondingly) and the classical and quantum capacities with a classical two-side communication (correspondingly C_2, Q_2). In classical information theory, it is well known that feedback does not increase the Shannon capacity of a memoryless channel. In the quantum case, a similar property is established [33] for the entanglement-assisted capacity $C_{ea}(\Phi)$. Regarding the quantum capacity $Q(\Phi)$, it is known that it cannot be increased by an additional unlimited forward classical communication [28, 18]. However, $Q(\Phi)$ can be increased if there is a possibility of transmitting the classical information in the backward direction. Such a protocol would allow one to create the maximum entanglement between the input and output, which can be used for quantum state teleportation. By this trick, even channels with zero quantum capacity supplemented with classical feedback can be used for the reliable transmission of quantum information [179, 33]. For a quantum channel, there is a hierarchy

$$\begin{array}{ccccccc} C_\chi & \leq & C_b & \leq & C_2 & \leq & C_{ea} \\ \text{VI} & & \text{VI} & & \text{VI} & & \\ Q & \leq & Q_b & \leq & Q_2 & \leq & Q_{ea} \end{array}$$

where $\leq$ should be understood as "less than or equal to for all channels and strictly less for some channels" (see Bennett, Devetak, Shor, and Smolin [24]). Also, $C_{ea} = 2Q_{ea}$ and for some other pairs of capacities both inequalities are possible. Furthermore, there exists a so-called "mother" protocol for information transmission that realizes all the protocols, by using additional resources (such as, e. g., feedback or entanglement) [1]. For a very detailed and thoroughly systematized survey of the modern state of the art in the quantum Shannon theory, see the treatises of Watrous [240] and Wilde [248].

10.11 11 Channels with Constrained Inputs

The importance of quantum channels with constrained inputs was clear from the beginning of quantum communication. A main question motivating the emergence of quantum information theory was the capacity of an optical channel with constrained energy of the input signal. From a mathematical point of view, the necessity for constraints appears when the system describing the information carrier is infinite, which in the quantum case means using infinite-dimensional Hilbert space. One such class of systems, called "continuous-variable" quantum systems, whose states are in a natural sense "Gaussian," will be considered in the next chapter. One of the main goals of the present chapter is to obtain general expressions for the capacities of infinitedimensional channels with constrained inputs, suitable for applications to quantum Gaussian channels with the energy constraint.

A new feature of the infinite-dimensional case is the discontinuity and unboundedness of the entropy of quantum states, which requires us to pay serious attention to the continuity of the entropic quantities. Another important feature of channels in infinite dimensions is the natural emergence of generalized "continuous" ensembles, understood as probability measures on the set of all quantum states. Various capacitylike quantities for a quantum channel involve optimization with respect to state ensembles that satisfy the appropriate constraint. The supremums in question turn out to be achievable under certain conditions, namely, continuity of the entropic quantity and the compactness of the constrained set. These two mathematical

problems will be studied in the present chapter. Another subject of this chapter is the structure of entanglement-breaking channels in infinite dimensions.

10.11.1 11.1 Convergence of Density Operators

In what follows, $\mathcal{H}$ is a separable Hilbert space. A linear operator A, defined on $\mathcal{H}$, is called bounded if it maps the unit ball into a norm-bounded subset of $\mathcal{H}$. Most of the definitions in Chapter 2 carry over to bounded operators, and we shall explicitly mention when a modification should be made (see also [193], Chapter VI). In particular, the operator norm $\|A\|$ is defined as in (1.16) with the maximum replaced by the supremum. The operator A is bounded if and only if $\|A\| < \infty$. All bounded operators form the Banach algebra $\mathfrak{B}(\mathcal{H})$. The trace norm $\|\cdot\|_1$ is defined as in (1.14), and the collection of all bounded operators with $\|T\|_1 < \infty$ forms the Banach space $\mathfrak{T}(\mathcal{H})$ of trace-class operators. The inequality

$$|\operatorname{Tr} TA| \leq \|T\|_1 \|A\| \tag{11.1}$$

holds for all $T \in \mathfrak{T}(\mathcal{H}), A \in \mathfrak{B}(\mathcal{H})$. The dual space of $\mathfrak{T}(\mathcal{H})$ is $\mathfrak{T}(\mathcal{H})^* = \mathfrak{B}(\mathcal{H})$, which means that every continuous linear functional on $\mathfrak{T}(\mathcal{H})$ has the form $T \to \operatorname{Tr} TA$ for some $A \in \mathfrak{B}(\mathcal{H})$, with the norm equal to $\|A\|$. Note also that

$$\|A\| \leq \|A\|_1 \tag{11.2}$$

and $\mathfrak{T}(\mathcal{H})$ is a proper subspace of $\mathfrak{B}(\mathcal{H})$ in the infinite-dimensional case.

A density operator (we also use the term state) is a positive trace-class operator with unit trace (cf. Definition 2.2). The state space $\mathfrak{S}(\mathcal{H})$ is the closed convex subset of $\mathfrak{T}(\mathcal{H})$ consisting of all density operators in $\mathcal{H}$. It is a complete separable metric space with the metric defined by the trace norm, i. e., $\rho(S_1, S_2) = \|S_1 - S_2\|_1$.

A sequence of bounded operators $\{A_n\}$ in $\mathcal{H}$ weakly converges to an operator A if $\lim_{n\to\infty}\langle\psi|A_n|\phi\rangle \to \langle\psi|A|\phi\rangle$ for all $\phi, \psi \in \mathcal{H}$. It turns out that the weak convergence, which is in general weaker than the trace norm convergence, coincides with it on $\mathfrak{S}(\mathcal{H})$.

Lemma 11.1. Let $\{S_n\}$ be a sequence of density operators in $\mathcal{H}$ weakly converging to a density operator S. Then it converges to S in the trace norm.

Proof. For any finite-dimensional projector P,

$$\begin{aligned}\|S_n - S\|_1 \leq \|P(S_n - S)P\|_1 + 2\|PS_n(I-P)\|_1 + 2\|PS(I-P)\|_1 \\ + \|(I-P)S_n(I-P)\|_1 + \|(I-P)S(I-P)\|_1.\end{aligned}$$

The first term on the right tends to zero for any choice of P, since $PS_nP \to PSP$ due to the weak convergence, and due to the equivalence of all kinds of convergence in the finite-dimensional case. For the last two terms we have

$$\|(I-P)S(I-P)\|_1 = \operatorname{Tr}(I-P)S(I-P) = \operatorname{Tr}(I-P)S = 1 - \operatorname{Tr} PS,$$

which can be made arbitrarily small by the choice of P, and

$$\|(I-P)S_n(I-P)\|_1 = 1 - \operatorname{Tr} PS_n \to 1 - \operatorname{Tr} PS$$

by the weak convergence. Finally, the intermediate terms can be evaluated as follows:

$$\|PS_n(I-P)\|_1 = \operatorname{Tr} U^* PS_n(I-P) = \operatorname{Tr} U^* P\sqrt{S_n}\sqrt{S_n}(I-P)$$

where U is the unitary operator from the polar decomposition of $PS_n(I-P)$. Now, by the operator Cauchy-Schwarz inequality for the trace,

$$\operatorname{Tr} U^* P\sqrt{S_n}\sqrt{S_n}(I-P) \le \sqrt{\operatorname{Tr} PS_n}\sqrt{1-\operatorname{Tr} PS_n} \to \sqrt{\operatorname{Tr} PS}\sqrt{1-\operatorname{Tr} PS},$$

which can again be made small by the choice of P.

In what follows, when speaking of convergence of density operators or states, we will have in mind the convergence in the sense of this lemma. A subset $K \subseteq \mathfrak{S}(\mathcal{H})$ is compact if any sequence $\{S_n\} \subset \mathfrak{S}(\mathcal{H})$ contains a subsequence that converges to a state $S \in K$.

Theorem 11.2. A trace norm closed subset K of $\mathfrak{S}(\mathcal{H})$ is compact if and only if for arbitrary $\varepsilon > 0$ there exists a finite-rank projector P_ε such that $\operatorname{Tr} P_\varepsilon S > 1-\varepsilon$ for all $S \in K$.

Proof. Let K be a trace norm compact subset of $\mathfrak{S}(\mathcal{H})$. Suppose that there exists $\varepsilon > 0$ such that for an arbitrary finite-rank projector P there exists a state $S \in K$ such that $\operatorname{Tr} PS \le 1-\varepsilon$. Let P_n be a sequence of finite-rank projectors in $\mathcal{H}$ converging monotonously to the identity operator $I_\mathcal{H}$ in the weak operator topology and let S_n be the corresponding sequence of states in K. By the compactness of K, there exists a subsequence S_{n_k} that converges to a state $S_0 \in K$. By construction $\operatorname{Tr} P_{n_l} S_{n_k} \le \operatorname{Tr} P_{n_k} S_{n_k} \le 1-\varepsilon$ for $k > l$. Hence,

$$\operatorname{Tr} S_0 = \lim_{l\to+\infty} \operatorname{Tr} P_{n_l} S_0 = \lim_{l\to+\infty} \lim_{k\to+\infty} \operatorname{Tr} P_{n_l} S_{n_k} \le 1-\varepsilon,$$

which contradicts the fact that $S_0 \in K \subseteq \mathfrak{S}(\mathcal{H})$.

Conversely, let K be a closed subset of $\mathfrak{S}(\mathcal{H})$ that satisfies the criterion, and let S_n be an arbitrary sequence in K. Since the unit ball in $\mathfrak{B}(\mathcal{H})$ is compact in the weak operator topology (this follows from the Banach-Alaoglu theorem, see, e. g., [193], Theorem VI.21), there exists a subsequence S_{n_k} that converges weakly to a positive operator S_0. We have

$$\operatorname{Tr} S_0 \le \liminf_{k\to\infty} \operatorname{Tr} S_{n_k} = 1.$$

Therefore, to prove that S_0 is a state, it is sufficient to show that $\operatorname{Tr} S_0 \ge 1$. Let $\varepsilon > 0$ and P_ε be the corresponding projector. We have

$$\operatorname{Tr} S_0 \ge \operatorname{Tr} P_\varepsilon S_0 = \lim_{k\to\infty} \operatorname{Tr} P_\varepsilon S_{n_k} > 1-\varepsilon,$$

where the equality follows from the fact that P_ε has finite rank. Thus, S_0 is a state. Lemma 11.1 implies that the subsequence S_{n_k} converges to the state S_0 in the trace norm. Thus, the set K is compact. □

In the sequel we will need the following partial infinite-dimensional analog of the spectral decomposition (1.5). Let $\{|e_j\rangle\}$ be an orthonormal basis in $\mathcal{H}$ and $\{f_j\}$ a sequence of real numbers bounded from below. In this case, the formula

$$F|\psi\rangle = \sum_j f_j\, |e_j\rangle\, \langle e_j \mid \psi\rangle \tag{11.3}$$

defines a self-adjoint operator F (see Section 12.1.1) on the dense domain

$$\mathcal{D}(F) = \left\{ \psi : \sum_j |f_j|^2\, |\langle e_j \mid \psi\rangle|^2 < \infty \right\}, \tag{11.4}$$

for which $|e_j\rangle$ are the eigenvectors and f_j are the corresponding eigenvalues.

Definition 11.3. An operator defined on the domain (11.4) by formula (11.3) will be called an operator of the type $\mathfrak{F}$.

In applications, F is the operator of energy (of an oscillator system). In connection with this, an important role will be played by the operator $\exp(-\theta F), \theta > 0$, defined by the relation

$$\exp(-\theta F)|\psi\rangle = \sum_j \exp\left(-\theta f_j\right)|e_j\rangle\langle e_j \mid \psi\rangle \tag{11.5}$$

which is a bounded positive operator of the type $\mathfrak{F}$.

Let F be an operator of the type $\mathfrak{F}$. For an arbitrary density operator S, we define the expectation

$$\operatorname{Tr} SF = \sum_{j=1}^{\infty} f_j \langle e_j| S |e_j\rangle \leq +\infty, \tag{11.6}$$

which is correctly defined, with values in $(-\infty, +\infty]$.

Lemma 11.4. The functional $S \to \operatorname{Tr} SF$ is affine lower semicontinuous on the set $\mathfrak{S}(\mathcal{H})$.

Proof. Affinity is obvious. Next, we will use the fact that the least upper bound of a family of continuous functions is lower semicontinuous. We have

$$\operatorname{Tr} SF = \sup_N \sum_{j=1}^{N} f_j \langle e_j| S |e_j\rangle$$

where all the finite sums are continuous. Hence, $S_n \to S$ implies

$$\liminf_{n\to\infty} \operatorname{Tr} S_n F \geq \operatorname{Tr} SF,$$

which means the lower semicontinuity. □

Lemma 11.5. Let the spectrum of the operator F consist of the eigenvalues f_n of finite multiplicity and $\lim_{n\to\infty} f_n = +\infty$. In this case, the set

$$\mathfrak{S}_E = \{S : \operatorname{Tr} SF \leq E\} \tag{11.7}$$

is compact.

Proof. Without loss of generality, we assume that f_n is monotonously nondecreasing, and we denote by P_n the finite-dimensional projector onto the eigenspace corresponding to the first n eigenvalues, so that $P_n \uparrow I$. The set $\mathfrak{S}_E$ is closed, due to Lemma 11.4. Since $f_{n+1}(I - P_n) \leq F$, we have $\operatorname{Tr} S(I - P_n) \leq f_{n+1}^{-1} \operatorname{Tr} SF \leq f_{n+1}^{-1} E < \varepsilon$ for large enough n and for all $S \in \mathfrak{S}_E$. By the criterion of compactness of Theorem 11.2, $\mathfrak{S}_E$ is compact. □

In applications this result implies the compactness of the set of quantum states with mean energy bounded by a certain constant.

10.11.2 11.2 Quantum Entropy and Relative Entropy

In the infinite-dimensional case, the von Neumann entropy $H(S)$ of a density operator S can be defined as in formula (5.7), although now it can take the value $+\infty$ if the corresponding series diverges. The relative entropy can be correctly defined by using formula (7.2). Most of the properties in Chapter 7 can be extended to this case, except for the continuity, which is weakened to the lower semicontinuity.

Theorem 11.6. The quantum entropy and relative entropy are lower semicontinuous on $\mathfrak{S}(\mathcal{H})$. Let $\{S_n\}$ (resp. $\{S'_n\}$) be a sequence of density operators in $\mathcal{H}$, converging to a density operator S (resp. S'). Then

$$H(S) \leq \liminf_{n\to\infty} H(S_n),$$
$$H(S; S') \leq \liminf_{n\to\infty} H(S_n; S'_n).$$

Proof. By inequality (11.2), we have $\|S_n - S\| \to 0$. The function $\eta(x) = -x \log x$ is continuous on the interval $[0, 1]$. Hence, $\|\eta(S_n) - \eta(S)\| \to 0$. Indeed, $\eta(x)$ can be uniformly approximated by a polynomial on $[0, 1]$, and then we can use the following estimate.

Exercise 11.7 For a polynomial f and arbitrary operators A, B of norm less than or equal to one,

$$\|f(A) - f(B)\| \leq C_f \|A - B\|$$

where the constant depends only on f. Hint: use the decomposition

$$A^k - B^k = \sum_{l=0}^{k-1} A^{k-l-1}(A - B)B^l$$

Therefore, for any finite-dimensional projector P, due to inequality (11.1) we have

$$|\operatorname{Tr} P(\eta(S_n) - \eta(S))| \leq \operatorname{Tr} P \|\eta(S_n) - \eta(S)\| \to 0. \tag{11.8}$$

On the other hand, by the same inequality, for a Hermitian positive operator A,

$$\operatorname{Tr} PA \leq \|P\| \operatorname{Tr} A,$$

and hence $\operatorname{Tr} A = \sup_P \operatorname{Tr} PA$, where P runs over all finite-dimensional projectors. Thus,

$$H(S) = \sup_P \operatorname{Tr} P\eta(S) \leq \liminf_{n\to\infty} \sup_P \operatorname{Tr} P\eta(S_n) = \liminf_{n\to\infty} H(S_n).$$

Similarly, by using representation (7.23) for the relative entropy, we get

$$H(S; S') = \sup_{\lambda>0} \frac{1}{\lambda} [H(\lambda S + (1-\lambda)S') - \lambda H(S) - (1-\lambda)H(S')]$$

hence

$$\begin{aligned} H(S; S') &= \sup_{P,\lambda>0} \frac{1}{\lambda} \operatorname{Tr} P [\eta(\lambda S + (1-\lambda)S') - \lambda\eta(S) - (1-\lambda)\eta(S')] \\ &\leq \liminf_{n\to\infty} \sup_{P,\lambda>0} \frac{1}{\lambda} \operatorname{Tr} P [\eta(\lambda S_n + (1-\lambda)S_n') - \lambda\eta(S_n) - (1-\lambda)\eta(S_n')] \\ &= \liminf_{n\to\infty} H(S_n; S_n') \end{aligned}$$

□

Lemma 11.8. Let F be an operator of type $\mathfrak{F}$, satisfying the condition

$$\operatorname{Tr} \exp(-\theta F) < \infty \quad \text{for all } \theta > 0. \tag{11.9}$$

In this case, the quantum entropy $H(S)$ is bounded and continuous on the set $\mathfrak{S}_E$ defined in (11.7).

Note that relation (11.9) implies that the operator F satisfies the conditions of Lemma 11.5, and hence the set $\mathfrak{S}_E$ is compact.

Proof. By introducing the density operator $S_\theta = \exp(-\theta F - c(\theta))$, where $c(\theta) = \ln \operatorname{Tr} \exp(-\theta F)$, we have

$$H(S) = -H(S; S_\theta) + \theta \operatorname{Tr} SF + c(\theta), \tag{11.10}$$

where $H(S; S_\theta)$ is the relative entropy. Hence,

$$H(S) \leq -H(S; S_\theta) + \theta E + c(\theta), \tag{11.11}$$

if $S \in \mathfrak{S}_E$. Therefore, the entropy $H(S)$ is bounded on $\mathfrak{S}_E$. Since $H(S)$, by Theorem 11.6, is lower semicontinuous, it is sufficient to show that it is also upper semicontinuous, and hence continuous, on the compact set $\mathfrak{S}_E$. Let $\{S_n\} \subset \mathfrak{S}_E$ be a sequence of states weakly converging to S. From inequality (11.11) applied to S_n, by the lower semicontinuity of the relative entropy,

$$\begin{aligned} \limsup_{n\to\infty} H(S_n) &\le -H(S;S_\theta) + \theta E + c(\theta) \\ &= H(S) + \theta(E - \operatorname{Tr} SF), \end{aligned} \tag{11.12}$$

where in the last equality we used (11.10). Letting $\theta \to 0$, we obtain the upper semicontinuity of $H(S)$. $\square$

Note that when F is the operator of the energy, S_θ is the density operator of the Gibbs equilibrium state at the inverse temperature θ, and the function $-\theta^{-1}c(\theta)$ is the free energy. The relation (11.10) and the nonnegativity of the relative entropy imply

$$H(S) \le \theta \operatorname{Tr} SF + c(\theta), \tag{11.13}$$

which is equivalent to the Gibbs variational principle.

10.11.3 11.3 Constrained c-q Channel

Let $\mathcal{X} = \{x\}$ be an infinite alphabet. For every x, let S_x be a density operator in $\mathcal{H}$ with finite von Neumann entropy $H(S_x)$. The map $x \to S_x$ will be called a c - q channel with input alphabet $\mathcal{X}$. Let $f(x)$ be a function defined on $\mathcal{X}$, taking values in $[0, +\infty]$. We shall consider the class $\mathcal{P}_E$ of finitely supported probability distributions $\pi = \{\pi_x\}$ on $\mathcal{X}$ satisfying the condition

$$\sum_x f(x)\pi_x \le E \tag{11.14}$$

where E is a positive real number. We assume that $\mathcal{P}_E$ is nonempty and impose the following condition onto the channel:

$$\sup_{\pi\in\mathcal{P}_E} H\left(\sum_x \pi_x S_x\right) < \infty \tag{11.15}$$

Definition 11.9. We define a code $(\ W, M\ )$ of size N and length n as in Definition 5.1, with the additional requirement that all codewords $w = (x_1, \dots, x_n) \in W$ satisfy the additive constraint

$$f(x_1) + \cdots + f(x_n) \le nE. \tag{11.16}$$

The average error $\bar{P}_e(W, M)$ and the minimal error $\bar{p}_e(n, N)$ of the code are given by formulas (5.5) and (5.6), respectively. The constrained classical capacity of channel $x \to S_x$ is defined as in Definition 5.2, i.e., as the supremum of achievable rates R such that $\lim_{n\to\infty} \bar{p}_e\left(n, 2^{nR}\right) = 0$.

Theorem 11.10. The constrained classical capacity C of a $c-q$ channel $x \to S_x$ that satisfies condition (11.15), with input constraint (11.16), is equal to the quantity

$$C_\chi = \sup_{\pi\in\mathcal{P}_E} \left[H\left(\sum_x \pi_x S_x\right) - \sum_x \pi_x H(S_x) \right]. \tag{11.17}$$

Proof. We denote by $\mathcal{P}_E^{(n)}$ the class of probability distributions on $\mathcal{X}^n$ satisfying the condition

$$\sum_{x_1,\dots,x_n} [f(x_1)+\cdots+f(x_n)]\,\pi_{x_1,\dots,x_n} \le nE \tag{11.18}$$

and define the quantity $C_\chi^{(n)}$ as in (5.29), with the modification that the supremum with respect to π is taken over $\mathcal{P}_E^{(n)}$, i.e.,

$$C_\chi^{(n)} = \sup_{\pi\in\mathcal{P}_E^{(n)}} \chi(\{\pi_w\};\{S_w\})$$

Lemma 11.11. The sequence $\left\{C_\chi^{(n)}\right\}$ is additive, i.e., $C_\chi^{(n)} = nC_\chi$.

Proof. By (5.30), we have

$$\chi_n(\pi) \le \sum_{k=1}^n \chi\left(\pi^{(k)}\right),$$

where $\pi^{(k)}$ is the k th marginal distribution of π on $\mathcal{X}$. Also,

$$\sum_{k=1}^n \chi\left(\pi^{(k)}\right) \le n\chi(\bar\pi), \tag{11.19}$$

where $\bar\pi = \frac{1}{n}\sum_{k=1}^n \pi^{(k)}$, since $\chi(\pi)$ is a concave function of π (as follows from concavity of the von Neumann entropy). Inequality (11.18) can be rewritten as

$$\frac{1}{n}\sum_{k=1}^n \sum_x f(x)\pi^{(k)}(x) \le E$$

which implies that $\bar\pi \in \mathcal{P}_E$ if $\pi \in \mathcal{P}_E^{(n)}$. Taking the supremum in relation (11.19) with respect to $\pi \in \mathcal{P}_E^{(n)}$, we obtain $C_\chi^{(n)} \le nC_\chi$. The converse inequality is obvious. □

The proof of the converse coding theorem can be based on the following corollary of the Fano inequality (cf. (5.32)):

$$\bar P_e(W,M) \ge 1 - \frac{\sup_{\pi\in\mathcal{P}_E^{(n)}} \sup_M \mathcal{I}_n(\pi,M)}{nR} - \frac{1}{nR}, \tag{11.20}$$

which is obtained as follows. Let again the words in the code (W, M) be taken with the input distribution $\pi^{(N)}$ assigning equal probability $1/N$ to each word. Consider inequality (4.37). Since the words in the code satisfy (11.16), we have $\pi^{(N)} \in \mathcal{P}_E^{(n)}$, and hence (11.20) follows.

Using inequality (11.20) and Theorem 5.9, we obtain

$$\bar p_e\left(n, 2^{nR}\right) \ge 1 - \frac{C_\chi}{R} - \frac{1}{nR},$$

where C_χ is defined by (11.17), which implies $p_e\left(n, 2^{nR}\right) \nrightarrow 0$ for $R > C_\chi$.

In the classical information theory, the direct coding theorem for channels with additive constraints can be proved by using random coding with a probability distribution (5.46) modified by a factor concentrated on words, for which the constraint holds close to the equality. The same tool can be applied to a c − q channel. Let π be a distribution on $\mathcal{X}$ satisfying (11.14), and let P be a distribution on the set of N words, under which the words are independent and have the probability distribution (5.46). Let $v_n = \mathrm{P}\left(\frac{1}{n}\sum_{k=1}^n f(x_k) \le E\right)$ and define the modified distribution $\tilde{\mathrm{P}}$ under which the words are still independent, but

$$\tilde{\mathrm{P}}\left(w=(x_1,\ldots,x_n)\right)=\begin{cases} v_n^{-1}\pi_{x_1}\cdots\pi_{x_n}, & \text{if } \sum_{k=1}^n f\left(x_k\right)\le nE,\\ 0, & \text{otherwise .}\end{cases} \tag{11.21}$$

Let us remark that since $\pi\in\mathcal{P}_E$, we have $Ef\le E$ (where E is the expectation corresponding to P) and hence, by the central limit theorem,

$$\lim_{n\to\infty} v_n\ge 1/2.$$

Therefore, $\tilde{\mathrm{E}}\xi\le 2^m\mathrm{E}\xi$ (where $\tilde{\mathrm{E}}$ is the expectation corresponding to $\tilde{\mathrm{P}}$) for any nonnegative random variable ξ depending on m different words.

For the error probability $\bar{P}_e(W,M)$, we have the basic upper bound (5.51). Now, take the expectation of this bound with respect to $\tilde{P}$. Since every term in the right-hand side of (5.51) depends on no more than two different words, we have

$$\tilde{\mathrm{E}}\inf_M \bar{P}_e(W,M)\le 4\mathrm{E}\inf_M \bar{P}_e(W,M),$$

and the expectation with respect to P can be made arbitrarily small for $N=2^{nR}, n\to\infty$, with $R<C_\chi-3\delta$. Thus, $\tilde{E}\bar{P}_e(W,M)$ can also be made arbitrarily small under the same circumstances. Since the distribution $\tilde{\mathrm{P}}$ is concentrated on words that satisfy (11.16), we can choose a code for which $\bar{P}_e(W,M)$ can be made arbitrarily small for sufficiently large n. □

10.11.4 11.4 Classical-Quantum Channel with Continuous Alphabet

Let the input alphabet $\mathcal{X}$ be a complete, separable metric space with the σ-algebra of Borel subsets. In applications, $\mathcal{X}$ is typically a domain in $\mathbb{R}^k$ that is locally compact. However, we need the more general case for the treatment of infinite-dimensional quantum channels in the next section. We consider the c − q channel given by a continuous mapping $x\to S_x$ from the alphabet $\mathcal{X}$ to the set of quantum states $\mathfrak{S}(\mathcal{H})$ (by Lemma 11.1, for continuity it is necessary and sufficient that all matrix elements $\langle\psi|S_x|\phi\rangle;\psi,\phi\in\mathcal{H}$ are continuous with respect to the metric in $\mathcal{X}$). We will obtain a convenient integral expression for the classical capacity C of the channel $x\to S_x$ under the constraint (11.16).

We assume that f is a nonnegative Borel function on $\mathcal{X}$. Consider the set $\mathcal{P}_E^B$ of Borel probability measures π on $\mathcal{X}$ satisfying

$$\int_{\mathcal{X}} f(x)\pi(dx)\le E. \tag{11.22}$$

Recall that a sequence of Borel probability measures $\{\pi_n\}$ converges weakly to π if

$$\int_{\mathcal{X}}\varphi(x)\pi_n(dx)\to\int_{\mathcal{X}}\varphi(x)\pi(dx)$$

for arbitrary $\varphi\in C(\mathcal{X})$, the Banach space of bounded continuous functions on $\mathcal{X}$ (see, e. g., Parthasarathy's book [186]).

Exercise 11.12 Let f be lower semicontinuous. In this case, the functional $\pi\to\int_{\mathcal{X}} f(x)\pi(dx)$ is lower semicontinuous with respect to the weak convergence of probability measures.

Hint: use the fact that f is the least upper bound of the family of all bounded continuous functions $\varphi\le f$.

We will need the following auxiliary result, the proof of which can be found in [186].
Lemma 11.13. Let f be lower semicontinuous. In this case, the set $\mathcal{P}_E$ of all finitely supported probability measures that satisfy (11.22) is weakly dense in $\mathcal{P}_E^B$.

Let us also give a convenient sufficient condition of weak compactness of the set $\mathcal{P}_E^B$.

Lemma 11.14. Assume that f is lower semicontinuous and for any positive k the set $\{x : f(x) \leq k\} \subset \mathcal{X}$ is compact. Then the subset of probability measures

$$\mathcal{P}_E^B = \left\{\pi : \int_{\mathcal{X}} f(x)\pi(dx) \leq E\right\}$$

is weakly compact.

Proof. The lower semicontinuity of f implies that the functional $\pi \to \int_{\mathcal{X}} f(x)\pi(dx)$ is lower semicontinuous with respect to the weak convergence of probability measures (Exercise 11.12). Hence, the set $\mathcal{P}_E^B$ is weakly closed. It is known that a weakly closed subset $\mathcal{P}$ of Borel probability measures on $\mathcal{X}$ is weakly compact if and only if for any $\varepsilon > 0$ there is a compact $K \subset \mathcal{X}$, such that $\pi(\bar{K}) \leq \varepsilon$ for all $\pi \in \mathcal{P}$ (see, e. g., [186]). For a given $\varepsilon > 0$, consider the compact set $K = \{x : f(x) \leq E/\varepsilon\}$. Then,

$$\pi(\bar{K}) \leq \frac{\varepsilon}{E} \int_{\bar{K}} f(x)\pi(dx) \leq \varepsilon$$

for $\pi \in \mathcal{P}_E^B$. Hence, the set $\mathcal{P}_E^B$ is weakly compact.

For an arbitrary Borel probability measure π on $\mathcal{X}$, we introduce the average state

$$\bar{S}_\pi = \int_{\mathcal{X}} S_x \pi(dx) \tag{11.23}$$

where, by assumption, the function S_x is continuous, the integral is well-defined, and it represents a density operator in $\mathcal{H}$.

Assuming $H\left(\bar{S}_\pi\right) < \infty$, consider the functional

$$\chi(\pi) = H\left(\bar{S}_\pi\right) - \int_{\mathcal{X}} H\left(S_x\right) \pi(dx) \tag{11.24}$$

where, by Theorem 11.6, the function $H\left(S_x\right)$ is nonnegative and lower semicontinuous and hence the integral is well-defined.

Theorem 11.15. Let there exist a self-adjoint operator F of the type $\mathfrak{F}$, satisfying condition (11.9), such that

$$f(x) \geq \operatorname{Tr} S_x F, \quad x \in \mathcal{X}. \tag{11.25}$$

Then the condition (11.15) holds and the classical capacity C of the channel $x \to S_x$ with the constraint (11.16) is finite and is given by the relation (11.17).

If, moreover, the function f satisfies the conditions of Lemma 11.14, then

$$C = \max_{\pi \in \mathcal{P}_E^B} \chi(\pi) \tag{11.26}$$

Proof. By integrating (11.25), we obtain

$$\operatorname{Tr} \bar{S}_\pi F \leq E \tag{11.27}$$

for $\pi \in \mathcal{P}_E$. Hence, by (11.13),

$$H\left(\bar{S}_\pi\right) \leq \theta \operatorname{Tr} \bar{S}_\pi F + c(\theta) \leq \theta E + c(\theta)$$

Therefore, condition (11.15) is fulfilled, C is finite and equal to (11.17).

If the function f satisfies the conditions of Lemma 11.14, the set $\mathcal{P}_E^B$ is weakly compact. Let us show that the functional $\pi \to \chi(\pi)$ is upper semicontinuous. From expression (11.17) and Lemma 11.13 it now follows that

$$C = \sup_{\pi \in \mathcal{P}_E} \chi(\pi) = \sup_{\pi \in \mathcal{P}_E^B} \chi(\pi).$$

Moreover, the last supremum is achieved by upper semicontinuity of $\chi(\pi)$ and compactness of $\mathcal{P}_E^B$.

Consider the first term in expression (11.24) for $\chi(\pi)$. Since the matrix elements of the family $\{S_x\}$ depend continuously on x, the mapping $\pi \to \bar{S}_\pi$ into the set $\mathfrak{S}_E$, equipped with the weak operator topology, is continuous with respect to the weak convergence of probability measures. By Lemma 11.1, the weak operator topology on $\mathfrak{S}(\mathcal{H})$ is equivalent to the trace norm topology. By Lemma 11.8, the entropy is continuous on $\mathfrak{S}_E$. Therefore, the functional $\pi \to H\left(\bar{S}_\pi\right)$ is continuous on the set $\mathcal{P}_E^B$.

The function $x \to H(S_x)$ is lower semicontinuous. Hence, by Exercise 11.12, the second term in (11.24) is upper semicontinuous in π. Thus, the functional (11.24) is also upper semicontinuous.

10.11.5 11.5 Constrained Quantum Channel

Let $\mathcal{H}_A, \mathcal{H}_B$ be separable Hilbert spaces called the input and output spaces, respectively.

Definition 11.16. By channel we call a linear, bounded, trace-preserving, completely positive map $\Phi : \mathfrak{T}(\mathcal{H}_A) \to \mathfrak{T}(\mathcal{H}_B)$. As in the finite-dimensional case, complete positivity means that, for any $n = 1, 2 \ldots$, the map $\Phi \otimes \mathrm{Id}_n$ is positive.

Exercise 11.17 Sow that any affine map $\Phi_s : \mathfrak{S}(\mathcal{H}_A) \to \mathfrak{S}(\mathcal{H}_B)$ extends uniquely to a linear, bounded, positive map $\Phi : \mathfrak{T}(\mathcal{H}_A) \to \mathfrak{T}(\mathcal{H}_B)$. Hint: to define the linear extension, use the construction of Exercise 2.7. To prove boundedness, use the argument from the proof of Lemma 10.12 (estimates of the type (10.22), (10.23) for $\|\Phi[T]\|_1$).

Example 11.18. Let $x \to S_x$ be a c-q channel with the input alphabet $\mathcal{X}$, which is a complete separable metric space. Then it can be extended to a quantum channel in the sense of Definition 11.16 as follows. Consider the Hilbert space $\mathcal{H}_A = L^2(\mathcal{X}, m)$, where m is a σ-finite measure on $\mathcal{X}$. Assume that S_X is an m-measurable family of density operators in $\mathcal{H}_B$. Any operator $S \in \mathfrak{T}(\mathcal{H}_A)$ is given by a kernel with a correctly defined diagonal value $\langle x|S|x\rangle$. Then the relation

$$\Phi[S] = \int_{\mathcal{X}} \langle x|S|x\rangle S_x m(dx)$$

defines a channel $\Phi : \mathfrak{T}(\mathcal{H}_A) \to \mathfrak{T}(\mathcal{H}_B)$.

In this section, we study the classical capacity of a channel under the additive constraint at its input. Let F be an operator of type $\mathfrak{F}$ in $\mathcal{H}_A$, representing an observable, the mean value of which is to be constrained. We assume that the input states $S^{(n)}$ of the composite channel $\Phi^{\otimes n}$ are subject to the additive constraint

$$\mathrm{Tr}\, S^{(n)} F^{(n)} \leq nE, \tag{11.28}$$

where

$$F^{(n)} = F \otimes \cdots \otimes I + \cdots + I \otimes \cdots \otimes F,$$

and E is a positive constant. Adapting Definition 8.1 and the proof of Proposition 8.2 to the case of the input states constrained by (11.28), one can prove the following.

Proposition 11.19. Let the channel Φ satisfy the condition

$$\sup_{S : \mathrm{Tr}\, SF \leq E} H(\Phi[S]) < \infty. \tag{11.29}$$

Then the classical capacity of this channel, under the constraint (11.28), is finite and is equal to

$$C(\Phi, F, E) = \lim_{n\to\infty} \frac{1}{n} C_\chi \left(\Phi^{\otimes n}, F^{(n)}, nE\right), \tag{11.30}$$

where

$$C_\chi(\Phi, F, E) = \sup_{\pi:\mathrm{Tr}\,\bar{S}_\pi F\le E} \left[H\left(\Phi\left[\bar{S}_\pi\right]\right) - \sum_i \pi_i H\left(\Phi\left[S_i\right]\right)\right] \tag{11.31}$$

Here, $\bar{S}_\pi = \sum_i \pi_i S_i$ is the average state of the ensemble $\pi = \{\pi_i, S_i\}$.
The finiteness of the capacity follows from the following.
Lemma 11.20. Condition (11.29) for the channel Φ implies a similar condition for the channel $\Phi^{\otimes n}$, namely,

$$\sup_{S^{(n)}:\mathrm{Tr}\,S^{(n)}F^{(n)}\le nE} H\left(\Phi^{\otimes n}\left[S^{(n)}\right]\right) \le n \sup_{S:\mathrm{Tr}\,SF\le E} H(\Phi[S]) \tag{11.32}$$

Proof. Denoting by S_j the partial state of $S^{(n)}$ in the j th tensor factor of $\mathcal{H}^{\otimes n}$, and letting $\bar{S} = \frac{1}{n}\sum_{j=1}^n S_j$, we have

$$H\left(\Phi^{\otimes n}\left[S^{(n)}\right]\right) \le \sum_{j=1}^n H\left(\Phi\left[S_j\right]\right) \le nH(\Phi[\bar{S}])$$

where in the first inequality we use subadditivity of the quantum entropy, while in the second we use its concavity. Moreover, $\mathrm{Tr}\,\bar{S}F = \frac{1}{n}\mathrm{Tr}\,S^{(n)}F^{(n)} \le E$ and hence (11.32) follows.

If the channel Φ satisfies the additivity property

$$C_\chi\left(\Phi^{\otimes n}, F^{(n)}, nE\right) = nC_\chi(\Phi, F, E) \tag{11.33}$$

then

$$C(\Phi, F, E) = C_\chi(\Phi, F, E)$$

This is closely related to the property of superadditivity of the convex hull of the output entropy (8.36), which implies the additivity of χ-capacity under the linear constraints (8.39) (see Section 8.3.2).

Exercise 11.21 Prove the following inequality:

$$C_X\left(\Phi^{\otimes n}, F^{(n)}, nE\right) \ge nC_X(\Phi, F, E) \tag{11.34}$$

In any case, the quantity (11.31) provides a lower bound for the classical capacity $C(\Phi, F, E)$. We shall obtain a more convenient expression for $C_\chi(\Phi, F, E)$, by using the results of the previous section. Consider a c-q channel with the alphabet $\mathcal{X} = \mathfrak{S}(\mathcal{H}_A)$, defined by the mapping $S \to \Phi[S]$. The constraint is given by the function $f(S) = \mathrm{Tr}\,SF$, which is affine and lower semicontinuous by Lemma 11.4, whereas the condition (11.15) turns into (11.29).

Definition 11.22. We call generalized ensemble an arbitrary Borel probability measure π on $\mathfrak{S}(\mathcal{H}_A)$. The average state of the generalized ensemble π is defined as the barycenter of the probability measure

$$\bar{S}_\pi = \int_{\mathfrak{S}(\mathcal{H}_A)} S\pi(dS).$$

The conventional ensembles correspond to finitely supported measures.
Theorem 11.6 implies, in particular, that the nonnegative function $S \to H(\Phi[S])$ is measurable. Hence, under condition $H\left(\Phi\left(\bar{S}_\pi\right)\right) < \infty$, the functional

$$\chi_\Phi(\pi) = H\left(\Phi\left(\bar{S}_\pi\right)\right) - \int_{\mathfrak{S}(\mathcal{H}_A)} H(\Phi(S))\pi(dS) \tag{11.35}$$

is well-defined.

Exercise 11.23 Show that the quantity $X_\Phi(\pi)$ is a concave functional of π. Hint: the second term is affine, the concavity of the first term follows from the concavity of the entropy.

Corollary 11.24. Let there exist a positive operator F' in $\mathcal{H}_B$, such that

$$\operatorname{Tr} \exp\left(-\theta F'\right) < +\infty, \quad \text{for all } \theta > 0 \tag{11.36}$$

and

$$\operatorname{Tr} \Phi[S]F' \leq \operatorname{Tr} SF, \quad S \in \mathfrak{S}(\mathcal{H}). \tag{11.37}$$

In this case, condition (11.29) is fulfilled and

$$C_\chi(\Phi, F, E) = \sup_{\pi:\operatorname{Tr}\bar{S}_\pi F \leq E} \chi_\Phi(\pi).$$

Moreover, the output entropy $H(\Phi[S])$ is continuous on the compact set $\mathfrak{S}_E = \{S : \operatorname{Tr} SF \leq E\}$.

If, additionally, F satisfies the conditions of Lemma 11.5, then there exists an optimal generalized ensemble, i.e.,

$$C_\chi(\Phi, F, E) = \max_{\pi:\operatorname{Tr}\bar{S}_\pi F \leq E} \chi_\Phi(\pi). \tag{11.38}$$

Proof. The statement is obtained by applying Theorem 11.15 to the c-q channel $S \to \Phi[S]$, with the constraint function $f(S) = \operatorname{Tr} SF$, the role of condition (11.25) is played by (11.37), and the operator F' plays the role of F. The function $f(S) = \operatorname{Tr} SF$ satisfies the conditions of Lemma 11.14, due to Lemmas 11.4, 11.5.

The continuity of the entropy $H(\Phi[S])$ follows from the continuity of the map $S \to S' = \Phi[S]$ and Lemma 11.8, which guarantees continuity of $H(S')$ on the compact set $\{S' : \operatorname{Tr} S'F' \leq E\}$. □

10.11.6 11.6 Entanglement-Assisted Capacity of Constrained Channels

Let systems A and B share an entangled (pure) state S_{AB}. We assume that the amount of entanglement is unlimited but finite, i.e., $H(S_A) = H(S_B) < \infty$. By generalizing the result of Section 9, one can prove the following.

Proposition 11.25. Let Φ be a channel that satisfies the condition (11.29) with the operator F satisfying (11.9). In this case, its entanglement-assisted classical capacity under the constraint (11.28) is finite and equals

$$C_{ea}(\Phi) = \sup_{S:\operatorname{Tr} SF \leq E} I(S, \Phi), \tag{11.39}$$

where

$$I(S, \Phi) = H(S) + H(\Phi[S]) - H(S; \Phi), \tag{11.40}$$

and $H(S;\Phi)$ is the entropy exchange.
Now, we investigate the problem when the supremum in the right-hand side of (11.39) is achieved. Note that condition (11.9) implies that F satisfies the condition of the Lemma 11.5 and, hence, the set $\mathfrak{S}_E = \{S : \operatorname{Tr} SF \le E\}$ is compact.

Proposition 11.26. Let the constraint operator F satisfy the condition (11.9), and let there exist a self-adjoint operator F' of the type $\mathfrak{F}$, satisfying (11.9) and (11.37). In this case,

$$C_{ea}(\Phi) = \max_{S:\operatorname{Tr} SF\le E} I(S,\Phi). \tag{11.41}$$

Moreover, if the channel Φ is such that

$$\sup_S I(S,\Phi) = \infty, \tag{11.42}$$

the maximum in (11.41) is achieved on a density operator S, that satisfies the constraint with the equality $\operatorname{Tr} SF = E$.

Proof. We will consider each term in formula (11.40) separately. Note that, by Theorem 11.6, the quantum entropy is lower semicontinuous. Since the entropy exchange can be represented as $H(S;\Phi) = H(\tilde{\Phi}[S])$, where $\tilde{\Phi}$ is the complementary channel from the system space $\mathcal{H}_A$ to the environment space $\mathcal{H}_E$, it is also lower semicontinuous and thus the last term in (11.40) is upper semicontinuous. Concerning the first term, by Lemma 11.8, it is continuous on the set $\mathfrak{S}_E = \{S : \operatorname{Tr} SF \le E\}$ if the constraint operator F satisfies (11.9). By using the proof of Corollary 11.24, we can apply a similar argument to the second term in (11.40), namely, $H(\Phi[S])$. Moreover, this corollary also implies that condition (11.29) and hence (11.39) hold. As follows from the above,
the mutual information (11.40) is upper semicontinuous on the compact set $\mathfrak{S}_E$, and hence attains its maximum.

To prove the second statement, we consider

$$f_0(E) = \max_{\operatorname{Tr} SF=E} I(S,\Phi),$$

and we assume that there exists a state S_1 such that

$$\operatorname{Tr} S_1F < E, \quad I(S_1,\Phi) > f_0(E).$$

Condition (11.42) implies that there exists a state S_2 such that

$$\operatorname{Tr} S_2F > E, \quad I(S_2,\Phi) > f_0(E).$$

Now, putting

$$\lambda = \frac{\operatorname{Tr} S_2F - E}{\operatorname{Tr} S_2F - \operatorname{Tr} S_1F},$$

we have $0 < \lambda < 1$ and $\operatorname{Tr}(\lambda S_1 + (1-\lambda)S_2)F = E$, so that

$$I(\lambda S_1 + (1-\lambda)S_2,\Phi) \le f_0(E) < \lambda I(S_1,\Phi) + (1-\lambda) I(S_2,\Phi),$$

which contradicts the concavity of $I(S,\Phi)$. $\square$

10.11.7 11.7 Entanglement-Breaking Channels in Infinite Dimensions

A state $S \in \mathfrak{S}(\mathcal{H}_1 \otimes \mathcal{H}_2)$ is called separable (unentangled) if it belongs to the convex closure (i. e., closure of the convex hull) of the set of all product states $S_1 \otimes S_2 \in \mathfrak{S}(\mathcal{H}_1 \otimes \mathcal{H}_2)$.

Proposition 11.27. State S is separable if and only if it admits a representation

$$S = \int_{\mathcal{X}} S_1(x) \otimes S_2(x) \pi(dx), \tag{11.43}$$

where $\pi(dx)$ is the Borel probability measure and $S_j(x), j = 1, 2$, are Borel $\mathfrak{S}(\mathcal{H}_j)$-valued functions on some complete, separable metric space $\mathcal{X}$.

Proof. According to the definition, the state S is separable if and only if $S = \lim_{n\to\infty} S_n$, where

$$S_n = \int_{\mathfrak{S}(\mathcal{H}_1)} \int_{\mathfrak{S}(\mathcal{H}_2)} S_1 \otimes S_2 \pi_n (dS_1 dS_2), \tag{11.44}$$

and $\{\pi_n\}$ is a sequence of Borel probability measures with finite supports.

Let S be representable in the form (11.43). In this case, by making a change of variable $x \to S_1(x) \otimes S_2(x)$, we can reduce the integral representation (11.43) to

$$S = \int_{\mathfrak{S}(\mathcal{H}_1)} \int_{\mathfrak{S}(\mathcal{H}_2)} S_1 \otimes S_2 \pi (dS_1 dS_2), \tag{11.45}$$

where we use the same notation π for the image of the initial measure under the change of variable. The mapping $\pi \to S$ is continuous under weak convergence of probability measures. This is clear if the set of density operators is equipped with the weak operator topology and, by Lemma 11.1, this topology coincides with the trace norm topology on this set. By Lemma 11.13, there is a sequence $\{\pi_n\}$ of Borel probability measures with finite supports, which converges weakly to π. By using the continuity of the mapping $\pi \to S$, we obtain $S = \lim_{n\to\infty} S_n$, where S_n is given by relation (11.44). Hence, S is separable.

Conversely, let S be a separable state. In this case, $S = \lim_{n\to\infty} S_n$, where S_n is given by (11.44). If we can prove that the sequence of measures $\{\pi_n\}$ is weakly relatively compact, this will imply representation (11.45), where π is a partial limit of this sequence. The converging sequence $\{S_n\}$ is relatively compact. Therefore, by Theorem 11.2, for any $\varepsilon > 0$ there is a finite-dimensional projection P such that $\operatorname{Tr} S_n(I - P) \le \varepsilon$ for all n. For $m = 1, 2, \ldots$ we denote by P_m the projection such that $\operatorname{Tr} S_n (I - P_m) \le 4^{-m}$, and hence

$$\int \operatorname{Tr} (S_1 \otimes S_2)(I - P_m) \pi_n (dS_1 dS_2) \le 4^{-m} \tag{11.46}$$

We introduce the following subsets in the direct product $\mathfrak{S}(\mathcal{H}_1) \times \mathfrak{S}(\mathcal{H}_2)$:

$$K_m = \left\{(S_1, S_2) : \operatorname{Tr} (S_1 \otimes S_2)(I - P_m) \le \delta^{-1} 2^{-m}\right\}, \quad \mathcal{K}_\delta = \cap_{m\ge 1} K_m,$$

where $\delta > 0$. By the same Theorem 11.2, the set $\mathcal{K}_\delta$ is compact by construction. Its complement satisfies

$$\pi_n\left(\overline{\mathcal{K}}_\delta\right) \le \sum_m \pi_n\left(\bar{K}_m\right) \le \delta \sum_m 2^m \int \operatorname{Tr} (S_1 \otimes S_2)(I - P_m) \pi_n (dS_1 dS_2) \le \delta$$

according to (11.46). Thus, the sequence of measures $\{\pi_n\}$ satisfies the criterion of weak relative compactness (see [186]), which completes the proof of the theorem.

Definition 11.28. Channel $\Phi : \mathfrak{T}(\mathcal{H}_A) \to \mathfrak{T}(\mathcal{H}_B)$ is called entanglement-breaking if for an arbitrary Hilbert space $\mathcal{H}_R$ and an arbitrary state $S \in \mathfrak{S}(\mathcal{H}_A \otimes \mathcal{H}_R)$, the state $(\Phi \otimes \mathrm{Id}_R)[S] \in \mathfrak{S}(\mathcal{H}_B \otimes \mathcal{H}_R)$, where Id_R is the identity map in $\mathfrak{T}(\mathcal{H}_R)$, is separable.

To describe the structure of such channels, we will need a generalization of the notion of an observable (Definition 2.9) to the case of an arbitrary set of outcomes.

Definition 11.29. Let $\mathcal{X}$ be a measurable space with a σ-algebra of measurable subsets $\mathcal{B}$. An observable with values in $\mathcal{X}$ is a probability operator-valued measure (POVM) on $\mathcal{X}$, i. e., a family $M = \{M(B), B \in \mathcal{B}\}$ of Hermitian operators in $\mathcal{H}$ satisfying the following conditions:
i. $M(B) \geq 0, B \in \mathcal{B}$;
ii. $M(\mathcal{X}) = I$;
iii. for any countable decomposition $B = \cup B_j$ $(B_i \cap B_j = \emptyset, i \neq j)$ one has $M(B) = \sum_j M(B_j)$ in the sense of weak operator convergence.

A probability operator-valued measure E is called orthogonal (or a spectral measure) if

$$E(B_1 \cap B_2) = E(B_1) E(B_2), \quad B_1, B_2 \in \mathcal{B}.$$

In this case, all operators $E(B)$ are projectors, and the projectors that correspond to disjoint subsets are orthogonal. The corresponding observable is called sharp.

The probability distribution of the observable M in the state S is given by the probability measure

$$\mu_S^M(B) = \mathrm{Tr}\, SM(B), \quad B \in \mathcal{B} \tag{11.47}$$

Note that the linear extension of the affine map $S \to \mu_S^M$ can be regarded as a generalization of the notion of a quantum-classical (q − c) channel (see Section 6.4).

Exercise 11.30 Prove that formula (11.47) defines a probability measure on $\mathcal{B}$.

Theorem 11.31. The channel Φ is entanglement-breaking if and only if there is a complete, separable metric space $\mathcal{X}$, a Borel $\mathfrak{S}(\mathcal{H}_B)$-valued function $S_B(x)$, and an observable M in $\mathcal{H}_A$ with values in $\mathcal{X}$ given by POVM $M(dx)$ such that

$$\Phi[S] = \int_{\mathcal{X}} S_B(x) \mu_S^M(dx) \tag{11.48}$$

Relation (11.48) is a continual version of representation (6.28), and to some extent the statement can be regarded as an infinite-dimensional generalization of Proposition 6.22, saying that an entanglement-breaking channel is a concatenation of a q − c channel (measurement of observable M) and a c-q channel (preparation of states $S_B(x)$ depending on the measurement outcome). In the infinite-dimensional case, the difference is that an observable with a nondiscrete set of outcomes cannot define a quantum channel in the sense of Definition 11.16. Indeed, in the finite-dimensional case, q − c channels are characterized by the property that all output states commute. Let Φ
be an infinite-dimensional channel with this property. This can then always be represented in the form (11.48), with a discrete set $\mathcal{X}$. There exists a basis $\{|k\rangle\}$ such that all commuting density operators $\Phi[S]$ are diagonal. Then

$$\Phi[S] = \sum_k |k\rangle\langle k|\Phi[S]|k\rangle\langle k| = \sum_k |k\rangle\langle k| \,\mathrm{Tr}\, SM_k,$$

where $M_k = \Phi^*[|k\rangle\langle k|]$ are the components of an observable with a discrete set of outcomes $\mathcal{X} = \{k\}$.

Sketch of the proof of Theorem 11.31. Let the channel have the form (11.48). Consider a state $\omega \in \mathfrak{S}(\mathcal{H}_A \otimes \mathcal{H}_R)$. Then

$$(\Phi \otimes \mathrm{Id}_R)(\omega) = \int_{\mathcal{X}} S_B(x) \otimes m_\omega(dx) \tag{11.49}$$

where

$$m_\omega(B) = \mathrm{Tr}_A\, \omega\left(M(B) \otimes I_R\right), \quad B \subseteq \mathcal{X}.$$

Any matrix element of the operator-valued measure m_ω (in a particular basis) is a complex-valued measure on $\mathcal{X}$, absolutely continuous with respect to the probability measure $\mu_\omega(B) = \mathrm{Tr}\, m_\omega(B), B \subseteq \mathcal{X}$. The Radon-Nikodym theorem implies the representation

$$m_\omega(B) = \int_B \sigma_\omega(x)\mu_\omega(dx)$$

where $\sigma_\omega(x)$ is a function on $\mathcal{X}$ that takes values in $\mathfrak{S}(\mathcal{H}_R)$. By using this representation, we can rewrite (11.49) as

$$(\Phi \otimes \mathrm{Id}_R)(\omega) = \int_{\mathcal{X}} S'(x) \otimes \sigma_\omega(x)\mu_\omega(dx) \tag{11.50}$$

which, by Proposition 11.27, is a separable state.
Conversely, let Φ be an entanglement-breaking channel. Fix a nondegenerate state σ_A in $\mathfrak{S}(\mathcal{H}_A)$ and let $\{|e_j\rangle, j = 1, \ldots\}$, be the basis of the eigenvectors of σ_A with corresponding (positive) eigenvalues $\{\lambda_j\}$. Consider the unit vector

$$|\Omega\rangle = \sum_{j=1}^{+\infty} \sqrt{\lambda_j}\, |e_j\rangle \otimes |e_j\rangle$$

in the space $\mathcal{H}_A \otimes \mathcal{H}_A$. Then $|\Omega\rangle\langle\Omega|$ is a purification of the state σ_A. Since Φ is entanglement-breaking, the state

$$\sigma_{AB} = (\mathrm{Id}_A \otimes \Phi)\left[|\Omega\rangle\langle\Omega|\right] \tag{11.51}$$

in $\mathfrak{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ is separable. By (11.43), there exists a probability measure π on $\mathfrak{S}(\mathcal{H}_A) \times \mathfrak{S}(\mathcal{H}_B)$ such that

$$\sigma_{AB} = \int_{\mathfrak{S}(\mathcal{H}_A)} \int_{\mathfrak{S}(\mathcal{H}_B)} S_A \otimes S_B \pi\left(dS_A dS_B\right). \tag{11.52}$$

This implies

$$\begin{aligned} \sigma_A &= \mathrm{Tr}_B\left(\mathrm{Id}_A \otimes \Phi\right)\left(|\Omega\rangle\langle\Omega|\right) \\ &= \int_{\mathfrak{S}(\mathcal{H}_A)} \int_{\mathfrak{S}(\mathcal{H}_B)} S_A \pi\left(dS_A dS_B\right) \\ &= \int_{\mathfrak{S}(\mathcal{H}_A)} \int_{\mathfrak{S}(\mathcal{H}_B)} \bar{S}_A \pi\left(dS_A dS_B\right), \end{aligned} \tag{11.53}$$

where the bar denotes complex conjugation in the basis $\{|e_i\rangle\}$. By this equality, for an arbitrary Borel set $B \subseteq \mathfrak{S}(\mathcal{H}_B)$, the operator

$$M(B) = \sigma_A^{-1/2} \left[\int_{\mathfrak{S}(\mathcal{H}_A)} \int_B \bar{S}_A \pi\left(dS_A dS_B\right)\right] \sigma_A^{-1/2} \tag{11.54}$$

can be correctly defined as a bounded positive operator on $\mathcal{H}_A$ such that $M(B) \leq M(\mathcal{X}) = I_A$. It is easy to check that M is an observable with values in $\mathcal{X} = \mathfrak{S}(\mathcal{H}_B)$.

Now, consider the entanglement-breaking channel

$$\hat{\Phi}(S) = \int_{\mathfrak{S}(\mathcal{H}_B)} S_B \mu_S^M (dS_B),$$

and let us show that $\Phi(S) = \hat{\Phi}(S)$. For this it is sufficient to prove that

$$\hat{\Phi}(|e_i\rangle\langle e_j|) = \Phi(|e_i\rangle\langle e_j|)$$

for all i, j. However,

$$\begin{aligned}\hat{\Phi}(|e_i\rangle\langle e_j|) &= \int_{\mathfrak{S}(\mathcal{H}_B)} S_B \langle e_j| M(dS_B) |e_i\rangle \\ &= \lambda_i^{-1/2}\lambda_j^{-1/2} \int_{\mathfrak{S}(\mathcal{H}_A)} \int_{\mathfrak{S}(\mathcal{H}_B)} \langle e_i| S_A |e_j\rangle S_B \pi(dS_A dS_B) \\ &= \lambda_i^{-1/2}\lambda_j^{-1/2} \operatorname{Tr}_A (|e_j\rangle\langle e_i| \otimes I_B)\sigma_{AB} = \Phi(|e_i\rangle\langle e_j|),\end{aligned}$$

where in the last equality relation (11.51) was used. □

As was shown in Section 8.3.3, in finite dimensions, entanglement-breaking channels form a large class, in which the additivity conjecture for the classical capacity holds. This fact can be generalized to the infinite-dimensional case.

Proposition 11.32. Let there be two channels Φ_1, Φ_2 with the corresponding input constraints F_1, F_2, satisfying the conditions of Corollary 11.24, and let Φ_1 be an entanglementbreaking channel. Then all additivity properties (8.36), (8.33), and (8.39) hold. In particular, the classical capacity of an entanglement-breaking channel Φ is equal to

$$C(\Phi, F, E) = C_\chi(\Phi, F, E)$$

The proof of this statement is obtained by generalizing the argument in the finitedimensional case (Proposition 8.19), with the replacement of sums with integrals and ensembles with generalized ensembles, taking into account that the conditions of Corollary 11.24 guarantee finiteness of all involved entropies.

10.11.8 11.8 Notes and References

1. The first attempt at a mathematically rigorous treatment of the basic notions of quantum mechanics in a separable Hilbert space was made in the classical treatise of von Neumann [237]. In particular, the difference between Hermitian (symmetric) and self-adjoint operators and the key role self-adjointness plays in the spectral decomposition were stressed, in contrast to the preceding works by physicists. The other important circle of ideas is related to the notions of trace and trace-class operators. A modern treatment of these concepts, in connection with applications in quantum theory, is given in the books [193], [56], and [122].

Lemma 11.1 is due to Dell'Antonio [58]; see also the Appendix to the book of Davies [56]. The compactness criterion for subsets of quantum states is a modification of a result of Sarymsakov [198], called by him the "noncommutative Prokhorov theorem." The latter provides a criterion for weak compactness of families of probability measures on a metric space; see [186]. It is used in Section 11.4.

2. It is well known that the topological properties of entropy in the infinite-dimensional case differ sharply from those in finite dimensions. In the last case, the entropy is a bounded, continuous function on $\mathfrak{S}(\mathcal{H})$, while in infinite dimensions it is discontinuous everywhere and

infinite "almost everywhere" in the sense that the set of states with finite entropy is a first-category subset of $\mathfrak{S}(\mathcal{H})$. See the survey of Wehrl [242], where a number of useful properties of the entropy, including Theorem 11.6 and Lemma 11.8, are discussed. For recent results concerning the topological properties of the entropy in infinite dimensions, see Shirokov [208].
3. The importance of considering input constraints for quantum channels was clear from the beginnings of quantum communication. For a detailed physical discussion of the problem of the determination of the capacity of an optical channel with constrained energy of the input signal, see the survey [43]. The present study of the classical capacity of a constrained c-q channel is based on the works [114] and [117], taking advantage of the random encoding (11.21), which is used in a similar classical problem.
4. Channels with a continuous alphabet were considered in the works of Holevo [117] and Holevo and Shirokov [130], where the notion of a generalized ensemble was systematically applied. Proofs of the used facts from the theory of probability measures on metric spaces, such as Exercise 11.12 and Lemma 11.13, can be found in the monograph of Parthasarathy [186].
5. For the proof of the boundedness of the map Φ in Exercise 11.17, see the book [56], Lemma 2.2.1. Our consideration of the χ-capacity of constrained quantum channels is based on the works [117] and [130]. A detailed investigation of the properties of the χ-capacity and other entropic characteristics of infinite-dimensional channels, without assuming finiteness of the output entropy, was made by Shirokov [210], [209].
6. This section is based on the results of the work [117]. In the paper of Shirokov and Holevo [131] one can find an extension of Proposition 11.25 to a natural degree of generality, free of any finiteness assumptions. In this paper, the question of coincidence of the classical entanglement-assisted and unassisted capacities was also studied. The energy-constrained quantum and private classical capacities of infinitedimensional channels were studied by Wilde and Qi [250], Davis, Shirokov and Wilde [57].
7. The concept of a quantum observable as POVM is presented in detail in the books [122], [115]. Theorem 11.31 is proved in the paper of Holevo, Shirokov, and Werner [132]. Concerning the proof of Proposition 11.32, see [121].

10.12 12 Gaussian Systems

The fundamental physical information carrier is electromagnetic waves, such as light or radio waves. Mathematically the radiation field is known to be equivalent to an ensemble of oscillators. In quantum optics one considers quantized fields and hence quantum oscillators. This is a typical "continuous-variable" bosonic quantum system, whose basic observables (oscillator amplitudes) satisfy the canonical commutation relations (CCRs). Many of the current experimental realizations of quantum information processing are carried out in such systems.

There is a class of particularly important states of bosonic systems which naturally correspond to classical multidimensional Gaussian distributions. From a physical viewpoint, this class comprises thermal equilibrium states of light as well as coherent and squeezed states produced by lasers and some "nonlinear" quantum optics devices. Mathematically, they are completely characterized by the mean and the covariance matrix, in a close parallel to the classical case. Restricting to a finite number of oscillator modes, which is an usual approximation in quantum optics, makes it possible to handle them with techniques from finite-dimensional linear algebra.

Our central problems will be unraveling the structure of quantum Gaussian channels and finding their capacities. Both problems appear rather involved mathematically and, up to now, have only been solved partially. Along with the established results, we give formulations of the basic conjectures, which, we hope, will stimulate attempts to their solutions.

A number of analytical complications related to infinite dimensionality and unboundedness of operators unavoidably arises in connection with bosonic systems and Gaussian states. In our treatment of CCRs we focus on the aspects essential for applications while a detailed presentation of related mathematical tools can be found in the literature. For the sake of convenience for nonspecialist readers, some mathematical and physical preliminaries, as well as motivation, are given in the introductory section.

10.12.1 12.1 Preliminary Material

10.12.2 12.1.1 Spectral Decomposition and Stone's Theorem

Let $\mathcal{H}$ be a separable Hilbert space and let $\{E(B); B \in \mathcal{B}(\mathbb{R})\}$ be a spectral measure on $\mathbb{R}$ where $\mathcal{B}(\mathbb{R})$ is the σ-algebra of Borel subsets. According to Definition 11.29, the spectral measure E defines a sharp real observable. As explained below, such observables are in one-to-one correspondence with self-adjoint operators in $\mathcal{H}$.

For the arbitrary unit vector $\psi \in \mathcal{H}$ the relation

$$\mu_\psi(B) = \langle\psi|E(B)|\psi\rangle$$

defines the Borel probability measure on $\mathbb{R}$. If $f(x)$ is a Borel measurable function on $\mathbb{R}$, then the integral

$$X_f = \int_{-\infty}^{\infty} f(x)E(dx) \tag{12.1}$$

converges strongly on the dense domain

$$\mathcal{D}\left(X_f\right) = \left\{\psi : \int_{-\infty}^{\infty} |f(x)|^2 \mu_\psi(dx) < \infty\right\}$$

and thus uniquely defines a linear operator on the domain $\mathcal{D}\left(X_f\right)$. (Strong convergence of operators $\{X_n\}$ to the operator X on the domain $\mathcal{D}$ means that $\lim_{n\to\infty} \|X_n\psi - X\psi\| = 0$ for $\psi \in \mathcal{D}$. In the case $\mathcal{D} = \mathcal{H}$ it is just the strong operator convergence.)

Indeed, if $f(x) = \sum_{i=1}^{\infty} f_i 1_{B_i}(x)$ is a countably-valued function (here $\{B_i\}$ is a measurable decomposition of $\mathbb{R}$), then

$$X_f = \sum_{i=1}^{\infty} f_i E\left(B_i\right),$$

and due to the orthogonality of the vectors $E\left(B_i\right)|\psi\rangle$,

$$\left\|X_f\psi\right\|^2 = \sum_{i=1}^{\infty} \left|f_i\right|^2 \langle\psi|E\left(B_i\right)|\psi\rangle = \sum_{i=1}^{\infty} \left|f_i\right|^2 \mu_\psi\left(B_i\right), \tag{12.2}$$

so that $\mathcal{D}\left(X_f\right)$ is just the set of all vectors $|\psi\rangle$ for which this series converges. This definition can be extended to an arbitrary Borel function $f(x)$, by approximating it uniformly with countably-valued functions and using (12.2). In particular, for the function $f(x) = x$ we obtain the operator

$$X = \int_{-\infty}^{\infty} xE(dx) \tag{12.3}$$

with the domain

$$\mathcal{D}(X) = \left\{ \psi : \int_{-\infty}^{\infty} |x|^2 \mu_\psi(dx) < \infty \right\},$$

for which

$$\langle \psi | X | \psi \rangle = \int_{-\infty}^{\infty} x \mu_\psi(dx), \quad \|X\psi\|^2 = \int_{-\infty}^{\infty} |x|^2 \mu_\psi(dx), \quad \psi \in \mathcal{D}(X) \tag{12.4}$$

The operators obtained in this way are self-adjoint in the following sense. For any densely defined operator X there is a unique adjoint X^* satisfying

$$\langle X^* \varphi \mid \psi \rangle = \langle \varphi \mid X\psi \rangle, \quad \psi \in \mathcal{D}(X), \varphi \in \mathcal{D}\left(X^*\right), \tag{12.5}$$

where $\mathcal{D}\left(X^*\right)$ is the (dense) subspace of all vectors φ such that the right-hand side is a bounded linear functional of ψ. The operator X is called Hermitian (symmetric) if

$$\langle X\varphi \mid \psi \rangle = \langle \varphi \mid X\psi \rangle, \tag{12.6}$$

for all $\varphi, \psi \in \mathcal{D}(X)$ and self-adjoint if $X = X^*$ in the sense that $\mathcal{D}\left(X^*\right) = \mathcal{D}(X)$ and (12.6) holds. Often one has to deal with essentially self-adjoint operators defined on some nonmaximal domain, which however extend uniquely to self-adjoint operators.

The spectral theorem (see, e. g., [193], Section VIII.3) says that for any self-adjoint operator X there exists a unique spectral measure E on $\mathbb{R}$ for which the relations (12.3), (12.4) hold. Thus, self-adjoint operators are those which have the spectral decomposition (12.3) over the real line. Such operators are naturally associated with (sharp) real observables in quantum mechanics. Then the measure μ_ψ gives the probability distribution of the observable X in the pure state $|\psi\rangle\langle\psi|$, and (12.4) gives the first and the second moments of this distribution.

In a certain sense which we will not comment here the relation $X_f = f(X)$ holds. By taking $f(x) = \exp(itx)$ in (12.1) we obtain the operators

$$V_t = \int_{-\infty}^{\infty} \exp(itx) E(dx) = \exp itX$$

Then the family $\{V_t; t \in \mathbb{R}\}$ is a strongly continuous group of unitary operators with the infinitesimal generator X, i.e.,

$$\lim_{t \to 0} (it)^{-1} \left(V_t - I\right) |\psi\rangle = X|\psi\rangle, \quad \psi \in \mathcal{D}(X) \tag{12.7}$$

Conversely, any strongly continuous group of unitary operators $\{V_t; t \in \mathbb{R}\}$ has the form $V_t = \exp itX$, where X is a uniquely defined self-adjoint operator. These statements are the content of Stone's theorem.

Exercise 12.1 1. Let $\mathcal{H} = L^2(\mathbb{R})$ be the Hilbert space of square integrable functions $\psi(\xi)$, $\xi \in \mathbb{R}$, and let $E = \{E(B); B \in \mathcal{B}(\mathbb{R})\}$ be defined by the expression

$$(E(B)\psi)(\xi) = 1_B(\xi)\psi(\xi), \quad \psi \in \mathcal{H}.$$

Prove that E is the spectral measure of the operator q of multiplication by ξ while V_t is the operator of multiplication by $\exp it\xi$, and in general X_f is the operator of multiplication by $f(\xi)$.

2. Consider the unitary operator in $\mathcal{H}$ defined by the Fourier transform

$$(\tilde{F}\psi)(\lambda) = \frac{1}{\sqrt{2\pi}} \int \exp(-i\lambda\xi)\psi(\xi) d\xi$$

Then $\tilde{E}(B) = \tilde{F}^* E(B)\tilde{F}$ is a spectral measure on $\mathbb{R}$, corresponding to the self-adjoint operator $p \equiv \tilde{q} = \frac{1}{i}\frac{d}{d\xi}$, which generates the group of unitary operators

$$(U_t\psi)(\xi) = \psi(\xi + t)$$

Self-adjoint operators $X_j, j = 1, \ldots, s$, commute if their spectral measures commute. The following is a multidimensional generalization of Stone's theorem.

Theorem 12.2. Let $V_x, x = [x_1, \ldots, x_s] \in \mathbb{R}^s$, be a strongly continuous group of unitary operators in a separable Hilbert space $\mathcal{H}$. Then there exists a family $X_j, j = 1, \ldots, s$, of commuting self-adjoint operators in $\mathcal{H}$ such that

$$V_x = \exp\left(i\sum_{j=1}^{s} x_j X_j\right). \tag{12.8}$$

Conversely, for any family $X_j, j = 1, \ldots, s$, of commuting self-adjoint operators in $\mathcal{H}$ the relation (12.8) defines strongly continuous unitary groups in $\mathcal{H}$.

10.12.3 12.1.2 Operators Associated with the Heisenberg Commutation Relation

In the Hilbert space $\mathcal{H} = L^2(\mathbb{R})$ we consider the operators

$$(q\psi)(\xi) = \xi\psi(\xi), \quad (p\psi)(\xi) = \frac{\hbar}{i}\frac{d}{d\xi}\psi(\xi),$$

defined on a common dense domain $\mathcal{D} \subseteq \mathcal{H}$. For example, $\mathcal{D}$ can be the subspace $\mathcal{S}(\mathbb{R})$ of infinitely differentiable rapidly decreasing functions, with all the derivatives tending to zero quicker than any degree of $|\xi|$ when $|\xi| \to \infty$. These operators are essentially self-adjoint, and hence they represent (sharp) real observables (see Section 12.1.1). Here $\hbar$ is a positive constant equal to Planck's constant in physical applications where it relates different systems of units (later we will choose the system in which $\hbar = 1$).

On this domain, q and p satisfy the Heisenberg commutation relation

$$[q, p] = i\hbar I. \tag{12.9}$$

For a unit vector ψ from the common domain of q, p consider a pure state $|\psi\rangle\langle\psi|$ and introduce the notation

$$x = \langle\psi|q|\psi\rangle, \quad y = \langle\psi|p|\psi\rangle,$$
$$\mathrm{D}_\psi(q) = \|(q - x)\psi\|^2, \quad \mathrm{D}_\psi(p) = \|(p - y)\psi\|^2$$

for the mean values and the variances of observables q, p. Then for any real ω

$$\begin{aligned}\omega^2\mathrm{D}_\psi(q) - \omega\hbar + \mathrm{D}_\psi(p) &= \omega^2\mathrm{D}_\psi(q) + i\omega\langle\psi|[q, p]|\psi\rangle + \mathrm{D}_\psi(p)\\ &= \|[\omega(q - x) + i(p - y)]\psi\|^2 \geq 0\end{aligned}$$

whence

$$\mathrm{D}_\psi(q)\mathrm{D}_\psi(p) \geq \frac{\hbar^2}{4}, \tag{12.10}$$

with equality attained if and only if there exists a positive ω such that

$$[\omega(q - x) + i(p - y)]\psi = 0.$$

This amounts to the differential equation

$$\left[\omega(\xi - x) + \left(\hbar\frac{d}{d\xi} - iy\right)\right]\psi(\xi) = 0, \tag{12.11}$$

the normalized solution of which, up to a constant factor of modulus one, is

$$\psi(\xi) = \sqrt[4]{\frac{\omega}{\pi\hbar}}\exp\left[\frac{iy}{\hbar}\left(\xi - \frac{x}{2}\right) - \frac{\omega(\xi - x)^2}{2\hbar}\right]. \tag{12.12}$$

Inequality (12.10) is the Heisenberg uncertainty relation and (12.12) are the minimal uncertainty state vectors with $\mathrm{D}_\psi(q) = \frac{\hbar}{2\omega}, \mathrm{D}_\psi(p) = \frac{\omega\hbar}{2}$.

By introducing the complex combinations

$$a = \frac{1}{\sqrt{2\hbar\omega}}(\omega q + ip), \quad \zeta = \frac{1}{\sqrt{2\hbar\omega}}(\omega x + iy)$$

and denoting the corresponding state vector (12.12) by $|\zeta\rangle$, we can rewrite the defining equation (12.11) as

$$a|\zeta\rangle = \zeta|\zeta\rangle, \quad \zeta \in \mathbb{C}. \tag{12.13}$$

In particular,

$$a|0\rangle = 0, \tag{12.14}$$

where $|0\rangle$ is the vector described by the function

$$\psi(\xi) = \sqrt[4]{\frac{\omega}{\pi\hbar}}\exp\left[-\frac{\omega\xi^2}{2\hbar}\right].$$

Operator $a = \frac{1}{\sqrt{2\hbar\omega}}(\omega q + ip)$ has the adjoint $a^\dagger = \frac{1}{\sqrt{2\hbar\omega}}(\omega q - ip)$. The commutation relation (12.9) can be rewritten as

$$\left[a, a^\dagger\right] = I. \tag{12.15}$$

Consider the operator

$$\mathcal{N} = a^\dagger a = aa^\dagger - I, \tag{12.16}$$

which is essentially self-adjoint. By (12.14) it satisfies

$$\mathcal{N}|0\rangle = 0.$$

Exercise 12.3 Applying successively the relation (12.16), show that the vectors

$$|n\rangle = \frac{\left(a^\dagger\right)^n}{\sqrt{n!}}|0\rangle \tag{12.17}$$

form an orthonormal system of eigenvectors of the operator $\mathcal{N}$, i. e.,

$$\mathcal{N}|n\rangle = n|n\rangle, \quad n = 0, 1, \ldots$$

The corresponding functions in $L^2(\mathbb{R})$ up to normalizing factors are

$$\left[\omega\xi - \hbar\frac{d}{d\xi}\right]^n \exp\left[-\frac{\omega\xi^2}{2\hbar}\right] \simeq H_n\left(\sqrt{\frac{\omega}{\hbar}}\xi\right)\exp\left[-\frac{\omega\xi^2}{2\hbar}\right],$$

where $H_n(\cdot), n = 0, 1, \ldots$, are the Hermite polynomials which form a complete orthogonal system in $L^2(\mathbb{R})$. Hence $\{|n\rangle; n = 0, 1, \ldots\}$ is an orthonormal basis in $\mathcal{H}$,

$$\sum_{n=0}^{\infty} |n\rangle\langle n| = I$$

and $\mathcal{N}$ has the spectral decomposition

$$\mathcal{N} = \sum_{n=0}^{\infty} n|n\rangle\langle n|. \tag{12.18}$$

Exercise 12.4 Operator $\mathcal{N}$ is self-adjoint of the type $\mathfrak{F}$ (Definition 11.3) with the domain

$$\mathcal{D}(\mathcal{N}) = \left\{ \psi : \sum_{n=0}^{\infty} n^2 |\langle n \mid \psi\rangle|^2 < \infty \right\}$$

and (12.18) holds in the sense of strong convergence on $\mathcal{D}(\mathcal{N})$.
Further, the relations

$$a|n\rangle = \sqrt{n}|n-1\rangle, \quad a^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle$$

hold. By introducing the group of unitary operators $\left\{e^{i\mathcal{N}\omega t}; t \in \mathbb{R}\right\}$, one has

$$e^{i\mathcal{N}\omega t} a e^{-i\mathcal{N}\omega t} = a e^{-i\omega t}, \quad e^{i\mathcal{N}\omega t} a^\dagger e^{-i\mathcal{N}\omega t} = a^\dagger e^{i\omega t}. \tag{12.19}$$

Coming back to the operators q, p, one sees that

$$\hbar\omega \left(a^\dagger a + \frac{I}{2} \right) = \frac{1}{2} \left(\omega^2 q^2 + p^2 \right) \equiv \hbar H \tag{12.20}$$

is the energy operator for the quantum harmonic oscillator with frequency ω. Then $\mathcal{N} = a^\dagger a$ is the number (of quanta) operator, $|n\rangle$ are the number state vectors, $|0\rangle$ is the vacuum state vector, and a (resp. $a^\dagger$) is the annihilation (resp. creation) operator. In quantum optics the operators $a, a^\dagger$ describe a mode of electromagnetic field corresponding to a definite frequency (and a definite polarization).

10.12.4 12.1.3 Classical Signal Plus Quantum Noise

The states $|\zeta\rangle\langle\zeta|, \zeta \in \mathbb{C}$, are called coherent. From (12.17), (12.13) we obtain

$$\langle n \mid \zeta\rangle = \frac{1}{\sqrt{n!}} \langle 0 \mid a^n \zeta\rangle = \frac{\zeta^n}{\sqrt{n!}} \langle 0 \mid \zeta\rangle = \frac{\zeta^n}{\sqrt{n!}} \exp\left(-\frac{|\zeta|^2}{2} \right),$$

where we also used the formula

$$\langle \zeta_1 \mid \zeta_2\rangle = \exp\left[-\frac{1}{2} \left(|\zeta_1|^2 + |\zeta_2|^2 - 2\bar{\zeta}_1 \zeta_2 \right) \right]. \tag{12.21}$$

Exercise 12.5 Prove (12.21) by using the real parametrization (12.12) of the vectors $|\zeta\rangle$.
Exercise 12.6 The system of vectors $\{|\zeta\rangle; \zeta \in \mathbb{C}\}$ is overcomplete in the sense

$$\frac{1}{\pi} \int |\zeta\rangle\langle\zeta| d^2\zeta = I$$

where $d^2\zeta = \frac{1}{2\hbar} dxdy$. Hint: the matrix elements of the integral in the basis $\{|n\rangle\}$ have the form

$$\frac{1}{\pi}\int \frac{\zeta^n}{\sqrt{n!}}\frac{\bar{\zeta}^m}{\sqrt{m!}}\exp\left(-|\zeta|^2\right)d^2\zeta = \delta_{nm}.$$

Let $p(\zeta)$ be a probability density on $\mathbb{C}$. Then

$$S = \int |\zeta\rangle\langle\zeta| p(\zeta) d^2\zeta \tag{12.22}$$

is a density operator of a state called (quasi-)classical in quantum optics. In particular, taking the complex Gaussian density with zero mean and the variance $N > 0$ we obtain the density operator

$$S_0 = \frac{1}{\pi N}\int |\zeta\rangle\langle\zeta| \exp\left(-\frac{|\zeta|^2}{N}\right) d^2\zeta \tag{12.23}$$

with the matrix elements

$$\langle n|S_0|m\rangle = \frac{1}{\pi N}\int \frac{\zeta^n}{\sqrt{n!}}\frac{\bar{\zeta}^m}{\sqrt{m!}}\exp\left(-\frac{(N+1)|\zeta|^2}{N}\right) d^2\zeta = \delta_{nm}\frac{1}{N+1}\left(\frac{N}{N+1}\right)^n.$$

Therefore the operator S_0 has the spectral decomposition

$$S_0 = \frac{1}{N+1}\sum_{n=0}^{\infty}\left(\frac{N}{N+1}\right)^n |n\rangle\langle n|. \tag{12.24}$$

This relation makes sense also for $N = 0$ when $S_0 = |0\rangle\langle 0|$ is defined by the Gaussian distribution degenerate at the point $\zeta = 0$.

Taking into account the spectral decomposition (12.18) and the relation (12.20), this can be written as

$$S_0 = \frac{\exp[-\theta H]}{\operatorname{Tr}\exp[-\theta H]}, \tag{12.25}$$

which is the Gibbs equilibrium (thermal) state of the quantum harmonic oscillator at the inverse temperature $\theta/\hbar = \frac{1}{\hbar\omega}\ln\frac{N+1}{N}$. The parameter $N = \operatorname{Tr} S_0 a^\dagger a$ is interpreted as the mean number of the oscillator energy quanta. The von Neumann entropy of the state (12.24)

$$H(S_0) = \frac{1}{N+1}\sum_{n=0}^{\infty}\left(\frac{N}{N+1}\right)^n [(n+1)\log(N+1) - n\log N] = g(N), \tag{12.26}$$

where we introduced the Gordon function

$$\begin{aligned} &g(x) = (x+1)\log(x+1) - x\log x, \quad x > 0, \\ &g(0) = 0. \end{aligned} \tag{12.27}$$

Another important density operator is obtained from the shifted probability density

$$S_\mu = \frac{1}{\pi N}\int |\zeta\rangle\langle\zeta| \exp\left(-\frac{|\zeta-\mu|^2}{N}\right) d^2\zeta, \tag{12.28}$$

where $\mu = \frac{1}{\sqrt{2\hbar\omega}}(\omega m_q + i m_p)$. Introducing the unitary operators

$$D(\zeta)\psi(\xi) = \exp\left[\frac{iy}{\hbar}\left(\xi - \frac{x}{2}\right)\right]\psi(\xi - x) \tag{12.29}$$

we see that

$$|\zeta\rangle = D(\zeta)|0\rangle$$
$$D\left(\zeta_2\right)|\zeta_1\rangle = \exp\left(i\,\mathrm{Im}\,\bar{\zeta}_1\zeta_2\right)|\zeta_1+\zeta_2\rangle$$

that is, the action of this operator is to make a displacement in mean values of q, p. Physically such a displacement is realized by action of an external source, such as an idealized laser producing coherent state $|\zeta\rangle\langle\zeta|$ from the vacuum state $|0\rangle\langle 0|$. The quasi-classical state (12.22) is a chaotic mixture of coherent states, while

$$S_\mu = D(\mu)S_0D(\mu)^* \tag{12.30}$$

represents transformation of the equilibrium state under the action of an external source characterized by complex amplitude μ. Note that the state S_μ is pure if and only if $N = 0$, in which case it coincides with the coherent state $|\mu\rangle\langle\mu|$. In information theoretic applications μ is the classical signal to be transmitted via the noisy quantum mode q, p. The state S_μ is thus a model for a classical signal plus quantum Gaussian noise (see the next section).

Exercise 12.7 Prove that the displacement operators satisfy the commutation relation

$$D\left(\zeta_2\right)D\left(\zeta_1\right) = \exp\left(i\,\mathrm{Im}\,\bar{\zeta}_1\zeta_2\right)D\left(\zeta_1+\zeta_2\right), \tag{12.31}$$

which implies

$$D(\mu)^*D(\zeta)D(\mu) = \exp(2i\,\mathrm{Im}\,\bar{\mu}\zeta)D(\zeta). \tag{12.32}$$

In what follows we need the noncommutative analog of the characteristic function for the state S_μ, i.e.,

$$\mathrm{Tr}\,S_\mu D(\zeta) = \exp\left[2i\,\mathrm{Im}\,\bar{\mu}\zeta - \left(N+\frac{1}{2}\right)|\zeta|^2\right]. \tag{12.33}$$

Proof of formula (12.33). By (12.30), (12.32) we have

$$\mathrm{Tr}\,S_\mu D(\zeta) = \exp\Big(2i\widetilde{J}\widetilde{\mu}\zeta\Big)\,\mathrm{Tr}\,S_0D(\zeta)$$

and it is sufficient to prove (12.33) for $\mu = 0$. Then

$$\begin{aligned}\mathrm{Tr}\,S_0D(\zeta) &= \int\langle\zeta_1|\,D(\zeta)\,|\zeta_1\rangle\,\frac{1}{\pi N}\exp\left(-\frac{|\zeta_1|^2}{N}\right)d^2\zeta_1 \\ &= \int\langle 0|D\left(\zeta_1\right)^*D(\zeta)D\left(\zeta_1\right)|0\rangle\frac{1}{\pi N}\exp\left(-\frac{|\zeta_1|^2}{N}\right)d^2\zeta_1 \\ &= \int\exp\left(2i\,\mathrm{Im}\,\bar{\zeta}_1\zeta\right)\langle 0|D(\zeta)|0\rangle\frac{1}{\pi N}\exp\left(-\frac{|\zeta_1|^2}{N}\right)d^2\zeta_1\end{aligned} \tag{12.34}$$

By using (12.21) we obtain

$$\langle 0|D(\zeta)|0\rangle = \langle 0\mid\zeta\rangle = \exp\left(-\frac{1}{2}|\zeta|^2\right).$$

Substituting this expression into (12.34) and using the expression for the characteristic function of Gaussian probability distribution, we obtain

$$\operatorname{Tr} S_0 D(\zeta) = \exp\left(-\left(N+\frac{1}{2}\right)|\zeta|^2\right).$$

□

10.12.5 12.1.4 The Classical-Quantum Gaussian Channel

The mapping $\mu \to S_\mu$ can be considered as a classical-quantum (c-q) channel in the sense of Section 11.4 realizing transmission of the classical signal $\mu \in \mathbb{C}$ with the additive quantum Gaussian noise of the power N. For the first two moments we have

$$\operatorname{Tr}_\mu a = \mu, \quad \operatorname{Tr}_\mu a^\dagger a = N + |\mu|^2 \tag{12.35}$$

To compute its classical capacity we can use the general approach of Section 11.4.

Assuming that the words $w = (\mu_1, \ldots, \mu_n)$ are transmitted by independent uses of this channel (memoryless channel), we impose the additive energy constraint on the signal μ of the type (11.16), i. e.,

$$|\mu_1|^2 + \cdots + |\mu_n|^2 \leq nE \tag{12.36}$$

which corresponds to the constraint function $f(\mu) = |\mu|^2$. Then the conditions of Theorem 11.15 are fulfilled with the choice $F = a^\dagger a \equiv \mathcal{N}$, and the classical capacity of the channel $\mu \to S_\mu$ with the energy input constraint (12.36) is equal to

$$C = \max_{\pi \in \mathcal{P}_E} \left[H\left(\bar{S}_\pi\right) - \int H\left(S_\mu\right) \pi\left(d^2\mu\right) \right] \tag{12.37}$$

where $\mathcal{P}_E$ is the set of the input distributions $\pi\left(d^2\mu\right)$ satisfying

$$\int |\mu|^2 \pi\left(d^2\mu\right) \leq E \tag{12.38}$$

and

$$\bar{S}_\pi = \int S_\mu \pi\left(d^2\mu\right)$$

is the average state.

Note that the states S_μ are unitarily equivalent by (12.30) and hence have the same entropy $H\left(S_\mu\right) = H\left(S_0\right) = g(N)$; see (12.26). Therefore for any input distribution $\pi\left(d^2\mu\right)$ the χ-quantity (11.24) is equal to

$$\chi(\pi) = H\left(\bar{S}_\pi\right) - H\left(S_0\right)$$

and the problem reduces to maximization of the entropy $H\left(\bar{S}_\pi\right)$ under the constraint (12.38). Due to (12.35), relation (12.38) implies

$$\operatorname{Tr} \bar{S}_\pi a^\dagger a \leq N + E \tag{12.39}$$

This is a restriction onto second moments of the state $\bar{S}_\pi$; according to the maximal entropy principle (see Lemma 12.26), the maximal value of the entropy

$$H\left(\bar{S}_\pi\right) = g(N+E) \tag{12.40}$$

is attained by the Gaussian density operator

$$\bar{S}_\pi = \frac{1}{N+E+1} \sum_{n=0}^{\infty} \left(\frac{N+E}{N+E+1} \right)^n |n\rangle\langle n|, \tag{12.41}$$

which turns (12.39) into equality. It corresponds to the optimal distribution

$$\pi\left(d^2\mu\right) = \frac{1}{\pi E} \exp\left(-\frac{|\mu|^2}{E} \right) d^2\mu \tag{12.42}$$

Finally, the capacity of the memoryless c-q Gaussian channel is given by the expression

$$\begin{aligned} C = C_\chi &= g(N+E) - g(N) \\ &= \log\left(1 + \frac{E}{N+1}\right) + (N+E)\log\left(1 + \frac{1}{N+E}\right) - N\log\left(1 + \frac{1}{N}\right) \end{aligned} \tag{12.43}$$

which behaves as $\log\left(1+\frac{E}{N+1}\right)$ asymptotically in the classical limit $N \to \infty, E/N \to \text{const}$. Thus the relation (12.43) can be regarded as quantum generalization of Shannon's formula (4.51) with Gaussian white noise of power N. The factor $1/2$ is absent in (12.43) because one oscillator mode amounts to the two independent identically distributed real amplitudes m_q, m_p.

In what follows we will develop a general theory of quantum Gaussian channels and their capacities.

10.12.6 12.2 Canonical Commutation Relations

10.12.7 12.2.1 Weyl-Segal Canonical Commutation Relation

In quantum mechanics the CCRs arise in quantization of a mechanical system with finite number of degrees of freedom or a classical field represented as an infinite collection of oscillators. In quantum optics one usually deals only with a finite number of relevant oscillator frequencies, thus again reducing to the case of mechanical system with a finite number s of degrees of freedom.

Consider the Hilbert space $\mathcal{H} = L^2\left(\mathbb{R}^S\right)$ of complex square integrable functions of the real variables $\xi_j, j = 1, \ldots, s$, where $\mathbb{R}^s$ is the coordinate space of the underlying classical system. In the space $\mathcal{H}$ we consider the two groups of unitary operators (cf. Exercise 12.1)

$$V_x\psi(\xi) = \exp\left(i\xi^\top x\right)\psi(\xi), \quad U_y\psi(\xi) = \psi(\xi+y) \tag{12.44}$$

where $\xi, x, y \in \mathbb{R}^s$ are understood as column vectors and $^\top$ denotes transposition. These groups satisfy the Weyl CCR

$$U_y V_x = \exp\left(iy^\top x\right) V_x U_y \tag{12.45}$$

Note analogy with the discrete groups arising from (6.51). The groups U_y, V_x describe the change of a quantum state under the displacements in position (resp. momentum) space, and the Weyl CCR is an expression for the kinematics of a nonrelativistic quantum mechanical system, which in fact can be derived from the Galilei covariance; see, e.g., [122].

Computing the generators of the groups V_x, U_y by a multidimensional analog of formula (12.7), we obtain a particular instance of Stone's theorem, Theorem 12.2, i. e.,

$$V_x = \exp\left(i\sum_{j=1}^{s} x_j q_j \right), \quad U_y = \exp\left(i\sum_{j=1}^{s} y_j p_j \right),$$

where $x = [x_1 \dots x_s]^\top, y = [y_1 \dots y_s]^\top$, and the self-adjoint operators

$$q_j = \xi_j, \quad p_j = \frac{1}{i}\frac{\partial}{\partial \xi_j}$$

are the canonical observables satisfying the Heisenberg CCRs

$$[q_j, p_k] = i\delta_{jk} I, \quad [q_j, q_k] = 0, \quad [p_j, p_k] = 0 \tag{12.46}$$

Here and in what follows we choose the units in which $\hbar = 1$. The operators q_j, p_j are unbounded, hence the relations (12.46) should be considered only on a common dense domain, such as the subspace $\mathcal{S}(\mathbb{R})$ of infinitely differentiable rapidly decreasing functions.

To make use of apparent symmetry between x, y, we introduce the $2s$-vector $z = [x_1, y_1, \dots, x_s, y_s]^\top$ and the unitary Weyl operators

$$W(z) = \exp\left(\frac{i}{2} y^\top x\right) V_x U_y \tag{12.47}$$

From (12.47) and (12.45) it follows that the operators $W(z)$ satisfy the Weyl-Segal CCR

$$W(z)W(z') = \exp\left[-\frac{i}{2}\Delta(z, z')\right] W(z + z') \tag{12.48}$$

where

$$\Delta(z, z') = \sum_{j=1}^{s} \left(x_j y'_j - x'_j y_j\right) = z^\top \Delta z' \tag{12.49}$$

is the canonical symplectic form. Here we denote by the same letter Δ the matrix of the form

$$\Delta = \begin{bmatrix} 0 & 1 & & & \\ -1 & 0 & & & \\ & & \ddots & & \\ & & & 0 & 1 \\ & & & -1 & 0 \end{bmatrix} \equiv \operatorname{diag}\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \tag{12.50}$$

From (12.48) and unitarity of the operators $W(z)$ it follows that $W(-z) = W(z)^*$. The relation (12.48) implies

$$W(z')^* W(z) W(z') = \exp\left[-i\Delta(z, z')\right] W(z). \tag{12.51}$$

Similarity between the commutation relations (12.31) and (12.48) is not accidental: in fact the operators $W(-\Delta^{-1} z)$ are the multimode generalization of the unitary displacement operators.

Exercise 12.8 Show that in the case of one degree of freedom

$$D(\mu) = W(m_p/\hbar, -m_q/\hbar), \tag{12.52}$$

where $\mu = \frac{1}{\sqrt{2\hbar\omega}}(\omega m_q + i m_p)$, so that

$$D(\mu)^* W(z) D(\mu) = \exp i\left(m_q x + m_p y\right) W(z). \tag{12.53}$$

Since $\Delta(z, z) \equiv 0$, the relation (12.48) implies that for any fixed z the one-parameter family $\{W(tz); t \in \mathbf{R}\}$ is a unitary group. The generator of this group computed according to formula (12.7) is the self-adjoint operator

$$Rz = \sum_{j=1}^{s} (x_j q_j + y_j p_j)$$

where

$$R = \left[\begin{array}{cccccc} q_1 & p_1 & \dots & q_s & p_s \end{array} \right]$$

is the row vector of the canonical observables. According to Stone's theorem,

$$W(z) = \exp iRz \tag{12.54}$$

Exercise 12.9 Use (12.51) to prove the relation

$$W\left(-\Delta^{-1}z\right)^* RW\left(-\Delta^{-1}z\right) = R + z^\top I \tag{12.55}$$

Exercise 12.10 Show that the Heisenberg commutation relations (12.46) can be written in the form

$$[Rz, Rz'] = i\Delta(z, z')\, I \tag{12.56}$$

10.12.8 12.2.2 The Symplectic Space

The space $Z = \mathbb{R}^{2s}$ equipped with the nondegenerate skew-symmetric form $\Delta(z, z')$ defined in (12.49) is a symplectic vector space. [1] It represents the phase space of the

classical system, the quantum version of which is described by the family of unitary operators $W(z)$ in the Hilbert space $\mathcal{H}$. This quantization is essentially unique: any irreducible family of unitary operators $W(z)$ in a Hilbert space satisfying the Weyl-Segal CCR is unitarily equivalent to the representation in $L^2(\mathbb{R}^s)$ described above, which is called the Schrödinger representation (Stone-von Neumann's uniqueness theorem; see, e. g., [193], [122]). In what follows $W(z), z \in Z$, can be any irreducible representation of the CCR.

A basis $\{e_j, h_j; j = 1, \dots, s\}$ in Z is called symplectic if

$$\Delta(e_j, h_k) = \delta_{jk}, \quad \Delta(e_j, e_k) = \Delta(h_j, h_k) = 0, \quad j, k = 1, \dots, s. \tag{12.57}$$

In any such basis the symplectic form $\Delta(z, z')$ has the standard expression (12.49). The transition matrix T from the initial symplectic basis in Z to the new symplectic basis is a matrix of symplectic transformation in (Z, Δ), which is characterized by the property

$$\Delta(Tz, Tz') = \Delta(z, z'), \quad z, z' \in Z.$$

Operator J in (Z, Δ) is called operator of complex structure if

$$J^2 = -I, \tag{12.58}$$

where I is the identity operator in Z, and it is Δ-positive in the sense that the bilinear form

$$j(z, z') = \Delta(z, Jz') \tag{12.59}$$

is an inner product in Z. Note that Δ-positivity is equivalent to the conditions

$$\Delta J = -J^\top \Delta, \quad \Delta J \geq 0. \tag{12.60}$$

[1] 1 Most of the content of this chapter can be adapted to the case of an abstract symplectic vector space equipped with an arbitrary nondegenerate skew-symmetric form.

Exercise 12.11 Operator / defines the structure of complex unitary space in Z (of dimensionality s) in which $iz = Jz$ and the inner product is

$$\frac{1}{2}\left[j\left(z,z'\right)+i\Delta\left(z,z'\right)\right]=\frac{1}{2}\left[\Delta\left(z,Jz'\right)+i\Delta\left(z,z'\right)\right]. \tag{12.61}$$

This structure will be studied in detail later in this Chapter.
In what follows we will consider various bilinear forms $\alpha,\ldots$ in the space $Z=\mathbb{R}^{2s}$, and the matrices of such forms will be denoted by the same letters, e. g., $\alpha\left(z,z'\right)=z^{\top}\alpha z'$, etc.

Lemma 12.12. Let $\alpha\left(z,z'\right)=z^{\top}\alpha z'$ be an inner product in the symplectic space (Z,Δ). Then there is a symplectic basis $\{e_j,h_j;j=1,\ldots,s\}$ in Z such that the form α is diagonal with the matrix

$$\tilde{\alpha}=\operatorname{diag}\left[\begin{array}{cc}\alpha_j & 0\\ 0 & \alpha_j\end{array}\right] \tag{12.62}$$

where $\alpha_j>0$.

Proof. Consider the operator $A=\Delta^{-1}\alpha$ satisfying

$$\alpha\left(z,z'\right)=\Delta\left(z,Az'\right)$$

The operator A is skew-symmetric in the Euclidean space (Z,α) : $A^{*}=-A$. According to a theorem from linear algebra, there is an orthogonal basis $\{e_j,h_j\}$ in (Z,α) and positive numbers $\{\alpha_j\}$ such that

$$Ae_j=\alpha_j h_j,\quad Ah_j=-\alpha_j e_j$$

Choosing the normalization $\alpha\left(e_j,e_j\right)=\alpha\left(h_j,h_j\right)=\alpha_j$ gives the symplectic basis in (Z,Δ) with the required properties.

For an arbitrary inner product α in Z there is at least one operator of complex structure J, commuting with the operator $A=\Delta^{-1}\alpha$, namely, the orthogonal operator J from the polar decomposition

$$A=|A|J=J|A| \tag{12.63}$$

in the Euclidean space (Z,α). Applying Lemma 12.12, we obtain that there is a symplectic basis $\{e_j,h_j;j=1,\ldots,s\}$ in which the form α is diagonal with the matrix (12.62) while J has the matrix

$$\tilde{J}=\operatorname{diag}\left[\begin{array}{cc}0 & -1\\ 1 & 0\end{array}\right], \tag{12.64}$$

so that

$$Je_j=h_j,\quad Jh_j=-e_j \tag{12.65}$$

Denoting by T the transition matrix from the initial symplectic basis in Z to the new symplectic basis, i. e., the matrix with the columns $\{e_j,h_j;j=1,\ldots,s\}$, we have

$$\Delta=T^{\top}\Delta T,\quad \tilde{\alpha}=T^{\top}\alpha T,\quad \tilde{J}=T^{-1}JT.$$

The canonical observables in the new basis are given by the relations

$$\tilde{q}_j=Re_j,\quad \tilde{p}_j=Rh_j,\quad j=1,\ldots,s, \tag{12.66}$$

so that $RT=\tilde{R}$, where $\tilde{R}=[\tilde{q}_1\tilde{p}_1\ldots\tilde{q}_s\tilde{p}_s]$.

10.12.9 12.2.3 Dynamics, Quadratic Operators, and Gauge Transformations

For any symplectic transformation T in Z there is a unitary operator U_T in $\mathcal{H}$ such that

$$U_T^* W(z) U_T = W(Tz) \tag{12.67}$$

This follows from the Stone-von Neumann uniqueness theorem because the operators $W(Tz), z \in Z$, again form an (irreducible) representation of the CCR (12.48) in $\mathcal{H}$. In view of relation (12.54) this is equivalently expressed in terms of canonical observables

$$U_T^* R U_T = RT \tag{12.68}$$

Let us consider one-parameter semigroup of symplectic transformations in Z

$$T_t = \mathrm{e}^{tD}, \quad t \in \mathbb{R}$$

describing linear dynamics in the classical phase space. We assume that the generator D is Δ-positive, i. e., $\Delta(z, Dz')$ is an inner product in Z. In matrix notations

$$\Delta D = -D^\top \Delta \geq 0 \tag{12.69}$$

Quantization of the linear dynamics T_t is given by the following theorem.
Theorem 12.13. Consider the operator $H = R\epsilon R^\top$ in $\mathcal{H}$ which is quadratic in the canonical variables R, where

$$\epsilon = -\frac{1}{2} D\Delta^{-1} \tag{12.70}$$

Then H is a positive self-adjoint operator in $\mathcal{H}$ generating the unitary group $\left\{\mathrm{e}^{itH}\right\}$ such that

$$W(T_t z) = \mathrm{e}^{itH} W(z) \mathrm{e}^{-itH} \tag{12.71}$$

Proof (sketch). In terms of generators of the Weyl unitaries, the relation (12.71) we wish to establish is equivalent to

$$R\mathrm{e}^{tD} = \mathrm{e}^{itR\epsilon R^\top} R \mathrm{e}^{-itR\epsilon R^\top} \tag{12.72}$$

with $D = -2\epsilon\Delta$.
Consider the bilinear form

$$\frac{1}{2}\Delta(z, Dz') = -z^\top \Delta\epsilon\Delta z'$$

which is an inner product by our assumption on the operator D. According to Lemma 12.12 there is a symplectic basis $\{e_j, h_j\}$ such that the matrix of this form is diagonal, i. e.,

$$-\Delta\tilde{\epsilon}\Delta = \mathrm{diag} \begin{bmatrix} \omega_j/2 & 0 \\ 0 & \omega_j/2 \end{bmatrix}$$

where $\omega_j > 0$, hence

$$\tilde{\epsilon} = \mathrm{diag} \begin{bmatrix} \omega_j/2 & 0 \\ 0 & \omega_j/2 \end{bmatrix}$$

By introducing the new canonical observables $\tilde{q}_j = Re_j, \tilde{p}_j = Rh_j, j = 1, \ldots, s$, we have

$$H = \sum_{j=1}^{s} \frac{\omega_j}{2} \left(\tilde{q}_j^2 + \tilde{p}_j^2 \right), \tag{12.73}$$

implying that H is a positive self-adjoint operator as a sum of operators of the type (12.20) referring to different modes. It is called the energy operator or Hamiltonian of the oscillator system. In terms of the creation-annihilation operators

$$\tilde{a}_j^\dagger = \frac{1}{\sqrt{2}} \left(\tilde{q}_j - i\tilde{p}_j \right), \quad \tilde{a}_j = \frac{1}{\sqrt{2}} \left(\tilde{q}_j + i\tilde{p}_j \right),$$

the energy operator is

$$H = \sum_{j=1}^{s} \omega_j \left(\tilde{a}_j^\dagger \tilde{a}_j + I/2 \right) \tag{12.74}$$

In the new basis $\{e_j, h_j\}$ the matrix of operator $D = -2\epsilon\Delta$ has the form

$$\tilde{D} = \operatorname{diag} \left[\begin{array}{cc} 0 & -\omega_j \\ \omega_j & 0 \end{array} \right] = \tilde{J} \left[\begin{array}{cc} \omega_j & 0 \\ 0 & \omega_j \end{array} \right]$$

where the last expression is just the polar decomposition of $\tilde{D}$, so that the complex structure $J = T\tilde{J}T^{-1}$ arises from the similar decomposition

$$D = J|D| = |D|J. \tag{12.75}$$

Consider formula (12.72), which we wish to establish in the new basis. Taking into account that the right action of J on R is equivalent to multiplication of the annihilation operators by $-i$, this formula reduces just to the equations of the type (12.19), i.e.,

$$\tilde{a}_j \mathrm{e}^{-i\omega_j t} = \mathrm{e}^{i\omega_j t \tilde{a}_j^\dagger \tilde{a}_j} \tilde{a}_j \mathrm{e}^{-i\omega_j t \tilde{a}_j^\dagger \tilde{a}_j}, \quad j = 1, \ldots, S \tag{12.76}$$

describing dynamics of quantum harmonic oscillators with frequencies ω_j.
The components of the quantum system described by the operators $\tilde{a}_j, \tilde{a}_j^\dagger$ or $\tilde{q}_j, \tilde{p}_j$, corresponding to the frequencies ω_j, are called normal modes and the approach based on the representation of the energy matrix ϵ in the diagonal form is just the normal mode decomposition.

With an operator of complex structure J we can associate the cyclic one-parameter group $\left\{ \mathrm{e}^{\varphi J}; \varphi \in [0, 2\pi] \right\}$ of symplectic transformations which we call the gauge group. According to the Theorem 12.13 above (with $D = J$), the gauge group in Z induces the unitary group of the gauge transformations $\{U_\varphi\}$ in $\mathcal{H}$ by the formula

$$W\left(\mathrm{e}^{\varphi J} z \right) = U_\varphi^* W(z) U_\varphi \tag{12.77}$$

where $U_\varphi = \mathrm{e}^{-i\varphi G}$, and $G = -\frac{1}{2} R J \Delta^{-1} R^\top$ is a positive self-adjoint operator in $\mathcal{H}$. In terms of generators, (12.77) reduces to the canonical transformation

$$R\mathrm{e}^{\varphi J} = \mathrm{e}^{i\varphi G} R \mathrm{e}^{-i\varphi G} \tag{12.78}$$

which is a particular case of (12.72).

Applying the previous argument to the case $D = J$ and using (12.58), (12.65), we obtain that there exists a symplectic basis $\{e_j, h_j; j = 1, \ldots, s\}$ such that $Je_j = h_j, Jh_j = -e_j$, in which

$$G = \sum_{j=1}^{s} \frac{1}{2} \left(\tilde{q}_j^2 + \tilde{p}_j^2 \right) = \mathcal{N} + \frac{s}{2} I \tag{12.79}$$

where

$$\mathcal{N} = \sum_{j=1}^{s} \tilde{a}_j^\dagger \tilde{a}_j$$

is the total number operator.
An operator X in $\mathcal{H}$ is called gauge invariant if

$$U_\varphi^* X U_\varphi = X$$

for all $\varphi \in [0, 2\pi]$. By using (12.78) and (12.60) we find that a quadratic operator $X = R\epsilon R^\top$, where ϵ is a symmetric positive matrix, is gauge invariant if

$$[J, \epsilon\Delta] = 0,$$

i. e., J is the operator of complex structure from the polar decomposition (12.75) of $D = -2\epsilon\Delta$. During the proof of Theorem 12.13 we established that such a complex structure exists for every energy matrix ϵ.

Exercise 12.14 Let $\omega_j, j = 1, \ldots, s$, be positive numbers, and let

$$H = \sum_{j=1}^{S} \frac{1}{2} \left(\omega_j^2 q_j^2 + p_j^2\right)$$

be the energy operator of ensemble of oscillators with the frequencies ω_j. Then $\tilde{q}_j = \sqrt{\omega_j} q_j, \tilde{p}_j = \sqrt{\omega_j}^{-1} p_j$, so that

$$\tilde{a}_j^\dagger = \frac{1}{\sqrt{2\omega_j}} \left(\omega_j q_j - i p_j\right), \quad \tilde{a}_j = \frac{1}{\sqrt{2\omega_j}} \left(\omega_j q_j + i p_j\right)$$

and

$$H = \sum_{j=1}^{S} \frac{\omega_j}{2} \left(\tilde{q}_j^2 + \tilde{p}_j^2\right) = \sum_{j=1}^{S} \omega_j \left(\tilde{a}_j^\dagger \tilde{a}_j + I/2\right).$$

The corresponding operator of complex structure is

$$J = \operatorname{diag} \begin{bmatrix} 0 & -\omega_j \\ \omega_j^{-1} & 0 \end{bmatrix},$$

while the gauge operator G in $\mathcal{H}$ is given by (12.79).

10.12.10 12.3 Gaussian States

10.12.11 12.3.1 Characteristic Function

The characteristic function of a quantum state S is defined as

$$\phi_S(z) = \operatorname{Tr} SW(z), \quad z \in Z.$$

This is a kind of noncommutative Fourier transform, uniquely defining the operator S. The corresponding inversion formula is

$$S = \frac{1}{(2\pi)^s} \int \phi_S(z) W(-z) d^{2s} z$$

where $d^{2s}z = dx_1 \dots dy_s$ is the element of symplectic volume in Z. Similar relations hold for arbitrary trace class operator S; see [122].

Positivity of the operator S implies (and is in fact equivalent to) the nonnegative definiteness of $n \times n$-matrices, i.e.,

$$\left[\phi_S\left(z_r - z_S\right) \exp\left(\frac{i}{2}\Delta\left(z_r, z_S\right)\right)\right]_{r,S=1,\dots,n} \geq 0. \tag{12.80}$$

for all $n = 1, 2, \dots$ and arbitrary collections $\{z_1, \dots, z_n\} \in Z$. To see the necessity of this condition, note that the matrix element is nothing but $\operatorname{Tr} W\left(z_s\right)^* SW\left(z_r\right)$ so that for arbitrary $c_1, \dots, c_n \in \mathbb{C}$

$$\sum_{r,S} c_r \bar{c}_S \phi_S\left(z_r - z_S\right) \exp\left(\frac{i}{2}\Delta\left(z_r, z_S\right)\right) = \operatorname{Tr} SAA^* \geq 0$$

where $A = \sum_r c_r W\left(z_r\right)$.

A density operator S has finite second moments if $\operatorname{Tr} S\left(q_j^2 + p_j^2\right) < \infty$ for all j, where the trace is defined as in (11.6). In this case one can define the mean vector $\operatorname{Tr} SR = m$ and the covariance matrix $\mathrm{B}_S(R) = \alpha$ (cf. Section 2.3.3 for the case of bounded observables). By CCR (12.56) the commutation matrix $\mathrm{C}_S(R) = -\Delta$, so that

$$\alpha + \frac{i}{2}\Delta = \operatorname{Tr}(R - m)^\top S(R - m) \tag{12.81}$$

This relation (and its transpose) implies the inequality

$$\alpha \geq \pm\frac{i}{2}\Delta \tag{12.82}$$

which is nothing but the uncertainty relation (2.20) for the canonical observables R. Below in Theorem 12.17 we show that the condition (12.82) is not only necessary but also sufficient for α to be the covariance matrix of a quantum state. We denote by $\Sigma(m, \alpha)$ the set of all states with the mean vector m and the covariance matrix α.

As in probability theory, the components of m, α (as well as higher moments) can be expressed via the derivatives of the characteristic function.

Exercise 12.15 Assuming existence of the corresponding moments, show that

$$\operatorname{Tr} S(Rz)^n = i^{-n} \frac{d^n}{dt^n} \phi(tz)\bigg|_{t=0}.$$

10.12.12 12.3.2 Definition and Properties of Gaussian States

The characteristic function (12.33) of the one-mode density operator (12.28), expressed in the real variables using (12.52), is

$$\operatorname{Tr} SW(z) = \exp\left[i\left(m_q x + m_p y\right) - \frac{\alpha}{2}\left(x^2 + y^2\right)\right] \tag{12.83}$$

where $\alpha = N + \frac{1}{2} \geq \frac{1}{2}$. We call such S elementary Gaussian state. Let us now elaborate the general definition of a multimode Gaussian state.

The state S is called Gaussian, if its characteristic function $\phi(z) = \operatorname{Tr} SW(z)$ has the form

$$\phi(z) = \exp\left(\mathrm{im}(z) - \frac{1}{2}\alpha(z, z)\right) \tag{12.84}$$

where $m(z) = mz$ is a linear form and $\alpha(z,z) = z^\top \alpha z$ is a bilinear form on $(\ Z, \Delta\ )$. Here m is a row $2s$-vector and α is a real symmetric $(\ 2s\ ) \times (2s)$-matrix.

Exercise 12.16 Considering the derivatives of (12.84) at $z = 0$, show that m is indeed the mean vector, and α is the covariance matrix determined from (12.81).

Usually $(\ m, \alpha\ )$ are called the parameters of the Gaussian state. In the case $m = 0$ we call the Gaussian state centered. If S_m is the Gaussian state with parameters $(\ m, \alpha\ )$, then

$$S_m = W\left(-\Delta^{-1} m^\top\right) S_0 W\left(-\Delta^{-1} m^\top\right)^* \tag{12.85}$$

as follows from (12.55). By this unitary equivalence many questions reduce to consideration of centered states.

Theorem 12.17. For relation (12.84) to define a quantum state, it is necessary and sufficient that the matrix α satisfies the condition (12.82). Under this condition formula (12.84) defines the unique Gaussian state in $\Sigma(m, \alpha)$.

Proof. It was already mentioned that the necessity follows from the relation (12.81). An alternative proof follows from the following lemma, which will be also needed in the sequel.

Lemma 12.18. Let α be an inner product and Δ a skew-symmetric form in Z, such that for all $n = 1, 2, \ldots$ and arbitrary collection $\{z_1, \ldots, z_n\} \subset Z$,

$$\left[\exp\left(\alpha\left(z_r, z_s\right) + \frac{i}{2}\Delta\left(z_r, z_s\right)\right)\right]_{r,s=1,\ldots n} \geq 0. \tag{12.86}$$

Then the matrices of forms α, Δ satisfy the condition (12.82).

Proof. Let $t > 0$. By writing the condition of nonnegative definiteness for the collection $\left\{0, \sqrt{t} z_1, \ldots, \sqrt{t} z_n\right\}$ with the variables $\{c_0, c_1, \ldots, c_n\} \in \mathbb{C}$ such that $c_0 = -\sum_{j=1}^n c_j$, we have

$$\sum_{r,S=1}^n \bar{c}_r c_S \left(\exp t\left[\alpha\left(z_r, z_S\right) + \frac{i}{2}\Delta\left(z_r, z_S\right)\right] - 1\right) \geq 0$$

Dividing by t and letting $t \to 0$ we obtain that the matrices with elements $\alpha\left(z_r, z_s\right) + \frac{i}{2}\Delta\left(z_r, z_S\right)$ are nonnegative definite for arbitrary collection $z_1, \ldots, z_n$, which is equivalent to the condition (12.82). This proves the lemma.

Substituting the Gaussian expression (12.84) into (12.80), one can see that

$$\phi\left(z_r - z_s\right) \exp\left[\frac{i}{2}\Delta\left(z_r, z_s\right)\right] = \phi\left(z_r\right) \overline{\phi\left(z_s\right)} \exp\left\{\alpha\left(z_r, z_s\right) + \frac{i}{2}\Delta\left(z_r, z_s\right)\right\}$$

thus the condition of Lemma 12.18 is fulfilled, implying inequality (12.82).

To prove sufficiency assume that the matrix α satisfies inequality (12.82). Lemma 12.12 then implies that there exists a symplectic transformation T such that

$$\tilde{\alpha} = T^\top \alpha T = \operatorname{diag}\begin{bmatrix} \alpha_j & 0 \\ 0 & \alpha_j \end{bmatrix} \tag{12.87}$$

where $\alpha_j > 0$, while inequality (12.82) is easily seen to be equivalent to

$$\alpha_j \geq \frac{1}{2}, \quad j = 1, \ldots, s \tag{12.88}$$

The relation (12.87) implies

$$\begin{aligned} \phi(Tz) &= \exp\left(i\tilde{m}z - \frac{1}{2} z^\top \tilde{\alpha} z\right) \\ &= \exp \sum_{j=1}^s \left[i\left(\tilde{m}_{jq} x_j + \tilde{m}_{jp} y_j\right) - \frac{1}{2}\alpha_j\left(x_j^2 + y_j^2\right)\right] \end{aligned}$$

where $\tilde{m} = mT$.
Denoting by $S^{(j)}$ the corresponding elementary one-mode Gaussian states (12.83) and putting

$$S = \bigotimes_{j=1}^{s} S^{(j)} \tag{12.89}$$

we obtain

$$\phi(Tz) = \operatorname{Tr} S \exp i\tilde{R}z = \operatorname{Tr} SW(Tz),$$

where $\tilde{R} = RT$ are the new canonical observables. It follows that the state S has the characteristic function $\phi(z)$. □

In quantum optics the representation of a Gaussian state in the form (12.89) is usually related to the normal mode decomposition.

Let J be an operator of complex structure in Z and $\{U_\varphi\}$ be the corresponding unitary group of gauge transformations in $\mathcal{H}$. A state S is gauge invariant if

$$S = U_\varphi S U_\varphi^* \tag{12.90}$$

for all φ, which by (12.77) is equivalent to the property $\phi(z) = \phi\left(\mathrm{e}^{\varphi J} z\right)$ of the characteristic function. From this it follows that the Gaussian density operator S is gauge invariant if $m(z) \equiv 0$ and $\alpha(z, z') = \alpha(Jz, Jz')$, which is equivalent to

$$m = 0, \quad J^\top \alpha + \alpha J = 0. \tag{12.91}$$

By using (12.60), the last equality can be written as

$$[J, A] = 0, \tag{12.92}$$

where $A = \Delta^{-1}\alpha$, which means that J is the complex structure from the polar decomposition (12.63), i. e., $J = T\tilde{J}T^{-1}$, where $\tilde{J}$ is defined by the relation (12.64).

Note that the elementary Gaussian state (12.83) is pure if and only if $N = 0$, i.e., $\alpha = 1/2$. Using the decomposition (12.89) this implies several equivalent conditions for purity of a general Gaussian state.

Exercise 12.19 Show that the Gaussian state S is pure if and only if one of the following equivalent conditions holds:
i. $\alpha_j = 1/2, j = 1, \ldots, s$;
ii. $|\det(2A)| = 1$;
iii. the operator $A = \Delta^{-1}\alpha$ satisfies

$$A^2 = -\frac{1}{4} l; \tag{12.93}$$

iv. $\alpha = \frac{1}{2}\Delta J$, where J is an operator of complex structure;
v. α is a minimal solution of inequality (12.82).

Hint: it is sufficient to check conditions ii-iv in the symplectic basis from Lemma 12.12.

Under these conditions the set $\Sigma(m, \alpha)$ consists of one pure Gaussian state.

Let S be a centered Gaussian state with the covariance matrix α, let J be an operator of complex structure from the polar decomposition (12.63), and let S_0 be the pure centered Gaussian state with the covariance matrix $\frac{1}{2}\Delta J$. Then both these states are gauge invariant under the unitary group $\{\exp(i\varphi G)\}$ corresponding to this complex structure.

Exercise 12.20 By using the normal mode decomposition (12.89) prove the following multi-mode generalization of formula (12.23):

$$S = \int W(z) S_0 W(z)^* P\left(d^{2s}z\right) \tag{12.94}$$

where P is the Gaussian probability distribution with the characteristic function

$$\int \mathrm{e}^{i\Delta(w,z)} P\left(d^{2s}z\right) = \exp\left[-w^\top\left(\alpha - \frac{1}{2}\Delta J\right)w\right]$$

This distribution is invariant under the complex structure J in Z.

The gauge invariant pure state S_0 plays the role of the vacuum state while $W\left(-\Delta^{-1}z\right) S_0 W\left(-\Delta^{-1}z\right)^*$ are the coherent states with respect to the complex structure J (usually one uses the complex parametrization, see below). Note that a state that is "squeezed" relative to a given complex structure can be always made "coherent" by using the complex structure associated with its covariance matrix. In physics the distinguished complex structure is one with which the oscillator Hamiltonian has the canonical form (12.73) and coherent/squeezed states are defined relative to that complex structure.

Let us come back to the coordinate picture of the symplectic space $Z = \mathbb{R}^{2s}$. Putting $z_j = \frac{1}{\sqrt{2}}\left(x_j + iy_j\right)$, we consider the complex linear space $\mathbf{Z} = \mathbb{C}^{\mathcal{S}}$ of s-dimensional complex column vectors $\mathbf{z} = \left[z_1, \ldots, z_s\right]^\top$. The symplectic form (12.49) is expressed as

$$\Delta\left(z, z'\right) = 2\,\mathrm{Im}\,\mathbf{z}^*\mathbf{z}'$$

where * denotes Hermitian conjugation of the vectors. The operator J acts as multiplication by i and the corresponding Hermitian inner product (12.61) in $\mathbf{Z}$ is just $\mathbf{z}^*\mathbf{z}'$. A symplectic basis $e_1, h_1, \ldots, e_s, h_s$ gives rise to the orthonormal basis $\sqrt{2}e_1, \ldots, \sqrt{2}e_s$ with respect to this inner product.

The canonical observables $R = \left[q_1, \ldots, q_s, p_1, \ldots, p_s\right]$ (note the rearrangement of the order of components) are replaced by the creation-annihilation operators $\mathbf{a}^\dagger = \left[a_1^\dagger, \ldots, a_s^\dagger\right], \mathbf{a} = \left[a_1, \ldots, a_s\right]^\top$, where

$$a_j^\dagger = \frac{1}{\sqrt{2}}\left(q_j - ip_j\right), \quad a_j = \frac{1}{\sqrt{2}}\left(q_j + ip_j\right)$$

satisfy the commutation relations

$$\left[a_j, a_k^\dagger\right] = \delta_{jk} I, \quad \left[a_j, a_k\right] = \left[a_j^\dagger, a_k^\dagger\right] = 0. \tag{12.95}$$

The complex parametrization of the Weyl operators is given by the displacement operators

$$D(\mathbf{z}) = W(-Jz), \quad \mathbf{z} \in \mathbf{Z}. \tag{12.96}$$

The relation (12.54) can be rewritten as $D(\mathbf{z}) = \exp\left(\mathbf{a}^\dagger\mathbf{z} - \mathbf{z}^*\mathbf{a}\right)$.
The linear operators in Z commuting with J are represented by complex $s \times s$-matrices. The gauge group acts in $\mathbf{Z}$ as multiplication by $e^{i\phi}$.

Consider the Gaussian state (12.84) with the correlation matrix

$$\alpha = \begin{bmatrix} \alpha_{qq} & \alpha_{qp} \\ \alpha_{pq} & \alpha_{pp} \end{bmatrix},$$

where $\alpha_{qq}, \alpha_{qp}, \alpha_{pp}$ are real $s \times s$-matrices satisfying

$$\alpha_{qq}^\top = \alpha_{qq} = \left[\mathrm{Tr}\, S\left(q_j \circ q_k\right)\right], \quad \alpha_{pp}^\top = \alpha_{pp} = \left[\mathrm{Tr}\, S\left(p_j \circ p_k\right)\right], \quad \alpha_{qp}^\top = \alpha_{pq} = \left[\mathrm{Tr}\, S\left(q_j \circ p_k\right)\right].$$

It is gauge invariant if its mean m is zero while the correlation matrix satisfies (12.91). With

$$J = \begin{bmatrix} 0 & -I_s \\ I_s & 0 \end{bmatrix}$$

this implies $\alpha_{qq} = \alpha_{pp}, \alpha_{qp} = -\alpha_{pq}$, hence (12.84) can be rewritten as

$$\phi(\mathbf{z}) = \operatorname{Tr} SD(\mathbf{z}) = \exp\left(-\mathbf{z}^* \boldsymbol{\alpha} \boldsymbol{z}\right), \tag{12.97}$$

where

$$\boldsymbol{\alpha} = \alpha_{qq} - i\alpha_{qp}.$$

Exercise 12.21 Show that the (nonvanishing identically) second moments of the gauge invariant state S satisfy the relation

$$\operatorname{Tr} \mathbf{a} S \mathbf{a}^\dagger = \left[\operatorname{Tr} a_j S a_k^\dagger\right] = \boldsymbol{\alpha} - \frac{1}{2}\mathbf{I}. \tag{12.98}$$

Note that

$$U^* \alpha U = \begin{bmatrix} \alpha_{qq} - i\alpha_{qp} & 0 \\ 0 & \alpha_{qq} + i\alpha_{qp} \end{bmatrix},$$

where

$$U = \frac{1}{\sqrt{2}} \begin{bmatrix} I_s & I_s \\ -iI_s & iI_s \end{bmatrix} \tag{12.99}$$

is a unitary $2s \times 2s$-matrix. It follows for real λ that

$$\det\left(\alpha - \lambda I_{2s}\right) = \left|\det\left(\alpha - \lambda I_s\right)\right|^2,$$

hence the Hermitian matrix $\boldsymbol{\alpha}$ has the eigenvalues α_j (see (12.88)), so that $\boldsymbol{\alpha} \geq \mathbf{I}/2$. The unique minimal solution of the last inequality is $\frac{1}{2}\mathbf{I}$, to which correspond the vacuum state S_0 and the family of coherent states $\{S_{\mathbf{z}}; \mathbf{z} \in \mathbf{Z}\}$, such that

$$S_{\mathbf{z}} = D(\mathbf{z}) S_0 D(\mathbf{z})^*$$

One has

$$\operatorname{Tr} S_{\mathbf{w}} D(\mathbf{z}) = \exp\left(2i \operatorname{Im} \mathbf{w}^* \mathbf{z} - \frac{1}{2}|\mathbf{z}|^2\right)$$

The relation (12.94) thus takes the form

$$S = \int S_{\mathbf{z}} P\left(d^{2s} z\right) \tag{12.100}$$

where P is the Gaussian probability distribution with the characteristic function

$$\int \mathrm{e}^{2i \operatorname{Im} \mathbf{w}^* \mathbf{z}} P\left(d^{2s} z\right) = \exp\left[-\mathbf{z}^* \left(\boldsymbol{\alpha} - \frac{1}{2}\mathbf{I}\right) \mathbf{z}\right]$$

10.12.13 12.3.3 The Density Operator of Gaussian State

The spectral decomposition of an arbitrary Gaussian state (12.89) can be obtained by tensor multiplication of the spectral decompositions of the one-mode states $S^{(j)}$ from the normal mode decomposition. We are going to prove the theorem which generalizes the relation (12.25) to arbitrary Gaussian states without a pure component.

Lemma 12.22. The Gaussian density operator S is nondegenerate if and only if

$$\det\left(\alpha+\frac{i}{2}\Delta\right)\neq 0.$$

Proof. The Gaussian density operator S is nondegenerate if and only if it has no pure component, i.e., $\alpha_j>\frac{1}{2}, j=1,\dots,s$. We will prove the lemma by establishing the identities

$$\det\left(\alpha+\frac{i}{2}\Delta\right)=\left[\det\left(-A^2-\frac{1}{4}I\right)\right]^{\frac{1}{2}}=\prod_{j=1}^{s}\left(\alpha_j^2-\frac{1}{4}\right), \tag{12.101}$$

where $A=\Delta^{-1}\alpha$. Choosing the symplectic basis as in Lemma 12.12, we have $A=T\left(\Delta^{-1}\tilde{\alpha}\right)T^{-1}$, where

$$\Delta^{-1}\tilde{\alpha}=\operatorname{diag}\begin{bmatrix}0 & -\alpha_j\\ \alpha_j & 0\end{bmatrix} \tag{12.102}$$

Hence the numbers $\pm i\alpha_j, j=1,\dots,s$, are the eigenvalues of the operator A. It follows that the symmetric operator $-A^2-\frac{1}{4}I$ in the Euclidean space (Z,α) is positive since its eigenvalues are $\alpha_j^2-1/4\geq 0$ (note that this operator is equal to 0 if and only if the state S is pure by (12.93)). Each of these eigenvalues appears twice, hence the second identity in (12.101) follows.

To prove the first identity note that

$$-\left(\Delta^{-1}\alpha\right)^2-\frac{1}{4}I=-\Delta^{-1}\left(\alpha+\frac{i}{2}\Delta\right)\Delta^{-1}\left(\alpha-\frac{i}{2}\Delta\right).$$

Taking into account that $\det\left(\pm\Delta^{-1}\right)=1$ and $\det\left(\alpha+\frac{i}{2}\Delta\right)=\det\left(\alpha-\frac{i}{2}\Delta\right)\geq 0$ we obtain the result.

Theorem 12.23. Let the matrix $\alpha+\frac{i}{2}\Delta$ be nondegenerate. Then the centered Gaussian density operator with covariance matrix α has the form

$$S_0=c\exp\left(-R\epsilon R^{\top}\right), \tag{12.103}$$

where

$$c=\left[\det\left(\alpha+\frac{i}{2}\Delta\right)\right]^{-\frac{1}{2}}=\left[\det\left(-4\sin^2\epsilon\Delta\right)\right]^{\frac{1}{4}} \tag{12.104}$$

and ϵ is found from the relation

$$2\Delta^{-1}\alpha=\cot\epsilon\Delta. \tag{12.105}$$

Proof. Rewriting the relation (12.25) (for $\omega=1$) in the form

$$\left(\mathrm{e}^{\theta/2}-\mathrm{e}^{-\theta/2}\right)\exp\left(-\frac{\theta}{2}\left(q^2+p^2\right)\right),$$

using the normal modes decomposition (12.87) diagonalizing α, and using (12.89) we have

$$S_0=c\exp\left(-\tilde{R}\tilde{\epsilon}\tilde{R}^{\top}\right),$$

where

$$c = \prod_{j=1}^{s} \left(\mathrm{e}^{\theta_j/2} - \mathrm{e}^{-\theta_j/2} \right), \quad \tilde{\epsilon} = \operatorname{diag} \begin{bmatrix} \theta_j/2 & 0 \\ 0 & \theta_j/2 \end{bmatrix},$$

and $\theta_j = \ln\left(\frac{\alpha_j+\frac{1}{2}}{\alpha_j-\frac{1}{2}}\right)$, so that

$$\mathrm{e}^{\theta_j/2} - \mathrm{e}^{-\theta_j/2} = \left(\alpha_j^2 - \frac{1}{4}\right)^{-\frac{1}{2}}. \tag{12.106}$$

Taking into account (12.101), the first of the expressions in (12.104) follows. Returning to the initial canonical observables R, we obtain (12.103) where $\epsilon = T\tilde{\epsilon}T^{\top}$.

Inverting formula (12.106) gives

$$\alpha_j = \frac{1}{2} \coth \frac{\theta_j}{2} \tag{12.107}$$

Further

$$\tilde{\epsilon}\Delta = \operatorname{diag} \begin{bmatrix} 0 & \theta_j/2 \\ -\theta_j/2 & 0 \end{bmatrix}.$$

Note that $\epsilon\Delta = T\tilde{\epsilon}\Delta T^{-1}$ and $\Delta^{-1}\alpha = T\Delta^{-1}\tilde{\alpha}T^{-1}$ are the matrices of operators, with $\Delta^{-1}\tilde{\alpha}$ given by the relation (12.102). The operators $-\tilde{\epsilon}\Delta$ and $\tilde{\Delta}^{-1}\tilde{\alpha}$ have the same eigenvectors with the eigenvalues $\pm i\theta_j/2$ and $\pm i\alpha_j$, therefore via the relation $\cot(i\lambda) = -i\coth\lambda$, (12.107) implies (12.105).

10.12.14 12.3.4 Entropy of a Gaussian State

To compute the von Neumann entropy of a general Gaussian state one can use the normal mode decomposition (12.89). By (12.85) the entropy is the same for all Gaussian states with arbitrary mean and covariance matrix α, reducing the problem to the case of centered state. For a single mode ($s = 1$), the density operator $S^{(j)}$ is unitarily equivalent to the state (12.24) with the entropy equal to $g(N)$; see (12.27). For a general Gaussian state we obtain by summing over normal modes

$$H(S) = \sum_{j=1}^{S} g\left(N_j\right) \tag{12.108}$$

where $N_j = \alpha_j - 1/2 \geq 0$. In particular, the entropy of the gauge invariant Gaussian state with characteristic function (12.97) is

$$H(S) = \operatorname{Spg}\left(\boldsymbol{\alpha} - \frac{1}{2}\mathbf{I}\right) \tag{12.109}$$

where Sp is used to denote the trace of a matrix as distinct from the trace Tr of operators in the underlying Hilbert space.

To write the relation (12.108) in the coordinate-free form, recall that the operator $A = \Delta^{-1}\alpha$ has the eigenvalues $\pm i\alpha_j$. Hence its matrix is diagonalizable (in the complex domain). For any diagonalizable matrix $M = U \operatorname{diag}(m_j) U^{-1}$, we put $\operatorname{abs}(M) = U \operatorname{diag}(|m_j|) U^{-1}$, similarly to other continuous functions on the complex plane. Then equation (12.108) can be written as

$$H(S) = \frac{1}{2} \operatorname{Spg}\left(\operatorname{abs}\left(\Delta^{-1}\alpha\right) - \frac{I}{2}\right) \tag{12.110}$$

An alternative expression for the entropy of a Gaussian state can be obtained from the representation (12.103). By definition, we have

$$H(S) = -\log c + \mathrm{Sp}\epsilon\alpha$$

which by (12.104) and (12.105) is equal to

$$\begin{aligned} &\frac{1}{4}\,\mathrm{Sp}\log\left[-\left(\Delta^{-1}\alpha\right)^2 - \frac{1}{4}I\right] + \mathrm{Sp}\left(\Delta^{-1}\alpha\right)\mathrm{arccot}\left(2\Delta^{-1}\alpha\right) \\ &\quad = -\frac{1}{4}\,\mathrm{Sp}\log\left(-\sin^2\epsilon\Delta\right) + \frac{1}{2}\,\mathrm{Sp}(\epsilon\Delta\cot\epsilon\Delta) \end{aligned} \tag{12.111}$$

Exercise 12.24 Use the relation

$$g\left(x-\frac{1}{2}\right) = \frac{1}{2}\log\left(x^2-\frac{1}{4}\right) + x\log\frac{x+\frac{1}{2}}{x-\frac{1}{2}}$$

to show that (12.110) and (12.111) are the same.

Example 12.25. In the case of a one-mode Gaussian density operator we have $\alpha = \begin{bmatrix} \alpha^{qq}\alpha^{qp} \\ \alpha^{qp}\alpha^{pp} \end{bmatrix}$ with $\alpha^{qq}\alpha^{pp} - (\alpha^{qp})^2 \geq \frac{1}{4}$ (this inequality is equivalent to the condition (12.82)). Then

$$-\left(\Delta^{-1}\alpha\right)^2 = \left[\alpha^{qq}\alpha^{pp} - (\alpha^{qp})^2\right]\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

hence

$$\left|\Delta^{-1}\alpha\right| = \sqrt{\alpha^{qq}\alpha^{pp} - (\alpha^{qp})^2}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

and

$$H(S) = g\left(\sqrt{\alpha^{qq}\alpha^{pp} - (\alpha^{qp})^2} - \frac{1}{2}\right).$$

Geometrically, the quantity $\pi\sqrt{\alpha^{qq}\alpha^{pp} - (\alpha^{qp})^2}$ is equal to the area of the deviation ellipsoid

$$z^\top\alpha^{-1}z = 1, \quad z = [x,y]^\top$$

for the two-dimensional Gaussian distribution with the covariance matrix α.
Note that in accordance with (12.93) the Gaussian state is pure if and only if it has the minimal uncertainty $\alpha^{qq}\alpha^{pp} - (\alpha^{qp})^2 = \frac{1}{4}$. This comprises both coherent states for which

$$\alpha^{qq} = \alpha^{pp} = \frac{1}{2}, \quad \alpha^{qp} = 0$$

and squeezed states for which this condition is violated (as distinct from quantum optics we use here real rather than complex parametrization). The case of many modes can be treated by using the normal mode decomposition.

While pure Gaussian states are the minimal uncertainty states for the canonical observables, a general Gaussian state is characterized by the following property of maximal entropic uncertainty under fixed moments of the canonical observables.

Lemma 12.26. The Gaussian state has the largest entropy among all states with the given mean m and the correlation matrix α. Therefore, for any set of states defined by restrictions

on the first and second moments, the maximum of the entropy always can be sought among the Gaussian states.

Proof. Let $S \in \Sigma(m,\alpha)$ and let $\tilde{S}$ be the unique Gaussian state in $\Sigma(m,\alpha)$. Without loss of generality we may assume that $\tilde{S}$ is nondegenerate. The general case can be reduced to this by separating the pure component in the tensor product decomposition of $\tilde{S}$. Indeed by making the normal modes decomposition, we can assume that $Z = Z_1 \oplus Z_2$ with $\Delta = \Delta_1 \oplus \Delta_2, \alpha = \alpha_1 \oplus \alpha_2$ (see the next section for the direct sum decompositions), where α_1 corresponds to the unique, necessarily pure Gaussian state in Z_1, while α_2 corresponds to a nondegenerate density operator. We have

$$H(\tilde{S}) - H(S) = H(S;\tilde{S}) + \mathrm{Tr}(S-\tilde{S})\log\tilde{S},$$

where the last term is equal to zero, because for a nondegenerate Gaussian $\tilde{S}$ the operator $\log\tilde{S}$ is a second-order polynomial in canonical variables by (12.103), while the first and second moments of $S, \tilde{S}$ coincide. Thus $H(\tilde{S}) - H(S) = H(S;\tilde{S}) \geq 0$. □

A similar result is obtained for the conditional quantum entropy [66]. In its formulation and proof we use the description of composite bosonic systems introduced in the next section 12.3.5.

Lemma 12.27. The Gaussian state has the largest conditional entropy among all states of a composite bosonic system AB with a given mean m and a correlation matrix α.

Proof. Let $S_{AB} \in \Sigma(m_{AB},\alpha_{AB})$ and let $\tilde{S}_{AB}$ be the unique Gaussian state in $\Sigma(m_{AB},\alpha_{AB})$. Then $S_A \in \Sigma(m_A,\alpha_A)$ and $\tilde{S}_A$ is the Gaussian state in $\Sigma(m_A,\alpha_A)$. Again we may assume that $\tilde{S}_{AB}$ is nondegenerate. Denoting

$$H(A \mid B) = H(S_{AB}) - H(S_B), \quad H(\tilde{A} \mid \tilde{B}) = H\left(\tilde{S}_{AB}\right) - H\left(\tilde{S}_B\right),$$

we have

$$\begin{aligned} H(\tilde{A} \mid \tilde{B}) - H(A \mid B) =& H\left(S_{AB};\tilde{S}_{AB}\right) - H\left(S_A;\tilde{S}_A\right) \\ &+ \mathrm{Tr}\left(S_{AB}-\tilde{S}_{AB}\right)\log\tilde{S}_{AB} - \mathrm{Tr}\left(S_A-\tilde{S}_A\right)\log\tilde{S}_A \\ =& H\left(S_{AB};\tilde{S}_{AB}\right) - H\left(S_A;\tilde{S}_A\right) \end{aligned}$$

because $\log\tilde{S}_{AB}, \log\tilde{S}_A$ are the second-order polynomials in canonical variables by (12.103). By monotonicity of the relative entropy, $H\left(S_{AB};\tilde{S}_{AB}\right) - H\left(S_A;\tilde{S}_A\right) \geq 0$. □

10.12.15 12.3.5 Separability and Purification

Consider two bosonic systems described by CCRs with the symplectic spaces (Z_1,Δ_1), (Z_2,Δ_2). The symplectic space of the composite system is the direct sum $Z = Z_1 \oplus Z_2$, the elements of which are conveniently represented by the column vectors $z = [z_1, z_2]^\top$ while the symplectic matrix Δ_{12} is block diagonal, i.e.,

$$\Delta_{12} = \begin{bmatrix} \Delta_1 & 0 \\ 0 & \Delta_2 \end{bmatrix}.$$

The Weyl operators of the composite system are defined as $W_{12}(z_1,z_2) = W_1(z_1) \otimes W_2(z_2)$. Let S_{12} be a Gaussian state of the composite system with the mean m_{12} and the covariance matrix α_{12}. The restriction of the Gaussian state S_{12} to the first factor is determined by the expectations of the Weyl operators $W_1(z_1) \otimes I_2 = W_{12}(z_1,0)$, hence according to (12.84), it has the mean m_1 which is just the first component of $m_{12} = [m_1 m_2]$, and the covariance matrix α_1 which is the first diagonal block in the block matrix decomposition

$$\alpha_{12} = \begin{bmatrix} \alpha_1 & \beta \\ \beta^\top & \alpha_2 \end{bmatrix}. \tag{12.112}$$

The covariance matrix α_{12} of a state S_{12} of the composite system is block diagonal ($\beta = 0$) if and only if the state is a product $S_{12} = S_1 \otimes S_2$.

Proposition 12.28. [244] The Gaussian state is separable if and only if there exist real symmetric matrices $\check{\alpha}_j$ satisfying

$$\check{\alpha}_j \geq \pm\frac{i}{2}\Delta_j, \quad j = 1, 2, \tag{12.113}$$

such that

$$\alpha_{12} \geq \begin{bmatrix} \check{\alpha}_1 & 0 \\ 0 & \check{\alpha}_2 \end{bmatrix}. \tag{12.114}$$

Proof. By using formula (12.85) and the fact that the action of the displacement operators is "local" and has no effect on (non)separability, we can assume without loss of generality that S_{12} is centered. Let S_{12} be separable. Then it has a representation (11.43). Since S_{12} has finite second moments, this representation implies that the states $S_1(x), S_2(x)$ have finite second moments for π-almost all x, hence their mean vectors $m_j(x)$ and covariance matrices $\alpha_j(x) \geq \pm\frac{i}{2}\Delta_j, j = 1, 2$, are defined for π-almost all x. In
view of (12.81) the representation (11.43) implies that α_{12} has the block decomposition (12.112) with

$$\alpha_j = \int_{\mathcal{X}} \left[\alpha_j(x) + m_j(x)^\top m_j(x)\right] \pi(dx), \quad j = 1, 2$$
$$\beta = \int_{\mathcal{X}} m_1(x)^\top m_2(x) \pi(dx)$$

Denoting $\check{\alpha}_j = \int_{\mathcal{X}} \alpha_j(x)\pi(dx)$, we have (12.113) and

$$\alpha_{12} - \begin{bmatrix} \check{\alpha}_1 & 0 \\ 0 & \check{\alpha}_2 \end{bmatrix} = \begin{bmatrix} \alpha_1 - \check{\alpha}_1 & \beta \\ \beta^\top & \alpha_2 - \check{\alpha}_2 \end{bmatrix}$$
$$= \int_{\mathcal{X}} \begin{bmatrix} m_1(x)^\top m_1(x) & m_1(x)^\top m_2(x) \\ m_2(x)^\top m_1(x) & m_2(x)^\top m_2(x) \end{bmatrix} \pi(dx) \geq 0$$

Conversely, if (12.114) holds, then let

$$\gamma_{12} = \alpha_{12} - \begin{bmatrix} \check{\alpha}_1 & 0 \\ 0 & \check{\alpha}_2 \end{bmatrix} \geq 0$$

and define π to be the Gaussian probability distribution on $Z = Z_1 \oplus Z_2$ with the characteristic function

$$\int_Z \mathrm{e}^{-i\Delta(w,z)} \pi\left(d^{2s}w\right) = \exp\left(-\frac{1}{2} z^\top \gamma_{12} z\right)$$

Then the comparison of the quantum characteristic functions shows that

$$S_{12} = \int_Z W_1(z_1) S_1 W_1(z_1)^* \otimes W_2(z_2) S_2 W_2(z_2)^* \pi\left(d^{2s}z\right) \tag{12.115}$$

where S_j is the centered Gaussian state with the covariance matrix $\check{\alpha}_j$, hence S_{12} is separable.

This proof shows in fact that a separable Gaussian state can be represented as a Gaussian mixture of Gaussian states.

From (12.114) and (12.82) it follows that the covariance matrix of a separable state, in addition to the usual condition $\alpha_{12} \geq \pm\frac{i}{2}\Delta_{12}$, satisfies

$$\alpha_{12} \geq \pm\frac{i}{2}\begin{bmatrix} \Delta_1 & 0 \\ 0 & -\Delta_2 \end{bmatrix} \tag{12.116}$$

This condition expresses the property that the state S_{12} has positive partial transpose (PPT) with respect to the second system. In fact, changing sign of the symplectic form Δ_2 corresponds to taking the transpose of the Weyl operators $W_2(z_2)$, as it follows from the CCR (12.48). As shown in [244], the PPT condition is in general weaker than the separability condition (12.114), which means that there exist bound entangled Gaussian states.

When considering purification, it is also sufficient to restrict to centered Gaussian states. Purification of one-mode Gaussian states can be performed by using the spectral decomposition (12.24) and the general purification recipe of Theorem 3.11; then for many-mode states one can use the decomposition (12.89). This leads to rather lengthy computations [106]; therefore we will just give the final result and check that it satisfies all the necessary requirements.

Now let S_1 be a Gaussian state with the covariance matrix α_1 on the symplectic space Z_1 with the form $\Delta_1 = \Delta$. It appears convenient to take $Z_2 = \bar{Z}_1$ with $\Delta_2 = -\Delta$, so that

$$\Delta_{12} = \begin{bmatrix} \Delta & 0 \\ 0 & -\Delta \end{bmatrix}. \tag{12.117}$$

Theorem 12.29. Consider the symplectic space $Z = Z_1 \oplus \bar{Z}_1$ and the Gaussian state S_{12} with the covariance matrix

$$\alpha_{12} = \begin{bmatrix} \alpha_1 & \alpha_1^{1/2}B^{-1}\sqrt{-B^2 - I/4}\alpha_1^{1/2} \\ -\alpha_1^{1/2}B^{-1}\sqrt{-B^2 - I/4}\alpha_1^{1/2} & \alpha_1 \end{bmatrix}, \tag{12.118}$$

where $B = \alpha_1^{1/2}\Delta^{-1}\alpha_1^{1/2}$. Then S_{12} is a purification of S_1.

Proof. We have seen in the proof of Lemma 12.22 that the operator $A = \Delta^{-1}\alpha_1$ is skewsymmetric in the Euclidean space (Z, α); moreover, $-A^2 - I/4 \geq 0$ with equality if and only if the Gaussian state is pure. Consider the block operator

$$A_{12} = \begin{bmatrix} A & \sqrt{-A^2 - I/4} \\ \sqrt{-A^2 - I/4} & -A \end{bmatrix} \tag{12.119}$$

in $Z = Z_1 \oplus \bar{Z}_1$, where the square root is the operator square root in the space (Z, α). It is easy to check that $-A_{12}^2 - I_{12}/4 = 0$ and hence the form $\alpha_{12} = \Delta_{12}A_{12}$ corresponds to the covariance matrix of a pure Gaussian state. Moreover, its restriction to Z_1 coincides with α_1. Formula (12.118) then gives the matrix expression for α_{12}. Note that the matrix (12.118) is symmetric nonnegative definite, which follows from the fact that $-B^2 - I/4 \geq 0$ while B is skew-symmetric. □

In the case of elementary Gaussian state (12.83) in one mode with

$$\alpha_1 = \begin{bmatrix} N + 1/2 & 0 \\ 0 & N + 1/2 \end{bmatrix},$$

formulas (12.117), (12.118) amount to

$$\Delta_{12} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix},$$

$$\alpha_{12} = \begin{bmatrix} N+1/2 & 0 & 0 & \sqrt{N^2+N} \\ 0 & N+1/2 & -\sqrt{N^2+N} & 0 \\ 0 & -\sqrt{N^2+N} & N+1/2 & 0 \\ \sqrt{N^2+N} & 0 & 0 & N+1/2 \end{bmatrix}$$

so that

$$\Delta_{12}^{-1}\alpha_{12} = \begin{bmatrix} 0 & -(N+1/2) & \sqrt{N^2+N} & 0 \\ N+1/2 & 0 & 0 & \sqrt{N^2+N} \\ \sqrt{N^2+N} & 0 & 0 & N+1/2 \\ 0 & \sqrt{N^2+N} & -(N+1/2) & 0 \end{bmatrix} \tag{12.120}$$

10.12.16 12.4 Gaussian Channels

10.12.17 12.4.1 Open Bosonic Systems

In this subsection we consider a class of quantum channels which arise naturally from the interaction of a bosonic system with a bosonic environment. Let Z_A, Z_B be symplectic spaces describing the input and the output of the channel and Z_D, Z_E their corresponding environments so that

$$Z_A \oplus Z_D = Z_B \oplus Z_E = Z \tag{12.121}$$

and let $W_A(z_A), \ldots$ be the Weyl operators on the Hilbert spaces $\mathcal{H}_A, \ldots$ of the corresponding bosonic systems. We may assume that in each subspace $Z_A, \ldots$ a symplectic basis is chosen, which allows to apply the coordinate representation.

Assume that the composite system in the Hilbert space

$$\mathcal{H}_A \otimes \mathcal{H}_D = \mathcal{H}_B \otimes \mathcal{H}_E = \mathcal{H} \tag{12.122}$$

is prepared in the initial state $S_A \otimes S_D$ and evolves according to the unitary operator U_T, which corresponds to a symplectic transformation T in Z by (12.67). In accordance with the direct sum decompositions (12.121), T can be written in the block matrix form

$$T = \begin{bmatrix} K & L \\ K_D & L_D \end{bmatrix} \tag{12.123}$$

where $K : Z_B \to Z_A, L : Z_E \to Z_A, K_D : Z_B \to Z_D, L_D : Z_E \to Z_D$.

The characteristic function of the system state after the interaction described by this unitary transformation U_T is

$$\begin{aligned} \varphi_B(z_B) &= \operatorname{Tr} U_T (S_A \otimes S_D) U_T^* (W_B(z_B) \otimes I_E) \\ &= \operatorname{Tr} (S_A \otimes S_D) U_T^* (W_B(z_B) \otimes W_E(0)) U_T \\ &= \operatorname{Tr} (S_A \otimes S_D) (W_A(Kz_B) \otimes W_D(K_D z_B)) \\ &= \varphi_A(Kz_B) \cdot \varphi_D(K_D z_B), \end{aligned}$$

where $\varphi_D(z_D) = \operatorname{Tr} S_D W_D(z_D)$ is the characteristic function of the initial state of the environment. This transformation can be written in the form

$$\varphi_B(z_B) = \varphi_A(Kz_B) \cdot f(z_B), \tag{12.124}$$

where

$$f(z_B) = \varphi_D(K_D z_B) \tag{12.125}$$

If the initial state of the environment is Gaussian with parameters (m_D, α_D), then f has the form of the Gaussian characteristic function

$$f(z_B) = \exp\left[il(z_B) - \frac{1}{2}\mu(z_B, z_B)\right], \tag{12.126}$$

where $l(z_B) = m_D(K_D z_B)$ and

$$\mu(z_B, z'_B) = \alpha_D(K_D z_B, K_D z'_B). \tag{12.127}$$

Transformation of states according to formula (12.124) is a concatenation of the unitary evolution and partial trace which are channels in the sense of Definition 11.16 and hence defines a quantum channel $\Phi : \mathfrak{T}(\mathcal{H}_A) \to \mathfrak{T}(\mathcal{H}_B)$. In what follows we will also use the abbreviation $\Phi : A \to B$.

Definition 12.30. A channel transforming states according to the rule (12.124) is called linear bosonic. If, additionally, f is a Gaussian characteristic function (12.126), where l is a linear form and μ is a pre-inner product on Z_B, the channel is called Gaussian with parameters (K, l, μ).

Let $R_A, \ldots$ be the vectors of canonical observables in $\mathcal{H}_A, \ldots$ with the commutation matrices $\Delta_A, \ldots$. From the tensor product decomposition (12.122) we have two different splits of the set of canonical observables of the composite system, i.e.,

$$[R_B R_E] = [R_A R_D].$$

According to (12.68), the action of the operator U_T is described by linear transformation

$$[R'_B R'_E] \equiv U_T^* [R_B R_E] U_T = [R_A R_D] T, \tag{12.128}$$

where T is the block matrix (12.123), and for simplicity of notations we write $R_A, \ldots$ instead of $R_A \otimes I_D, \ldots$ In particular,

$$R'_B = R_A K + R_D K_D. \tag{12.129}$$

The commutation and the covariance matrices of the canonical observables R'_B at the output of the channel are given by the expression

$$\alpha_B + \frac{i}{2}\Delta_B = \mathrm{Tr}\,(R'_B)^\top S R'_B$$

where $S = S_A \otimes S_D$ and S_A, S_D are density operators in $\mathcal{H}_A$ and $\mathcal{H}_D$ with the covariance matrices α_A and α_D, respectively. By using (12.129), we obtain

$$\Delta_B = K^\top \Delta_A K + K_D^\top \Delta_D K_D, \tag{12.130}$$

$$\alpha_B = K^\top \alpha_A K + K_D^\top \alpha_D K_D. \tag{12.131}$$

Note that in the Gaussian case $\mu = K_D^\top \alpha_D K_D$ is the matrix of the corresponding form that enters the expression for the function (12.126) defining the channel. Since $\alpha_D \geq \pm\frac{i}{2}\Delta_D$, the relation (12.130) implies the inequality

$$\mu \geq \pm \frac{i}{2} \left[\Delta_B - K^\top \Delta_A K \right] \tag{12.132}$$

which will play a key role in what follows.

Equation (12.129) is the "input-output relation" describing the channel in the way closest to the classical description "signal plus Gaussian noise." Here R_A is the quantum signal and $N_D = R_D K_D$ is the Gaussian noise with the covariance matrix $\mu = K_D^\top \alpha_D K_D$. Note that the noise can be partially quantum, partially classical because of possible degeneracy of the commutator matrix $\Delta_B - K^\top \Delta_A K$.

The final state of the environment is defined by a similar equation for the canonical observables R_E after the interaction, i.e.,

$$R'_E = R_A L + R_D L_D$$

Remark 12.31. The weakly complementary channel $\Phi_E : A \to E$ (see Section 6.6) is defined by the relation

$$\varphi_E(z_E) = \varphi_A(L z_E) \cdot \varphi_D(L_D z_E)$$

and hence it is also linear bosonic and it is Gaussian if the state S_D is Gaussian. If the initial state of the environment is pure, $S_D = |\psi_D\rangle \langle \psi_D|$, then the channel Φ_E is complementary to Φ, with the Stinespring isometry given by the formula $V = U_T |\psi_D\rangle$.

Theorem 12.32. Inequality (12.132) is necessary and sufficient condition for a set of parameters (K, l, μ) to define Gaussian channel.

Proof. The necessity of the condition (12.132) was established before. Let us show now that under this condition one can construct the symplectic transformation T defining the dynamics of the open bosonic system which gives rise to the required Gaussian channel. In doing this we can always restrict ourselves to the centered case ($l = 0$) by performing a displacement operation (12.85).

First of all, note that for the given operators K, K_D satisfying (12.130) one can always extend the transformation (12.129) to a symplectic transformation T. Indeed, the relation (12.130) means that the transformation $z_B \to [K z_B, K_D z_B]^\top$ is a symplectic embedding of Z_B into $Z_A \oplus Z_D = Z$, i.e., the columns of the matrix $[K, K_D]^\top$ form a system which can be complemented to a symplectic basis in Z, which forms the matrix T. Thus the problem reduces to the following: for given K, μ, satisfying inequality (12.132), find a symplectic space (Z_D, Δ_D), an operator $K_D : Z_B \to Z_D$, and an inner product in Z_D, defined by symmetric matrix $\alpha_D \geq \pm \frac{i}{2} \Delta_D$, such that

$$K_D^\top \Delta_D K_D = \Delta_B - K^\top \Delta_A K \equiv \tilde{\Delta}_D \tag{12.133}$$

$$K_D^\top \alpha_D K_D = \mu \tag{12.134}$$

Assume first that μ is nondegenerate. Consider the Euclidean space (Z_B, μ) with the skew-symmetric form $\tilde{\Delta}_D$. Let $2n = \dim Z_B$. By the assumption, $\mu \geq \pm \frac{i}{2} \tilde{\Delta}_D$. Consider the skew-symmetric operator S, defined by the relation

$$\tilde{\Delta}_D(z_B, z'_B) = \alpha_D(z_B, S z'_B), \quad z_B, z'_B \in Z_B.$$

According to a theorem from linear algebra, there is an orthonormal basis $\tilde{e}_j, j = 1, \ldots, 2n - l, \tilde{h}_j, j = 1, \ldots, l$, in (Z_B, μ) such that

$$S\tilde{e}_j = s_j \tilde{h}_j, S\tilde{h}_j = -s_j \tilde{e}_j, \quad j = 1, \ldots, l, \quad S\tilde{e}_j = 0, \quad j = l+1, \ldots, 2n-l$$

The condition $\mu \geq \pm\frac{i}{2}\tilde{\Delta}_D$ implies $I - \frac{i}{2}S \geq 0$, hence $0 < s_j \leq 2$.
Let (Z_D, Δ_D) be the standard symplectic space of dimensionality $2l + 2(2n-2l) = 2(2n-l)$ with the basis $e_j, h_j, j = 1, \ldots, 2n-l$. Define α_D as a form with the diagonal matrix

$$\alpha_D e_j = s_j^{-1} e_j, \quad \alpha_D h_j = s_j^{-1} h_j, \quad j = 1, \ldots, l,$$
$$\alpha_D e_j = e_j, \quad \alpha_D h_j = \frac{1}{4} h_j, \quad j = l+1, \ldots, 2n-l.$$

Then $\alpha_D \geq \pm\frac{i}{2}\Delta_D$. Define the operator $K_D : Z_B \to Z_D$ by the formula

$$K_D \tilde{e}_j = \sqrt{s_j} e_j, \quad K_D \tilde{h}_j = \sqrt{s_j} h_j, \quad j = 1, \ldots, l,$$
$$K_D \tilde{e}_j = e_j, \quad j = l+1, \ldots, 2n-l. \tag{12.135}$$

Then the relations (12.133), (12.134) follow from the consideration of the values of the corresponding quadratic forms on the basis vectors $\tilde{e}_j, j = 1, \ldots, 2n-l, \tilde{h}_j, j = 1, \ldots, l$, in Z_B. Note that by construction, α_D is the covariance matrix of a pure state if and only if $s_j = 2, j = 1, \ldots, l$.

If, on the other hand, μ vanishes on a nontrivial subspace of $Z_0 \subset Z_B$, then $\tilde{\Delta}_D$ also vanishes on Z_0 due to the condition $\mu \geq \pm\frac{i}{2}\tilde{\Delta}_D$. Therefore the vectors $\tilde{e}_j, j = l+1, \ldots, 2n-l$, can be chosen in such a way that part of them will form a basis in Z_0. Then the definition (12.135) can be modified by requiring $K_D \tilde{e}_j = 0$ for $\tilde{e}_j \in Z_0$, and the relations (12.133), (12.134) will be fulfilled. □

10.12.18 12.4.2 Gaussian Channels: Basic Properties

Formula (12.124) is equivalent to the following equation for the dual channel:

$$\Phi^* \left[W_B \left(z_B \right) \right] = W_A \left(K z_B \right) f \left(z_B \right), \tag{12.136}$$

which shows that the Weyl operators are mapped into Weyl operators, up to a factor. In the case of Gaussian channels

$$\Phi^* \left[W_B \left(z_B \right) \right] = W_A \left(K z_B \right) \exp \left[il \left(z_B \right) - \frac{1}{2} \mu \left(z_B, z_B \right) \right]. \tag{12.137}$$

From the point of view of information theory, the Gaussian channels can be defined abstractly by the relation (12.137) without reference to the picture of interaction with the environment considered in the previous section. According to Theorem 12.32 the parameters (K, l, μ) satisfy the necessary and sufficient condition (12.132) ensuring the complete positivity of Φ.

We will make use of the following properties of Gaussian channels:
i. A Gaussian channel transforms Gaussian states into Gaussian states. The parameters of the input state are transformed according to the relations

$$m_B = m_A K + l$$
$$\alpha_B = K^\top \alpha_A K + \mu. \tag{12.138}$$

Compare these with the relation (12.131).
This property is a characteristic one, i. e., any channel, which transforms Gaussian states into Gaussian states, is Gaussian [60].
ii. The dual of a linear bosonic channel transforms any polynomial in the canonical observables

R_B into a polynomial in R_A of the same order, provided the function f has derivatives of sufficiently high order. This property follows by differentiating the relation (12.136) at the point $z_B = 0$.

iii. A concatenation of Gaussian channels is a Gaussian channel. Indeed, let $\Phi_j, j = 1{,}2$, be two Gaussian channels with parameters K_j, l_j, μ_j. Then applying the definition (12.137) we get the Gaussian channel $\Phi_2 \circ \Phi_1$ with parameters

$$\begin{aligned} K &= K_1 K_2 \\ l &= K_2^\top l_1 + l_2 \\ \mu &= K_2^\top \mu_1 K_2 + \mu_2 \end{aligned} \tag{12.139}$$

iv. Any linear bosonic, in particular Gaussian, channel is covariant in the sense that

$$\Phi\left[W_A(z)^* S W_A(z)\right] = W_B\left(K'z\right)^* \Phi[S] W_B\left(K'z\right), \tag{12.140}$$

where $K' = \Delta^{-1} K^\top \Delta$ is the symplectic adjoint of K.

10.12.19 12.4.3 Gaussian Observables

Assume we have two symplectic spaces Z_A, Z_B with the corresponding Weyl systems in Hilbert spaces $\mathcal{H}_A, \mathcal{H}_B$. Let M be an observable in $\mathcal{H}_A$ with the outcome set Z_B, given by the probability operator-valued measure $M\left(d^{2n}z\right)$. In what follows we occasionally skip the index $_B$ so that $Z = Z_B$, etc. The observable is completely determined by the operator characteristic function

$$\phi_M(w) = \int \mathrm{e}^{-i\Delta(w,z)} M\left(d^{2n}z\right).$$

Note the following apparent property of the operator characteristic function: for any choice of a finite subset $\{w_j\} \subset Z_B$ the block matrix with operator entries $\phi_M\left(w_j - w_k\right)$ is nonnegative definite.

The observable M will be called Gaussian if its operator characteristic function has the form

$$\phi_M(w) = W_A(Kw) \exp\left(-\frac{1}{2}\alpha(w,w)\right) = \exp\left(iR_A K w - \frac{1}{2}\alpha(w,w)\right), \tag{12.141}$$

where $K : Z_B \to Z_A$ is a linear operator and α is a pre-inner product on Z_B. The pair (K, α) defines parameters of the Gaussian observable.

Theorem 12.33. A necessary and sufficient condition for relation (12.141) to define an observable is the matrix inequality

$$\alpha \geq \pm\frac{i}{2} K^\top \Delta_A K. \tag{12.142}$$

Proof. For an operator function given by (12.141),

$$\phi_M\left(w_j - w_k\right) = C_k^* C_j \exp\left[\alpha\left(w_j, w_k\right) - \frac{i}{2}\Delta\left(Kw_j, Kw_k\right)\right]$$

where $C_j = W_A\left(Kw_j\right) \exp\left[-\frac{1}{2}\alpha\left(w_j, w_j\right)\right]$, and nonnegative definiteness of matrices with scalar entries $\exp\left[\alpha\left(w_j, w_k\right) - \frac{i}{2}\Delta\left(Kw_j, Kw_k\right)\right]$ implies inequality (12.142) according to Lemma 12.18.

Sufficiency of the condition (12.142) will be established by a direct construction of the Naimark extension of observable M in the spirit of Corollary 3.8.

Proposition 12.34. Assume the condition (12.142). Then one can find bosonic systems in the space $\mathcal{H}_C$ with the canonical observables R_C, for which $\mathcal{H}_B \subseteq \mathcal{H}_A \otimes \mathcal{H}_C$, and the Gaussian state $S_C \in \mathfrak{S}(\mathcal{H}_C)$, such that

$$M(U) = \mathrm{Tr}_C (I_A \otimes S_C) E_{AC}(U), \quad U \subseteq Z_B \tag{12.143}$$

where E_{AC} is the sharp observable in the space $\mathcal{H}_A \otimes \mathcal{H}_C$, given by the spectral measure of commuting self-adjoint operators

$$X_B = (R_A K + R_C K_C) \Delta_B^{-1} \tag{12.144}$$

(here we again abbreviate the notations as R_A instead of $R_A \otimes I_C$, etc.), where $K_C : Z_B \to Z_C$ is operator such that

$$K_C^\top \Delta_C K_C = -K^\top \Delta_A K \tag{12.145}$$

Proof. The condition (12.145) means that $K_C^\top \Delta_C K_C + K^\top \Delta_A K = 0$, that is, commutativity of operators (12.144). By adapting the proof of Theorem 12.32, we obtain a symplectic space $(\ Z_C, \Delta_C\ )$, an operator $K_C : Z_B \to Z_C$, and an inner product in Z_C, given by the symmetric matrix $\alpha_C \geq \pm \frac{i}{2} \Delta_C$ such that (12.145) holds along with

$$K_C^\top \alpha_C K_C = \alpha$$

Then the characteristic function of the observable E_{AC} is

$$\begin{aligned} \phi_{E_{AC}}(w) &= \int \mathrm{e}^{-i\Delta(w,z)} E_{AC}\left(d^{2n} z\right) \\ &= \exp\left(i X_B \Delta_B w\right) = \exp i \left(R_A K + R_C K_C\right) w \\ &= W_A(Kw) W_C\left(K_C w\right) \end{aligned}$$

whence, denoting by S_C the centered Gaussian state with the correlation matrix α,

$$\begin{aligned} \mathrm{Tr}_C (I_A \otimes S_C) \phi_{E_{AC}}(w) &= W_A(Kw) \exp\left(-\frac{1}{2} \alpha_C\left(K_C w, K_C w\right)\right) \\ &= W_A(Kw) \exp\left(-\frac{1}{2} \alpha(w, w)\right) = \phi_M(w) \end{aligned}$$

and (12.143) follows.
The observable M is sharp if and only if $\alpha = 0$, in which case it is related to the spectral measure of the commuting self-adjoint operators $R_A K$.

Example 12.35. If $R = [qp]$ are the canonical observables of one mode A and $R_C = [q_C p_C]$ those of another mode C, then the operators $X_B = \left[\begin{array}{cc} q' & p' \end{array}\right]$ defined as

$$q' = q - q_C, \quad p' = p + p_C$$

are commuting essentially self-adjoint. If S_C is the elementary Gaussian state (12.83) with parameters $(\ 0, \alpha\ )$, then we have an extension, in the sense of Proposition 12.34, of a Gaussian observable M with parameters $(\ \Delta, \alpha\ )$. In quantum optics the observable M describes statistics of optical heterodyning.

On the other hand, a single self-adjoint operator $X = k_q q + k_p p$, where k_q, k_p are real, describes the sharp Gaussian observable with parameters $\left(\ \left[\begin{array}{cc} k_q & k_p \end{array}\right]^\top, 0\ \right)$ corresponding to optical homodyning. See, e. g., [43], [122] for more detail.

10.12.20 12.4.4 Gaussian Entanglement-Breaking Channels

Theorem 12.36. A Gaussian channel Φ with parameters $(K, 0, \mu)$ is entanglementbreaking if and only if μ admits the decomposition

$$\mu = \alpha_A + \alpha_B, \quad \text{where } \alpha_A \geq \pm\frac{i}{2}K^\top \Delta_A K, \alpha_B \geq \pm\frac{i}{2}\Delta_B. \tag{12.146}$$

In this case Φ has the representation

$$\Phi[S] = \int_{Z_B} W_B(z) S_B W_B(z)^* \mu_S\left(d^{2n}z\right) \tag{12.147}$$

where S_B is the Gaussian state with parameters $(0, \alpha_B)$ and $\mu_S(U) = \operatorname{Tr} S M_A(U), U \subseteq Z_B$, is the probability distribution of the Gaussian observable M_A with the characteristic function

$$\phi_{M_A}(w) = W_A(Kw)\exp\left(-\frac{1}{2}\alpha_A(w,w)\right). \tag{12.148}$$

Proof. First, assume that μ admits the decomposition (12.146) and consider the channel defined by (12.147); we have to show that

$$\Phi^*\left[W_B(w)\right] = W_A(Kw)\exp\left[-\frac{1}{2}\mu(w,w)\right]. \tag{12.149}$$

Indeed, for arbitrary state S

$$\begin{aligned}
\operatorname{Tr} S\Phi^*\left[W_B(w)\right] &= \operatorname{Tr}\Phi[S]W_B(w) = \int_{Z_B} \operatorname{Tr} W_B(z) S_B W_B(z)^* W_B(w) \mu_S\left(d^{2n}z\right) \\
&= \int_{Z_B} \operatorname{Tr} S_B W_B(z)^* W_B(w) W_B(z) \mu_S\left(d^{2n}z\right) \\
&= \operatorname{Tr} S_B W_B(w) \int_{Z_B} \exp[-i\Delta(w,z)]\mu_S\left(d^{2n}z\right) \\
&= \exp\left[-\frac{1}{2}\alpha_B(w,w)\right]\operatorname{Tr} S\phi_{M_A}(w) \\
&= \operatorname{Tr} S W_A(Kw)\exp\left[-\frac{1}{2}\alpha_B(w,w) - \frac{1}{2}\alpha_A(w,w)\right],
\end{aligned} \tag{12.150}$$

whence (12.149) follows.

Conversely, let the channel Φ be Gaussian and entanglement-breaking. We will use a Gaussian version of the proof of Theorem 11.31. Fix a nondegenerate Gaussian state σ_A in $\mathfrak{S}(\mathcal{H}_A)$ and let $\{|e_j\rangle\}_{j=1}^{+\infty}$ be the basis of eigenvectors of σ_A with the corresponding (positive) eigenvalues $\{\lambda_j\}_{j=1}^{+\infty}$. Consider the unit vector

$$|\Omega\rangle = \sum_{j=1}^{+\infty} \sqrt{\lambda_j}\,|e_j\rangle \otimes |e_j\rangle$$

in the space $\mathcal{H}_A \otimes \mathcal{H}_A$. Then $|\Omega\rangle\langle\Omega|$ is Gaussian purification of σ_A. Since Φ is entanglement-breaking, the Gaussian state

$$\sigma_{AB} = (\mathrm{Id}_A \otimes \Phi)\left[|\Omega\rangle\langle\Omega|\right] \tag{12.151}$$

in $\mathfrak{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ is separable. This implies representation (12.115), i.e.,

$$\sigma_{AB} = \int_{Z_A}\int_{Z_B} W_A(z_A)\, S_A W_A(z_A)^* \otimes W_B(z_B)\, S_B W_B(z_B)^*\, P\left(d^{2m}z_A d^{2n}z_B\right), \qquad (12.152)$$

where S_A, S_B are Gaussian states with covariance matrices α_A, α_B and P is a Gaussian probability distribution.

Taking partial trace with respect to B, this gives

$$\begin{aligned}\sigma_A &= \mathrm{Tr}_B\left(\mathrm{Id}_A \otimes \Phi\right)\left[|\Omega\rangle\langle\Omega|\right] \\ &= \int_{Z_A}\int_{Z_B} W_A(z_A)\, S_A W_A(z_A)^*\, P\left(d^{2m}z_A d^{2n}z_B\right) \\ &= \int_{Z_A}\int_{Z_B} \overline{W_A(z_A)\, S_A W_A(z_A)^*} P\left(d^{2m}z_A d^{2n}z_B\right),\end{aligned}$$

where the bar means complex conjugation in the basis of eigenvectors of σ_A. Then similarly to (11.54), we conclude that the relation

$$M_A(U) = \sigma_A^{-1/2}\left[\int_{Z_A}\int_U \overline{W_A(z_A)\, S_A W_A(z_A)^*} P\left(d^{2m}z_A d^{2n}z_B\right)\right]\sigma_A^{-1/2}$$

defines a bounded positive operator such that $M_A(U) \leq M_A(Z_B) = I_A$. It is easy to see that $M_A(U)$ is a POVM on Borel subsets $U \subseteq Z_B$.

Let us show that the representation (12.147) holds for the channel Φ with these M_A and S_B. Consider an entanglement-breaking channel

$$\hat{\Phi}[S] = \int_{Z_B} W_B(z) S_B W_B(z)^* \mu_S\left(d^{2n}z\right),$$

where $\mu_S(U) = \mathrm{Tr}\, S M_A(U), U \subseteq Z_B$. To prove $\Phi = \hat{\Phi}$, it is sufficient to show that $\hat{\Phi}\left[|e_j\rangle\langle e_k|\right] = \Phi\left[|e_j\rangle\langle e_k|\right]$ for all j, k. But

$$\begin{aligned}\hat{\Phi}\left[|e_j\rangle\langle e_k|\right] &= \int_{Z_B} W_B(z) S_B W_B(z)^* \langle e_k|\, M_A\left(d^{2n}z\right)|e_j\rangle \\ &= \lambda_j^{-1/2}\lambda_k^{-1/2}\iint_{Z_A}\langle e_j|\, W_A(z_A)\, S_A W_A(z_A)^*\, |e_k\rangle\, W_B(z_B)\, S_B W_B(z_B)^*\, P\left(d^{2m}z_A d^{2n}z_B\right) \\ &= \lambda_j^{-1/2}\lambda_k^{-1/2}\,\mathrm{Tr}_A\left(|e_k\rangle\langle e_j| \otimes I_B\right)\sigma_{AB} = \Phi\left[|e_j\rangle\langle e_k|\right]\end{aligned}$$

according to (12.151), (12.152).

It remains to show that M_A is Gaussian observable with the characteristic function (12.148) where $\alpha_A = \mu - \alpha_B$, and α_B is the covariance matrix of the state S_B; without loss of generality we can assume its mean is zero. Indeed, the density operator S_B can be modified with the help of the Weyl operators to have zero mean, resulting only in a change in the probability distribution (12.152), which however will remain Gaussian. But from (12.150),

$$\Phi^*\left[W_B(w)\right] = \exp\left[-\frac{1}{2}\alpha_B(w,w)\right]\phi_{M_A}(w)$$

for any channel Φ with the representation (12.147), whence taking into account (12.149), we indeed get (12.148) with $\alpha_A = \mu - \alpha_B$. $\square$

A necessary condition for the decomposability (12.146) and hence for the channel to be entanglement-breaking is

$$\mu \geq \frac{i}{2}\left(\Delta_B \pm K^\top \Delta_A K\right). \tag{12.153}$$

In general this condition means that for any input Gaussian state of the channel $\mathrm{Id}_A \otimes \Phi$, the output has PPT. Indeed, this channel transforms the covariance matrix of the input state according to the rule

$$\begin{bmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{bmatrix} \to \begin{bmatrix} I & 0 \\ 0 & K^\top \end{bmatrix} \begin{bmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{bmatrix} \begin{bmatrix} I & 0 \\ 0 & K \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & \alpha \end{bmatrix} \equiv \alpha_{AB}.$$

The right-hand side representing the covariance matrix of the output state satisfies

$$\begin{aligned} \alpha_{AB} &\geq \frac{i}{2}\begin{bmatrix} I & 0 \\ 0 & K^\top \end{bmatrix} \begin{bmatrix} \Delta_A & 0 \\ 0 & \Delta_A \end{bmatrix} \begin{bmatrix} I & 0 \\ 0 & K \end{bmatrix} + \frac{i}{2}\begin{bmatrix} 0 & 0 \\ 0 & \pm\Delta_B - K^\top \Delta_A K \end{bmatrix} \\ &= \frac{i}{2}\begin{bmatrix} \Delta_A & 0 \\ 0 & \pm\Delta_B \end{bmatrix}, \end{aligned}$$

where in the estimate of the second term we used (12.153) with its transpose. However, this is equivalent to the condition (12.116), which is necessary and sufficient for the output state to have PPT. Thus the condition (12.153) characterizes the class of Gaussian PPT channels which in general is larger than the class of entanglement-breaking channels.

The condition of the theorem is automatically fulfilled in the special case where

$$K^\top \Delta_A K = 0.$$

In this case the operators $R_A K$ commute, hence M_A is a sharp observable given by their spectral measure and the probability distribution $\mu_S\left(d^{2n}z\right)$ can be arbitrarily sharply peaked around any point z by appropriate choice of the state S. Hence in this case it is natural to identify Φ as $\mathrm{c}-\mathrm{q}$ channel determined by the family of states $z \to W(z) S_B W(z)^*$.

10.12.21 12.5 The Capacities of Gaussian Channels

10.12.22 12.5.1 Maximization of the Mutual Information

We start with the classical entanglement-assisted capacity which can be computed most effectively in the Gaussian case. When the state S and the channel Φ are Gaussian, the quantities $H(S), H(\Phi[S]), H(S,\Phi)$, and $I(S,\Phi)$ can be found by using formulas (12.110), (12.131), (12.118). Namely, $H(\Phi[S])$ is given by formula (12.110) with α replaced by $\alpha' = \alpha_B$ computed via (12.131). By purifying the input state and using formula (7.49), we obtain

$$H(S,\Phi) = \frac{1}{2}\,\mathrm{Spg}\left(\mathrm{abs}\left(\Delta_{12}^{-1}\alpha'_{12}\right) - \frac{I}{2}\right),$$

where the matrix

$$\alpha'_{12} = \begin{bmatrix} \alpha' & K\beta \\ \beta^\top K^\top & \alpha \end{bmatrix} \tag{12.154}$$

is computed by inserting R'_B given by (12.129) into

$$\alpha'_{12} - \frac{i}{2}\Delta'_{12} = \mathrm{Tr}\left[R'_B R_2\right]^\top S\left[R'_B R_2\right],$$

where R_2 are the (unchanged) canonical observables of the reference system. Alternatively, if an explicit description of the complementary channel $\tilde{\Phi}$ is available, the entropy exchange can be calculated as its output entropy $H(\tilde{\Phi}[S])$.

The following result greatly simplifies computation of the entanglement-assisted capacity of Gaussian channels, by reducing to the case of Gaussian input states.

Proposition 12.37. Let Φ be a Gaussian channel and S be a state with finite first and second moments. Let $\tilde{S}$ be the Gaussian channel with the same first and second moments as S. Then

$$I(S,\Phi) \leq I(\tilde{S},\Phi).$$

Proof. By using the representation (7.53) for the quantum mutual information, we can write

$$I(S,\Phi) = H(B \mid E) + H(B),$$

where B is the output of the channel and E is the environment. For a Gaussian channel first and second moments are transformed in the same way for all states in $\Sigma(m,\alpha)$. By using Lemma 12.26 we have

$$H(B) = H(\Phi[S]) \leq H(\widetilde{\Phi[S]}) = H(\Phi[\tilde{S}]) = H(\tilde{B}),$$

where $\widetilde{\Phi[S]}$ (resp. $\tilde{S}$) is the Gaussian state with the same first and second moments as $\Phi[S]$ (resp. S). The channel $S \to S_{BE} = VSV^*$, where V is the Stinespring isometry for Φ, is also Gaussian, since it is implemented by a unitary operator U_T with Gaussian state of environment, namely,

$$\operatorname{Tr} S_{BE} W(z_B) \otimes W(z_E) = \phi_A(Kz_B + Lz_E)\,\phi_D(K_D z_B + L_D z_E). \tag{12.155}$$

Therefore a similar argument based on Lemma 12.27 implies that $H(B \mid E) \leq H(\tilde{B} \mid \tilde{E})$. Thus $I(S,\Phi) \leq I(\tilde{S},\Phi)$. $\square$

This result implies that if the maximum of $I(S,\Phi)$ over a set of density operators defined by an arbitrary constraint on the first and second moments is achieved, then it is achieved on a Gaussian density operator. Now consider the energy constraint

$$\operatorname{Tr} SF \leq E, \tag{12.156}$$

where $F = R\epsilon R^\top$ is the quadratic operator with positive nondegenerate energy matrix ϵ. Note that

$$\operatorname{Tr} SF = \operatorname{Sp}(\epsilon\alpha_A) + m_A \epsilon m_A^\top,$$

where m_A is the mean vector and α_A is the covariance matrix of the state S. The expression for the entanglement-assisted classical capacity $C_{ea}(\Phi)$ given by Proposition 11.26 is the maximum of the quantum mutual information $I(S,\Phi)$ over all states S satisfying the constraint (12.156).

Corollary 12.38. The maximum of the quantum mutual information over all states S satisfying the constraint (12.156) is attained on a Gaussian state.

Proof. The set of conditions for Proposition 11.26 is fulfilled for the operator $F = R\epsilon R^\top$. Indeed, by Theorem 12.23, the operator F satisfies the condition (11.9). Taking

$$\tilde{F} = c\left[R_A R_A^\top - \left(\operatorname{Sp} K_D \alpha_D K_D^\top\right) I\right],$$

and using the input-output relation (12.129), we have $\Phi^*[\tilde{F}] = cR_B K^\top K R_B^\top$ and we can always choose positive c such that $\Phi^*[\tilde{F}] \leq F$. Moreover, $\tilde{F}$ satisfies the condition (11.9). Therefore the maximum of the quantity $I(S,\Phi)$ is achieved and formula (11.41) holds. Since the energy constraint can be expressed in terms of m_A, α_A, the maximal value $C_{ea}(\Phi,F,E)$ is achieved on the Gaussian state.

Further reduction of the maximization problem can be obtained by invoking gauge covariance.

10.12.23 12.5.2 Gauge Covariant Channels I

Consider a channel $\Phi : A \to B$. Assume that in the spaces Z_A, Z_B some operators of complex structure J_A, J_B are fixed, and let U_ϕ^A, U_ϕ^B be the unitary groups of gauge transformations in $\mathcal{H}_A, \mathcal{H}_B$ according to formula (12.77). The channel is called gauge covariant, if

$$\Phi\left[U_\phi^A S \left(U_\phi^A\right)^*\right] = U_\phi^B \Phi[S] \left(U_\phi^B\right)^* \tag{12.157}$$

for all input states S and all $\phi \in [0, 2\pi]$. In the case of a linear bosonic channel Φ, due to (12.77), (12.124), this is equivalent to the following:

$$\phi\left(\mathrm{e}^{-\varphi J_A} K z_B\right) f\left(z_B\right) = \phi\left(K \mathrm{e}^{-\varphi J_B} z_B\right) f\left(\mathrm{e}^{-\varphi J_B} z_B\right),$$

where $\phi\left(z_A\right)$ is the characteristic function of the state S. For the Gaussian channel (12.137) with parameters $(\ K, l, \mu\ )$ this reduces (cf. (12.91)) to

$$l = 0, \quad K J_B - J_A K = 0, \quad J_B^\top \mu + \mu J_B = 0 \tag{12.158}$$

By using (12.60), the last equation can be written as

$$\left[J_B, \Delta^{-1} \mu\right] = 0 \tag{12.159}$$

Channel Φ is called gauge contravariant if

$$\Phi\left[U_\phi^A S \left(U_\phi^A\right)^*\right] = \left(U_\phi^B\right)^* \Phi[S] U_\phi^B \tag{12.160}$$

for all input states S and all $\phi \in [0, 2\pi]$. For the Gaussian channel (12.137) with parameters $(\ K, l, \mu\ )$ this amounts to

$$l = 0, \quad K J_B + J_A K = 0, \quad J_B^\top \mu + \mu J_B = 0. \tag{12.161}$$

Thus, for a gauge covariant or contravariant channel, a natural choice of the complex structure in Z_B is given by any J_B, commuting with the operator $\Delta_B^{-1} \mu$. Existence of such a complex structure is proved similarly to (12.92) with the difference that the matrix μ can be degenerate.

In optimization problems with bounded mean energy a natural complex structure in Z_A is determined by the energy operator $F = R \epsilon R^\top$, namely, J_A is the operator of complex structure in Z_A, commuting with the operator $\epsilon \Delta_A$, so that

$$J_A \epsilon + \epsilon J_A^\top = 0 \tag{12.162}$$

In the case where F is the usual Hamiltonian of the oscillator system, the action of J_A reduces to multiplication by i in the complexification associated with creationannihilation operators.

Let now the Gaussian channel Φ be gauge covariant or contravariant with respect to these natural complex structures. Then

$$I\left(U_\phi^A S \left(U_\phi^A\right)^*, \Phi\right) \equiv I(S, \Phi),$$

which follows from the similar property of the three terms comprising $I(S, \Phi)$. For $H(S)$ this is simply a consequence of the unitary invariance of the entropy, for $H(\Phi[S])$ the covariance of the channel Φ is additionally used, and for $H(S, \Phi) = H(\tilde{\Phi}[S])$ this follows from covariance of the complementary channel $\tilde{\Phi}$ (Exercise 6.38). Defining the average gauge invariant state

$$S_{av} = \frac{1}{2\pi} \int_0^{2\pi} U_\phi^A S \left(U_\phi^A\right)^* d\phi$$

we have

$$\operatorname{Tr} SF = \operatorname{Sp}(\epsilon\alpha_A) + m_A\epsilon m_A^\top \geq \operatorname{Sp}(\epsilon\alpha_A) = \operatorname{Tr} S_{av}F,$$

where m_A, α_A are the first and the second moments of the state S and the last equality follows because of (12.162), i. e.,

$$\begin{aligned}\operatorname{Tr} S_{av}F &= \frac{1}{2\pi}\int_0^{2\pi} \operatorname{Tr} U_\phi^A S \left(U_\phi^A\right)^* \left(R\epsilon R^\top\right) d\phi \\ &= \frac{1}{2\pi}\int_0^{2\pi} \operatorname{Sp}\left(\mathrm{e}^{\phi J_A}\epsilon \mathrm{e}^{\phi J_A^\top}\alpha_A\right) d\phi = \operatorname{Sp}(\epsilon\alpha_A)\end{aligned}$$

Now using the concavity of the mutual information $I(S,\Phi)$, we conclude that $I(S,\Phi) \leq I(\bar{S},\Phi)$. Thus the maximum of the quantum mutual information over the set of states with bounded mean energy $\operatorname{Tr} SF \leq E$ is attained on a gauge invariant (G_A-invariant) Gaussian state. The first and the second moments of such a state necessarily satisfy the relations $m_A = 0, [J_A, \Delta^{-1}\alpha_A] = 0$. Considering the Gaussian state with these first and second moments, we finally obtain the following.

Corollary 12.39. Let Φ be a Gaussian channel which is gauge covariant or contravariant with respect to the natural complex structures J_A, J_B (where J_A is associated with the energy operator). Then the maximum of the quantum mutual information over the set of states with bounded mean energy is attained on a gauge invariant (G_A-invariant) Gaussian state.

10.12.24 12.5.3 Maximization of the Coherent Information

Consider the coherent information

$$I_c(S,\Phi) = H(\Phi[S]) - H(S,\Phi).$$

Proposition 12.40. Let Φ be a Gaussian channel which is degradable,

$$\tilde{\Phi} = \Gamma \circ \Phi, \tag{12.163}$$

such that Γ is a Gaussian channel. Then the quantum capacity

$$Q(\Phi) = \sup_{\tilde{S}} I_c(\tilde{S},\Phi),$$

where the supremum is taken over Gaussian states $\tilde{S}$. If in addition the channel is gauge covariant or contravariant, then the supremum can be taken only over gauge invariant (G_A-invariant) Gaussian states.

Proof. Assuming that the channel is degradable, i. e., (12.163) holds, where $\tilde{\Phi}$ is the complementary channel and Γ is some channel, we have (see Section 10.3.3)

$$I_c(S,\Phi) = H(E' \mid E) = H(S_{E'E}) - H(S_E), \tag{12.164}$$

where $S_{E'E} = V'S_BV'^*$ and $V' : \mathcal{H}_B \to \mathcal{H}_E \otimes \mathcal{H}_{E'}$ is the minimal Stinespring isometry for the channel Γ. Now if the channel Γ can be chosen Gaussian, then the channel $S_B \to S_{E'E}$ is also Gaussian and the argument invoking Lemma 12.27 applies. Therefore $I_c(S,\Phi) = H(E' \mid E) \leq H\left(\tilde{E}' \mid \tilde{E}\right) = I_c(\tilde{S},\Phi)$. By using Proposition 10.27 it follows that the quantum capacity of the degradable channel is given by

$$Q(\Phi) = \sup_S I_c(S,\Phi) = \sup_{\tilde{S}} I_c(\tilde{S},\Phi),$$

where the supremum is taken over Gaussian states $\tilde{S}$.

If in addition Φ is gauge covariant, then concavity of the conditional quantum entropy (12.164) implies that the supremum can be taken only over gauge invariant Gaussian states.

10.12.25 12.5.4 The Classical Capacity

The Conjectures

It is natural to consider the classical capacity of a quantum Gaussian channel Φ under the additive input constraint (11.28) with

$$F^{(n)} = F \otimes I \otimes \cdots \otimes I + \cdots + I \otimes \cdots \otimes I \otimes F,$$

where $F = R\epsilon R^\top$ is the quadratic energy operator with positive definite matrix ϵ. However finding the classical capacity $C(\Phi, F, E)$ in general depends on the solution of the problem of additivity of the constrained χ-capacity (11.33) which is still open for the Gaussian channels with quadratic input constraints. In any case, the χ-capacity $C_\chi(\Phi, F, E)$, defined by the relation (11.31), is a lower estimate for $C(\Phi, F, E)$ which coincides with $C(\Phi, F, E)$ in the case of additivity, e. g., for entanglement-breaking channels. A related open problem is additivity of the minimal output entropy (8.33) in the class of all Gaussian channels.

However even the computation of $C_\chi(\Phi, F, E)$ for Gaussian channels remains in general an open problem (except for the case of c − q channels and the channels with gauge symmetry considered in the rest of this section). At least in this situation an optimal generalized ensemble always exists, because the conditions of Corollary 11.24 for $F = R\epsilon R^\top$ are fulfilled, as was shown in Section 12.5.1. Thus the maximum of the quantity $\chi_\Phi(\pi)$ defined in (11.35) is achieved and $C_\chi(\Phi, F, E)$ is given by the relation (11.38).

Consider the following.

Hypothesis of Gaussian optimal ensembles. For a Gaussian channel Φ with the quadratic input energy constraint the maximum of the quantity $\chi_\Phi(\pi)$ in the expression (11.38) for $C_\chi(\Phi, F, E)$ is attained on the Gaussian generalized ensemble π, consisting of generalized coherent states $W(z)S_0W(z)^*$, where S_0 is a pure Gaussian state, with a Gaussian probability distribution $P\,(d^{2n}z)$.

For such an ensemble the covariance property (12.140) implies

$$H\left(\Phi\left[W(z)S_0W(z)^*\right]\right) = H\left(\Phi\left[S_0\right]\right)$$

hence

$$\chi_\Phi(\pi) = H\left(\Phi\left[\bar{S}_\pi\right]\right) - H\left(\Phi\left[S_0\right]\right) \tag{12.165}$$

where $\bar{S}_\pi$ is the average state of the ensemble, which leads us to the following.

Hypothesis of Gaussian minimizers for the output entropy. For a Gaussian channel Φ the minimum of the output entropy is attained on a (pure) Gaussian state S_0.

These two hypotheses turn out to be closely related. In what follows we describe positive solutions for both of them in an important class of Gaussian channels with the gauge symmetry. However both conjectures remain open for general quantum Gaussian channels.

Gauge Covariant Channels II

In what follows we restrict to channels that are gauge covariant or contravariant with respect to fixed complex structures. Similar to the end of Section 12.3.2, we realize a symplectic space $Z = \mathbb{R}^{2s}$ as the complex space $\mathbf{Z} = \mathbb{C}^s$ with the symplectic form

$$\Delta\left(z, z'\right) = 2\,\mathrm{Im}\,\mathbf{z}^*\mathbf{z}'.$$

An operator in Z commuting with $J = \begin{bmatrix} 0 & -I_s \\ I_s & 0 \end{bmatrix}$ is represented by a $2s \times 2s$-matrix of the form

$$M = \begin{bmatrix} X & Y \\ -Y & X \end{bmatrix}, \tag{12.166}$$

where X, Y are real $s \times s$-matrices. In the complex space $\mathbf{Z}$ the action of M is described by the action of the complex $2s \times 2s$-matrix

$$\mathbf{M} = X - iY.$$

The correspondence $M \to \mathbf{M}$ preserves algebraic operations and involution, i.e., $M^\top \to \mathbf{M}^*$. This follows from the relation

$$U^* M U = \begin{bmatrix} X - iY & 0 \\ 0 & X + iY \end{bmatrix}, \tag{12.167}$$

where U is the unitary matrix (12.99). This relation holds also for complex matrices of the form (12.166); in particular, for $i\Delta = \begin{bmatrix} 0 & iI_s \\ -iI_s & 0 \end{bmatrix}$ one obtains

$$U^*(i\Delta)U = \begin{bmatrix} I_s & 0 \\ 0 & -I_s \end{bmatrix}. \tag{12.168}$$

An important consequence of (12.167) is that for a complex matrix M of the form (12.166), nonnegative definiteness $M \geq 0$ is equivalent to $X \pm iY \geq 0$.

With these facts at hand, we pass to the consideration of Gaussian gauge co(contra)variant channels.

Let $\mathbf{Z}_A, \mathbf{Z}_B$ be the input and the output symplectic spaces. We denote by $s_A = \dim \mathbf{Z}_A, s_B = \dim \mathbf{Z}_B$ the numbers of modes of the input and the output of the channel.

The description obtained above for matrices commuting with complex structures extends with obvious changes to the case $s_A \neq s_B$ by including consideration of rectangular matrices M of the form (12.166). The action of a Gaussian gauge covariant channel is described by (12.137) where $l = 0$, and the matrices K, μ satisfy (12.158), hence they have the form (12.166). The relation (12.137) then can be rewritten as

$$\Phi^* \left[D_B(\mathbf{z}) \right] = D_A(\mathbf{K}\mathbf{z}) \exp\left(-\mathbf{z}^* \boldsymbol{\mu} \mathbf{z} \right), \quad \mathbf{z} \in \mathbf{Z}_B, \tag{12.169}$$

where $K \to \mathbf{K}$ is a complex $s_B \times s_A$-matrix, and $\mu \to \boldsymbol{\mu}$ is a Hermitian $s_B \times s_B$-matrix. The condition (12.132) turns into

$$\boldsymbol{\mu} \geq \pm \frac{1}{2} \left(\mathbf{I}_B - \mathbf{K}^* \mathbf{K} \right), \tag{12.170}$$

by the properties of the correspondence $M \to \mathbf{M}$. Here $\mathbf{I}_B$ is the unit $s_B \times s_B$-matrix which appears since $i\Delta \to \mathbf{I}$ due to the relation (12.168).

Later we will need the following.

Lemma 12.41. The channel Φ defined via (12.169) is injective if and only if ${}^2\mathbf{K}\mathbf{K}^* > \mathbf{0}$ (in which case necessarily $s_B \geq s_A$).

Proof. Injectivity means that $\Phi\left[S_1\right] = \Phi\left[S_2\right]$ implies $S_1 = S_2$. But $\Phi\left[S_1\right] = \Phi\left[S_2\right]$ is equivalent to $\operatorname{Tr} S_1 \Phi^* \left[D_B(\mathbf{z})\right] = \operatorname{Tr} S_2 \Phi^* \left[D_B(\mathbf{z})\right]$, i. e., $\operatorname{Tr} S_1 D_A(\mathbf{K}\mathbf{z}) = \operatorname{Tr} S_2 D_A(\mathbf{K}\mathbf{z})$ for all $\mathbf{z} \in \mathbf{Z}_B$. By irreducibility of the Weyl system, this property is equivalent to $\operatorname{Ran} \mathbf{K} = \mathbf{Z}_A$, i. e., $\operatorname{Ker} \mathbf{K}^* = \{\mathbf{0}\}$ or $\mathbf{K}\mathbf{K}^* > 0$. $\square$

The channel (12.169) is extreme [3] if μ is a minimal solution of inequality (12.170). Special cases of the maps (12.169) are provided by the attenuator and amplifier channels, characterized

by matrix $\mathbf{K}$ fulfilling the inequalities $\mathbf{K}^*\mathbf{K} \leq \mathbf{I}$ and $\mathbf{K}^*\mathbf{K} \geq \mathbf{I}$, respectively. We are particularly interested in the extreme attenuator which corresponds to

$$\mathbf{K}^*\mathbf{K} \leq \mathbf{I}_B, \quad \boldsymbol{\mu} = \frac{1}{2}\left(\mathbf{I}_B - \mathbf{K}^*\mathbf{K}\right) \tag{12.171}$$

and the extreme amplifier

$$\mathbf{K}^*\mathbf{K} \geq \mathbf{I}_B, \quad \boldsymbol{\mu} = \frac{1}{2}\left(\mathbf{K}^*\mathbf{K} - \mathbf{I}_B\right). \tag{12.172}$$

In the case of a contravariant channel the parameters satisfy (12.161), in particular, K anticommutes with J. Let $\Lambda = \begin{bmatrix} I_s & 0 \\ 0 & -I_s \end{bmatrix}$, so that Λz corresponds to $\overline{\mathbf{z}}$ - the column vector obtained by taking the complex conjugates of the elements of $\mathbf{z}$. One has $\Lambda^2 = I_{2s}$,

$\Lambda J + J\Lambda = 0$. Then $K = \Lambda K_1$, where $K_1 = \Lambda K$ commutes with J. The action of the Gaussian gauge contravariant channel (12.137) is then described as

$$\Phi^*\left[D_B(\mathbf{z})\right] = D_A\left(-\overline{\mathbf{K}_1\mathbf{z}}\right)\exp\left(-\mathbf{z}^*\boldsymbol{\mu}\mathbf{z}\right). \tag{12.173}$$

The condition (12.132) takes the form

$$\mu \geq \pm\frac{i}{2}\left(\Delta_B + K_1^\top \Delta_A K_1\right),$$

which reduces to

$$\boldsymbol{\mu} \geq \frac{1}{2}\left(\mathbf{I}_B + \mathbf{K}_1^*\mathbf{K}_1\right). \tag{12.174}$$

These maps are extreme if

$$\boldsymbol{\mu} = \frac{1}{2}\left(\mathbf{I}_B + \mathbf{K}_1^*\mathbf{K}_1\right). \tag{12.175}$$

In what follows, we will use the notation $\mathbf{K}$ instead of $\mathbf{K}_1$.

The Structure of Gauge Covariant Channels

Proposition 12.42. Any Gaussian gauge covariant channel $\Phi : A \to B$ is a concatenation $\Phi = \Phi_2 \circ \Phi_1$ of an extreme attenuator $\Phi_1 : A \to B$ and an extreme amplifier $\Phi_2 : B \to B$.

Any Gaussian gauge contravariant channel $\Phi : A \to B$ is a concatenation of an extreme attenuator $\Phi_1 : A \to B$ and an extreme gauge contravariant channel $\Phi_2 : B \to B$.

Proof. The concatenation $\Phi = \Phi_2 \circ \Phi_1$ of Gaussian gauge covariant channels Φ_1 and Φ_2 obeys the following rule:

$$\mathbf{K} = \mathbf{K}_1\mathbf{K}_2, \tag{12.176}$$
$$\boldsymbol{\mu} = \mathbf{K}_2^*\boldsymbol{\mu}_1\mathbf{K}_2 + \boldsymbol{\mu}_2. \tag{12.177}$$

By inserting relations

$$\boldsymbol{\mu}_1 = \frac{1}{2}\left(\mathbf{I}_B - \mathbf{K}_1^*\mathbf{K}_1\right) = \frac{1}{2}\left(\mathbf{I}_B - |\mathbf{K}|_1^2\right), \quad \boldsymbol{\mu}_2 = \frac{1}{2}\left(\mathbf{K}_2^*\mathbf{K}_2 - \mathbf{I}_B\right) = \frac{1}{2}\left(|\mathbf{K}_2|^2 - \mathbf{I}_B\right)$$

[0]2 For Hermitian matrices M, N, the strict inequality $M > N$ means that $M - N$ is positive definite.
3 In physical literature such channels are called quantum-limited.

into (12.177) and using (12.176) we obtain

$$|\mathbf{K}_2|^2 = \mathbf{K}_2^*\mathbf{K}_2 = \boldsymbol{\mu} + \frac{1}{2}\left(\mathbf{K}^*\mathbf{K} + \mathbf{I}_B\right) \geq \left\{ \begin{array}{l} \mathbf{I}_B \\ \mathbf{K}^*\mathbf{K} \end{array} \right. \tag{12.178}$$

from inequality (12.170). By using operator monotonicity of the square root (see, e. g., [31], Section V.1), we have

$$|\mathbf{K}_2| \geq \mathbf{I}_B, \quad |\mathbf{K}_2| \geq |\mathbf{K}|.$$

The first inequality (12.178) implies that choosing

$$\mathbf{K}_2 = |\mathbf{K}_2| = \sqrt{\boldsymbol{\mu} + \frac{1}{2}\left(\mathbf{K}^*\mathbf{K} + \mathbf{I}_B\right)} \tag{12.179}$$

and the corresponding $\boldsymbol{\mu}_2 = \frac{1}{2}\left(|\mathbf{K}_2|^2 - \mathbf{I}_B\right)$, we obtain the extreme amplifier $\Phi_2 : B \to B$. Then with

$$\mathbf{K}_1 = \mathbf{K}\,|\mathbf{K}_2|^{-1} \tag{12.180}$$

we obtain, taking into account the second inequality in (12.178) and Lemma 12.43,

$$\mathbf{K}_1\mathbf{K}_1^* = \mathbf{K}\,|\mathbf{K}_2|^{-2}\,\mathbf{K}^* = \mathbf{K}\left[\boldsymbol{\mu} + \frac{1}{2}\left(\mathbf{K}^*\mathbf{K} + \mathbf{I}_B\right)\right]^{-1}\mathbf{K}^* \leq \mathbf{I}_A \tag{12.181}$$

which implies $\mathbf{K}_1^*\mathbf{K}_1 \leq \mathbf{I}_B$, hence $\mathbf{K}_1$ with the corresponding $\boldsymbol{\mu}_1 = \frac{1}{2}\left(\mathbf{I}_B - \mathbf{K}_1^*\mathbf{K}_1\right)$ give the extreme attenuator.

Lemma 12.43. Let $\mathbf{M} \geq \mathbf{K}^*\mathbf{K}$. Then $\mathbf{K}\mathbf{M}^{-}\mathbf{K}^* \leq \mathbf{I}_A$, where $^-$means (generalized) inverse.
Proof. By the definition of the generalized inverse,

$$u^*\mathbf{M}^{-}u = \sup_{v \in \operatorname{Ran}\mathbf{M}, v \neq 0} \frac{|u^*v|^2}{v^*\mathbf{M}v}$$

By inserting $\mathbf{K}^*u$ in place of u and using the Cauchy-Schwarz inequality in the numerator of the fraction, we obtain

$$u^*\mathbf{K}\mathbf{M}^{-}\mathbf{K}^*u \leq u^*u \sup_{v \in \operatorname{Ran}\mathbf{M}, v \neq 0} \frac{v^*\mathbf{K}^*\mathbf{K}v}{v^*\mathbf{M}v} \leq u^*u$$

In the case of a contravariant channel the relations (12.176), (12.177) are replaced with

$$\overline{\mathbf{K}} = \mathbf{K}_1\overline{\mathbf{K}}_2, \tag{12.182}$$

$$\boldsymbol{\mu} = \mathbf{K}_2^*\overline{\boldsymbol{\mu}}_1\mathbf{K}_2 + \boldsymbol{\mu}_2. \tag{12.183}$$

By substituting

$$\boldsymbol{\mu}_1 = \frac{1}{2}\left(\mathbf{I} - \mathbf{K}_1^*\mathbf{K}_1\right), \quad \mu_2 = \frac{1}{2}\left(\mathbf{K}_2^*\mathbf{K}_2 + \mathbf{I}_B\right)$$

into (12.183) and using (12.174) we obtain

$$|\mathbf{K}_2|^2 = \mathbf{K}_2^*\mathbf{K}_2 = \boldsymbol{\mu} + \frac{1}{2}\left(\mathbf{K}^*\mathbf{K} - \mathbf{I}_B\right) \geq \mathbf{K}^*\mathbf{K} \tag{12.184}$$

Taking $\mathbf{K}_2 = |\mathbf{K}_2|, \boldsymbol{\mu}_2 = \frac{1}{2}\left(|\mathbf{K}_2|^2 + \mathbf{I}_B\right)$ gives the extreme gauge contravariant channel $\Phi_2 : B \to B$. With

$$\overline{\mathbf{K}}_1 = \mathbf{K}\,|\mathbf{K}_2|^- \tag{12.185}$$

we obtain, by using Lemma 12.43,

$$\begin{aligned}\overline{\mathbf{K}}_1\overline{\mathbf{K}}_1^* &= \mathbf{K}\left(|\mathbf{K}_2|^-\right)^2\mathbf{K}^* \\ &= \mathbf{K}\left[\boldsymbol{\mu} + \frac{1}{2}\left(\mathbf{K}^*\mathbf{K} - \mathbf{I}_B\right)\right]^-\mathbf{K}^* \leq \mathbf{I}_A,\end{aligned} \tag{12.186}$$

which implies $\mathbf{K}_1\mathbf{K}_1^* \leq \mathbf{I}_A$, so $\mathbf{K}_1$ and the corresponding $\boldsymbol{\mu}_1$ define the extreme attenuator $\Phi_1 : A \to B$. $\square$

Remark 12.44. In the case of a gauge covariant channel, the equality in (12.181) shows that $\mathbf{K}\mathbf{K}^* > 0$ implies $\mathbf{K}_1\mathbf{K}_1^* > 0$, while the inequality $\boldsymbol{\mu} > \frac{1}{2}\left(\mathbf{K}^*\mathbf{K} - \mathbf{I}_B\right)$ implies $\mathbf{K}_1\mathbf{K}_1^* < \mathbf{I}_A$. In the case of a gauge contravariant channel, the inequality $\boldsymbol{\mu} > \frac{1}{2}\left(\mathbf{I}_B + \mathbf{K}^*\mathbf{K}\right)$ implies $0 < \mathbf{K}_1\mathbf{K}_1^* < \mathbf{I}_A$ via (12.186).

Special Properties of Attenuators and Amplifiers

In this subsection we will establish several properties which will be used in the proof of the main theorem, Theorem 12.52.

Proposition 12.45. The extreme attenuator with matrix $\mathbf{K}$ and the extreme attenuator with matrix $\widetilde{\mathbf{K}} = \sqrt{\mathbf{I}_A - \mathbf{K}\mathbf{K}^*}$ are mutually complementary.

The extreme amplifier with matrix $\mathbf{K}$ and the extreme gauge contravariant channel with matrix $\widetilde{\mathbf{K}} = \sqrt{\overline{\mathbf{K}\mathbf{K}}^* - \mathbf{I}_A}$ are mutually complementary.

Proof. For the simple case of one mode, see Section 12.6.1. Below we sketch the proof for several modes, based on Remark 12.31. Namely, assume that there is a composite quantum system $AD = BE$ in the Hilbert space

$$\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_D \simeq \mathcal{H}_B \otimes \mathcal{H}_E,$$

which is initially prepared in the state $S_A \otimes S_D$ and then evolves according to the unitary operator U. Then the output state S_B depending on the input state $S_A = S$ is

$$\Phi_B[S] = \mathrm{Tr}_E\, U\left(S \otimes S_D\right)U^*, \tag{12.187}$$

while the output state of the "environment" E is the output of the channel

$$\Phi_E[S] = \mathrm{Tr}_B\, U\left(S \otimes S_D\right)U^*. \tag{12.188}$$

We will occasionally use the notation $P_\psi = |\psi\rangle\langle\psi|$ for a density operator of pure state ($|\psi\rangle$ is a unit vector). If the initial state of D is pure, i. e., $S_D = P_{\psi_D}$, then by introducing the isometry $V : \mathcal{H}_A \to \mathcal{H}_B \otimes \mathcal{H}_D$, which acts as

$$V\psi = U\left(\psi \otimes \psi_D\right), \quad \psi \in \mathcal{H}_A,$$

we see that the relations (12.187), (12.188) convert into (6.38), and Φ_E is just the complementary of Φ_B.

Now, define $\mathbf{Z}_E \simeq \mathbf{Z}_A, \mathbf{Z}_D \simeq \mathbf{Z}_B$, so that $\mathbf{Z} = \mathbf{Z}_A \oplus \mathbf{Z}_D \simeq \mathbf{Z}_B \oplus \mathbf{Z}_E$.
In the case of an attenuator, consider the block unitary matrix in $\mathbf{Z}$,

$$\mathbf{V} = \begin{bmatrix} \mathbf{K} & \sqrt{\mathbf{I}_A - \mathbf{K}\mathbf{K}^*} \\ \sqrt{\mathbf{I}_B - \mathbf{K}^*\mathbf{K}} & -\mathbf{K}^* \end{bmatrix}, \tag{12.189}$$

which defines unitary dynamics U in $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_D \simeq \mathcal{H}_B \otimes \mathcal{H}_E$ by the relation $U^* D_{BE}(\mathbf{z}_{BE}) U = D_{AD}(\mathbf{V}\mathbf{z}_{BE})$. Here $\mathbf{z}_{BE} = [\mathbf{z}_B \mathbf{z}_E]^\top$, $D_{BE}(\mathbf{z}_{BE}) = D_B(\mathbf{z}_B) \otimes D_E(\mathbf{z}_E)$, and unitarity follows from the relation

$$\mathbf{K}\sqrt{\mathbf{I}_B - \mathbf{K}^*\mathbf{K}} = \sqrt{\mathbf{I}_A - \mathbf{K}\mathbf{K}^*}\mathbf{K} \tag{12.190}$$

(In general, $\mathbf{K} f(\mathbf{K}^*\mathbf{K}) = f(\mathbf{K}\mathbf{K}^*)\mathbf{K}$ for any polynomial f, and this can be extended to a continuous function f via standard approximation.)

Let $S_D = S_0$ be the vacuum state, and let $S_A = S$ an arbitrary state. Then formulas (12.187), (12.188) define the mutually complementary extreme attenuators as described in the first statement. The proof is obtained by computing the characteristic function of the output states for the channels. For the state of the composite system $S_{BE} = U(S \otimes S_D)U^*$ we have

$$\begin{aligned}
\phi_{BE}(\mathbf{z}_{BE}) &= \operatorname{Tr} U(S \otimes S_D) U^* [D_B(\mathbf{z}_B) \otimes D_E(\mathbf{z}_E)] \\
&= \operatorname{Tr} (S \otimes S_D) U^* [D_B(\mathbf{z}_B) \otimes D_E(\mathbf{z}_E)] U \\
&= \operatorname{Tr} (S \otimes S_D) \left[D_A\left(\mathbf{K}\mathbf{z}_B + \widetilde{\mathbf{K}}\mathbf{z}_E\right) \otimes D_D\left(\sqrt{\mathbf{I}_B - \mathbf{K}^*\mathbf{K}}\mathbf{z}_B - \mathbf{K}^*\mathbf{z}_E\right)\right] \\
&= \phi_A\left(\mathbf{K}\mathbf{z}_B + \widetilde{\mathbf{K}}\mathbf{z}_E\right) \exp\left[-\frac{1}{2}\left|\sqrt{\mathbf{I}_B - \mathbf{K}^*\mathbf{K}}\mathbf{z}_B - \mathbf{K}^*\mathbf{z}_E\right|^2\right].
\end{aligned} \tag{12.191}$$

By setting $\mathbf{z}_E = 0$ or $\mathbf{z}_B = 0$ we obtain

$$\begin{aligned}
\phi_B(\mathbf{z}_B) &= \phi_A(\mathbf{K}\mathbf{z}_B) \exp\left[-\frac{1}{2}\mathbf{z}_B^*(\mathbf{I}_B - \mathbf{K}^*\mathbf{K})\mathbf{z}_B\right] \\
\phi_E(\mathbf{z}_E) &= \phi_A\left(\widetilde{\mathbf{K}}\mathbf{z}_E\right) \exp\left[-\frac{1}{2}\mathbf{z}_E^*\mathbf{K}\mathbf{K}^*\mathbf{z}_E\right]
\end{aligned}$$

as required.

In the case of an amplifier, set

$$\mathbf{V} = \begin{bmatrix} \mathbf{K} & -\sqrt{\mathbf{K}\mathbf{K}^* - \mathbf{I}_A}\Lambda_A \\ -\Lambda_B\sqrt{\mathbf{K}^*\mathbf{K} - \mathbf{I}_B} & \Lambda_B\mathbf{K}^*\Lambda_A \end{bmatrix}$$

where Λ is the operator of complex conjugation in the corresponding complex subspace, anticommuting with multiplication by i. By using the property $\Delta(\Lambda z, \Lambda z') = -\Delta(z, z')$, we obtain that $\mathbf{V}$ corresponds to a symplectic transformation in $\mathbf{Z}$ generating unitary dynamics U in $\mathcal{H}$.

Exercise 12.46 Check the identity

$$\Delta_{BE}(\mathbf{V}\mathbf{z}_{BE}, \mathbf{V}\mathbf{z}'_{BE}) = \Delta_{BE}(\mathbf{z}_{BE}, \mathbf{z}'_{BE}),$$

where

$$\Delta_{BE}(\mathbf{z}_{BE}, \mathbf{z}'_{BE}) \equiv \Delta_B(z_B, z'_B) + \Delta_E(z_E, z'_E).$$

Let again $S_D = S_0$ be the vacuum state of the environment. Then formulas (12.187), (12.188) define the mutually complementary channels as described in the second statement of the proposition, and the proof is similar. □

In general, we will say that two density operators S and $\widetilde{S}$ (possibly acting in different Hilbert spaces) are isometrically equivalent if there is a partial isometry W such that $S = W\widetilde{S}W^*, \widetilde{S} = W^*SW$. Apparently, this is the case if and only if nonzero spectra (counting multiplicity) of the density operators S and $\widetilde{S}$ coincide. We denote this fact with the notation $S \sim \widetilde{S}$.

Lemma 12.47. Let $\Phi, \widetilde{\Phi}$ be mutually complementary channels. Then $\Phi[P_\psi] \sim \widetilde{\Phi}[P_\psi]$ for all $\psi \in \mathcal{H}_A$.

Proof. Let $V : \mathcal{H}_A \to \mathcal{H}_B \otimes \mathcal{H}_E$ be the isometry from the representations of complementary channels (6.38). Then $S_{BE} = VP_\psi V^*$ is a pure state in $\mathcal{H}_B \otimes \mathcal{H}_E$, and the statement follows from Theorem 3.10 (the "Schmidt decomposition"): if S_{BE} is a pure state in $\mathcal{H}_B \otimes \mathcal{H}_E$ and $S_B = \operatorname{Tr}_E S_{BE}, S_E = \operatorname{Tr}_B S_{BE}$ are its partial states, then S_B, S_E have identical nonzero eigenvalues, i. e., $S_B \sim S_E$. $\square$

Lemma 12.48. Let $\Phi_1 : A \to B$ be an extreme attenuator with $\mathbf{0} < \mathbf{K}_1\mathbf{K}_1^* < \mathbf{I}_A$. Then $\Phi_1[P_\psi] = P_{\psi'}$ (a pure state) if and only if P_ψ is a coherent state.

Proof. According to Proposition 12.45, the complementary channel $\widetilde{\Phi}_1$ is an extreme attenuator with the matrix $\widetilde{\mathbf{K}} = \sqrt{\mathbf{I}_A - \mathbf{K}_1\mathbf{K}_1^*}$, such that $\mathbf{0} < \widetilde{\mathbf{K}} < \mathbf{I}_A$. Its output is also pure, $\widetilde{\Phi}_1[P_\psi] = P_{\psi'_E}$, as the outputs of complementary channels have identical nonzero spectra by Lemma 12.47. Thus

$$U(\psi \otimes \psi_0) = \psi' \otimes \psi'_E,$$

where $\psi_0 \in \mathcal{H}_D$ is the vacuum vector and U is the unitary operator in $\mathcal{H}$ implementing the symplectic transformation corresponding to the unitary (12.189) in $\mathbf{Z}_A \oplus \mathbf{Z}_D \simeq \mathbf{Z}_B \oplus \mathbf{Z}_E$, with $\mathbf{Z}_D \simeq \mathbf{Z}_B, \mathbf{Z}_E \simeq \mathbf{Z}_A$. Denoting by

$$\phi(\mathbf{z}) = \operatorname{Tr} P_\psi D_A(\mathbf{z}), \quad \phi'(\mathbf{z}_B) = \operatorname{Tr} P_{\psi'} D_B(\mathbf{z}_B), \quad \phi_E(\mathbf{z}_E) = \operatorname{Tr} P_{\psi'_E} D_E(\mathbf{z}_E)$$

the quantum characteristic functions and using the relation (12.191), we have the functional equation

$$\phi'(\mathbf{z}_B)\,\phi_E(\mathbf{z}_E) = \phi\left(\mathbf{K}_1\mathbf{z}_B + \widetilde{\mathbf{K}}\mathbf{z}_E\right) \exp\left[-\frac{1}{2}\left|\sqrt{\mathbf{I}_B - \mathbf{K}_1^*\mathbf{K}_1}\mathbf{z}_B - \mathbf{K}_1^*\mathbf{z}_E\right|^2\right]. \tag{12.192}$$

By letting $\mathbf{z}_E = 0$ or $\mathbf{z}_B = 0$, we obtain, respectively,

$$\phi'(\mathbf{z}_B) = \phi(\mathbf{K}_1\mathbf{z}_B) \exp\left[-\frac{1}{2}\left|\sqrt{\mathbf{I}_B - \mathbf{K}_1^*\mathbf{K}_1}\mathbf{z}_B\right|^2\right],$$
$$\phi_E(\mathbf{z}_E) = \phi\left(\widetilde{\mathbf{K}}\mathbf{z}_E\right) \exp\left[-\frac{1}{2}\left|\mathbf{K}_1^*\mathbf{z}_E\right|^2\right],$$

thus, after the change of variables $\mathbf{z} = \mathbf{K}_1\mathbf{z}_B, \mathbf{z}' = \widetilde{\mathbf{K}}\mathbf{z}_E$, and using (12.190), equation (12.192) reduces to

$$\phi(\mathbf{z})\phi(\mathbf{z}') = \phi(\mathbf{z} + \mathbf{z}') \exp[\operatorname{Re} \mathbf{z}^*\mathbf{z}']$$

The condition of the lemma ensures that $\operatorname{Ran} \mathbf{K}_1 = \operatorname{Ran} \widetilde{\mathbf{K}} = \mathbf{Z}_A$. Substituting $\omega(\mathbf{z}) = \phi(\mathbf{z}) \exp\left[\frac{1}{2}|\mathbf{z}|^2\right]$, the last equation becomes

$$\omega(\mathbf{z})\omega(\mathbf{z}') = \omega(\mathbf{z} + \mathbf{z}') \tag{12.193}$$

for all $\mathbf{z}, \mathbf{z}' \in \mathbf{Z}_A$. The function $\omega(\mathbf{z})$, as well as the characteristic function $\phi(\mathbf{z})$, is continuous and satisfies $\omega(-\mathbf{z}) = \overline{\omega(\mathbf{z})}$. The only solution of (12.193) satisfying these conditions is the exponent $\omega(\mathbf{z}) = \exp[i \operatorname{Im} \mathbf{w}^*\mathbf{z}]$ for some complex $\mathbf{w}$. Thus

$$\phi(\mathbf{z}) = \exp\left[i \operatorname{Im} \mathbf{w}^*\mathbf{z} - \frac{1}{2}|\mathbf{z}|^2\right]$$

is the characteristic function of the coherent state $S_{\mathbf{w}/2}$.
For a natural number n we denote by $\mathfrak{L}_n$ the finite-dimensional subspace spanned by the eigenvectors of the total number operator

$$\mathcal{N} = \sum_{j=1}^{s} a_j^\dagger a_j$$

corresponding to all its eigenvalues $\leq n$. We also denote by $\mathfrak{P}_n$ the subspace of finiterank Hermitian operators supported by $\mathfrak{L}_n$.

Lemma 12.49. An extreme attenuator $\Phi : A \to A$ leaves the subspace $\mathfrak{P}_n$ invariant.
Proof. (sketch) We will consider the case $s = 1$, which clearly demonstrates the idea of the proof avoiding somewhat cumbersome multiindex notations. The operators $S \in \mathfrak{P}_n$ can be characterized by the equation $a^{n+1}S = 0$, where a is the annihilation operator of the mode. By using Lemma 5.4.3 in [122] we obtain the characteristic function of the operator aS, i.e.,

$$\phi_{aS}(z) = \mathrm{e}^{-|z|^2/2} \left(\frac{d}{dz}\right) \mathrm{e}^{|z|^2/2} \phi_S(z)$$

where $\frac{d}{dz} = \frac{1}{\sqrt{2}} \left(\frac{d}{dx} - i\frac{d}{dy}\right)$. Thus $S \in \mathfrak{P}_n$ is equivalent to the fact that $\mathrm{e}^{|z|^2/2}\phi_S(z)$ is a polynomial in z of the degree $\leq n$. By using the equation of the extreme attenuator

$$\Phi^*[D(z)] = D(kz) \exp\left(-\frac{1-k^2}{2}|z|^2\right), \quad 0 < k < 1,$$

we obtain

$$\mathrm{e}^{|z|^2/2}\phi_{\Phi[S]}(z) = \mathrm{e}^{|kz|^2/2}\phi_S(kz).$$

Thus, if $S \in \mathfrak{P}_n$, then $\mathrm{e}^{|z|^2/2}\phi_S(z)$ is a polynomial in z of the degree $\leq n$, and the righthand side of this equality and hence also the left-hand side are as well. □

Gaussian Optimizers

Denote by $\mathfrak{F}$ the class of real concave functions f on $[0, 1]$, such that $f(0) = 0$. For any $f \in \mathfrak{F}$ and for any density operator S we can consider the quantity

$$\operatorname{Tr} f(S) = \sum_j f(\lambda_j),$$

where λ_j are the (nonzero) eigenvalues of the density operator S, counting multiplicity. Note that this quantity is defined unambiguously with values in $(-\infty, \infty]$. This follows from the fact that $f(x) \geq cx$, where $c = f(1)$, hence $\operatorname{Tr} f(S) \geq c \operatorname{Tr} S = c$. We also will use the fact that the functional $S \to \operatorname{Tr} f(S)$ is (strictly) concave on $\mathfrak{S}(\mathcal{H})$ if f is (strictly) concave (see, e. g., [40]).

Denote by $\lambda_j^\downarrow(S)$ the eigenvalues of a density operator S, counting multiplicity, arranged in nonincreasing order. One says that the density operator S majorizes the density operator S' if

$$\sum_{j=1}^{k} \lambda_j^\downarrow(S) \geq \sum_{j=1}^{k} \lambda_j^\downarrow(S'), \quad k = 1, 2, \ldots$$

A consequence of a well-known result (see, e. g., [40]) is that this is the case if and only if $\operatorname{Tr} f(S) \leq \operatorname{Tr} f(S')$ for all $f \in \mathfrak{F}$.

Moreover, the functional $\operatorname{Tr} f(S)$ is lower semicontinuous in the trace norm distance. In fact, for arbitrary concave f on $[0, 1]$ there is a monotonously nondecreasing sequence of

concave polygonal functions f_m converging to f pointwise. Any such function is Lipschitz, $|f_m(x) - f_m(y)| \le x_m|x-y|$, hence the corresponding functional $\operatorname{Tr} f_m(S)$ is continuous.

Lemma 12.50. Let $|f(x) - f(y)| \le x|x-y|$ for $x, y \in [0,1]$. Then for any density operators S, S'

$$|\operatorname{Tr} f(S') - \operatorname{Tr} f(S)| \le \varkappa \|S' - S\|_1 .$$

Proof. Let $\lambda_1 \ge \lambda_2 \ge \cdots (\mu_1 \ge \mu_2 \ge \cdots)$ be the eigenvalues of S' (correspondingly, S). By Mirsky's theorem (Lemma IV.3.2 in [31])

$$\sum_i |\lambda_i - \mu_i| \le \|S' - S\|_1 .$$

Therefore

$$|\operatorname{Tr} f(S') - \operatorname{Tr} f(S)| \le \sum_i |f(\lambda_i) - f(\mu_i)| \le \varkappa \sum_i |\lambda_i - \mu_i| \le \varkappa \|S' - S\|_1 .$$

□

Then $\operatorname{Tr} f(S)$ is a pointwise limit of monotonously nondecreasing sequence of continuous functionals $\operatorname{Tr} f_m(S)$ and hence is lower semicontinuous. Thus the Jensen inequality

$$\operatorname{Tr} f\left(\sum_j p_j S_j\right) \ge \sum_j p_j \operatorname{Tr} f(S_j) \tag{12.194}$$

holds not only for finite but also for countable convex decompositions.

For a quantum channel Φ we introduce the quantity

$$\check{f}(\Phi) = \inf_{S \in \mathfrak{S}(\mathcal{H})} \operatorname{Tr} f(\Phi[S]) = \inf_{P_\psi \in \mathfrak{P}(\mathcal{H})} \operatorname{Tr} f(\Phi[P_\psi]) , \tag{12.195}$$

where the second equality follows from the concavity of the functional $S \to \operatorname{Tr} f(\Phi[S])$ on the convex set $\mathfrak{S}(\mathcal{H})$. Moreover, for strictly concave f, any minimizer is of the form P_ψ for some vector $\psi \in \mathcal{H}$.

In particular, taking $f(x) = -x \log x$ we obtain $\check{f}(\Phi) = \check{H}(\Phi)$.

Lemma 12.51. If $\Phi, \widetilde{\Phi}$ are complementary channels, then $\check{f}(\Phi) = \check{f}(\widetilde{\Phi})$.

Proof. From Lemma 12.47, $\Phi[P_\psi]$ and $\widetilde{\Phi}[P_\psi]$ have identical nonzero spectra ($\Phi[P_\psi] \sim \widetilde{\Phi}[P_\psi]$). Then

$$\operatorname{Tr} f(\Phi[P_\psi]) = \operatorname{Tr} f\left(\widetilde{\Phi}[P_\psi]\right) \tag{12.196}$$

since $f(0) = 0$. The second equality in (12.195) implies $\check{f}(\Phi) = \check{f}(\widetilde{\Phi})$. □

Theorem 12.52. (i) Let Φ be a gauge covariant or contravariant channel and let f be a real concave function on $[0,1]$, such that $f(0) = 0$. Then

$$\operatorname{Tr} f(\Phi[S]) \ge \operatorname{Tr} f(\Phi[S_{\mathbf{w}}]) = \operatorname{Tr} f(\Phi[S_0]) \tag{12.197}$$

for all states S and any coherent state $S_{\mathbf{w}}$ (the value on the right is the same for all coherent states by the unitary covariance property of a Gaussian channel (12.140)).

(ii) Let f be strictly concave. Then equality in (12.197) is attained only if S is a coherent state in the following cases:

(a) $s_B = s_A$ and Φ is an extreme amplifier with $\boldsymbol{\mu} = \frac{1}{2}(\mathbf{K}^*\mathbf{K} - \mathbf{I}_B) > 0$;

(b) $s_B \ge s_A$, the channel Φ is gauge covariant with $\mathbf{K}\mathbf{K}^* > 0$, and

$$\boldsymbol{\mu} > \frac{1}{2}(\mathbf{K}^*\mathbf{K} - \mathbf{I}_B) ; \tag{12.198}$$

(c) $s_B \geq s_A$, the channel Φ is gauge contravariant with $\mathbf{K}\mathbf{K}^* > 0$, and $\boldsymbol{\mu} > \frac{1}{2}(\mathbf{I}_B + \mathbf{K}^*\mathbf{K})$.

Proof. (i) We first prove inequality (12.197) for strictly concave f. Then the inequality for arbitrary concave f follows by the monotone approximation $f(x) = \lim_{\varepsilon \downarrow 0} f_\varepsilon(x)$, since $f_\varepsilon(x) = f(x) - \varepsilon x^2$ are strictly concave. Also, by concavity, it is sufficient to prove (12.197) only for $S = P_\psi$.

By Proposition 12.42, $\Phi = \Phi_2 \circ \Phi_1$, where $\Phi_1 : A \to B$ is an extreme attenuator and $\Phi_2 : B \to B$ is either an extreme amplifier or an extreme gauge contravariant channel. Any extreme attenuator maps a vacuum state into vacuum. Indeed,

$$\begin{aligned}\operatorname{Tr}\Phi_1[S_0]\, D_B(\mathbf{z}) &= \operatorname{Tr} S_0 \Phi_1^*[D_B(\mathbf{z})] \\ &= \operatorname{Tr} S_0 D_A(\mathbf{K}\mathbf{z}) \exp\left(-\frac{1}{2}\mathbf{z}^*(\mathbf{I}_B - \mathbf{K}^*\mathbf{K})\,\mathbf{z}\right) \\ &= \exp\left(-\frac{1}{2}|\mathbf{z}|^2\right) = \operatorname{Tr} S_0 D_B(\mathbf{z})\end{aligned}$$

and therefore, $\operatorname{Tr} f(\Phi[S_0]) = \operatorname{Tr} f(\Phi_2[S_0])$. Then it is sufficient to prove (12.197) for all extreme amplifiers and all extreme gauge contravariant channels Φ_2. Indeed, assume that we have proved

$$\operatorname{Tr} f(\Phi_2[P_\psi]) \geq \operatorname{Tr} f(\Phi_2[S_0]) \tag{12.199}$$

for any state vector ψ. Consider the spectral decomposition $\Phi_1[P_\psi] = \sum_j p_j P_{\phi_j}$, where $p_j > 0$. Then

$$\begin{aligned}\operatorname{Tr} f(\Phi[P_\psi]) &= \operatorname{Tr} f(\Phi_2[\Phi_1[P_\psi]]) && (12.200)\\ &\geq \sum_j p_j \operatorname{Tr} f\left(\Phi_2\left[P_{\phi_j}\right]\right) && (12.201)\\ &\geq \operatorname{Tr} f(\Phi_2[S_0]) && (12.202)\\ &= \operatorname{Tr} f(\Phi_2[\Phi_1[S_0]]) = \operatorname{Tr} f(\Phi[S_0]) && (12.203)\end{aligned}$$

Then, according to the second statement of Proposition 12.45 and Lemma 12.47,

$$\operatorname{Tr} f(\Phi_2[P_\psi]) = \operatorname{Tr} f\left(\widetilde{\Phi}_2[P_\psi]\right),$$

where Φ_2 is an extreme amplifier and $\widetilde{\Phi}_2$ is an extreme gauge contravariant channel. Thus it is sufficient to prove (12.199) only for an extreme amplifier $\Phi_2 : B \to B$, with Hermitian matrix $\mathbf{K}_2 \geq \mathbf{I}_B$.

Lemma 12.53. For an extreme amplifier $\Phi_2 : B \to B$, with matrix $\mathbf{K}_2 \geq \mathbf{I}_B$, there is an extreme attenuator Φ_1' such that for all $\psi \in \mathcal{H}_B$

$$\Phi_2(P_\psi) \sim (\Phi_2 \circ \Phi_1')(P_\psi). \tag{12.204}$$

If $\mathbf{K}_2 > \mathbf{I}_B$, then the attenuator satisfies the conditions of Lemma 12.48.

Proof. By Proposition 12.45 and Lemma 12.47, $\Phi_2(P_\psi) \sim \widetilde{\Phi}_2(P_\psi)$ for all $\psi \in \mathcal{H}_B$, where $\widetilde{\Phi}_2$ is an extreme gauge contravariant channel with the matrix $\widetilde{\mathbf{K}} = \sqrt{\overline{\mathbf{K}}_2^2 - \mathbf{I}_B}$.

Define the transposition map $\mathcal{T} : B \to B$ by the relation $\mathcal{T}[D(\mathbf{z})] = D(-\overline{\mathbf{z}})$. The concatenation $\Phi = \mathcal{T} \circ \widetilde{\Phi}_2$ is a gauge covariant Gaussian channel, i. e.,

$$\Phi^*[D(\mathbf{z})] = \widetilde{\Phi}_2^* \circ \mathcal{T}[D(\mathbf{z})] = D\left(\sqrt{\mathbf{K}_2^2 - \mathbf{I}_B}\mathbf{z}\right) \exp\left(-\frac{1}{2}\mathbf{z}^*\mathbf{K}_2^2\mathbf{z}\right),$$

and $\Phi(P_\psi) \sim \widetilde{\Phi}_2(P_\psi)$ since transposition preserves the spectrum. Applying decomposition from Proposition 12.42, namely, the relation (12.178), gives $\Phi = \Phi_2 \circ \Phi_1'$, where Φ_2 is the original amplifier, and $\Phi_1' : B \to B$ is another extreme attenuator with matrix $\mathbf{K}_1 = \sqrt{\mathbf{I}_B - \mathbf{K}_2^{-2}}$. This implies the relation (12.204). Also $\mathbf{K}_2 > \mathbf{I}_B$ implies $0 < \mathbf{K}_1\mathbf{K}_1^* < \mathbf{I}_B$. $\square$

Lemma 12.53 and Lemma 12.51 imply

$$\operatorname{Tr} f(\Phi_2(P_\psi)) = \operatorname{Tr} f((\Phi_2 \circ \Phi_1')(P_\psi)) \tag{12.205}$$

At this point we fix a natural number n and restrict to $\psi \in \mathfrak{L}_n$, the finite-dimensional subspace spanned by the eigenvectors of the total number operator $\mathcal{N}$ corresponding to eigenvalues $\leq n$. According to Lemma 12.49, the attenuator Φ_1' maps P_ψ into a density operator supported by $\mathfrak{L}_n$. Therefore, in its spectral decomposition

$$\Phi_1'(P_\psi) = \sum_j p_j' P_{\psi_j}, \quad p_j' > 0$$

we must have $\psi_j \in \mathfrak{L}_n$. By concavity,

$$\operatorname{Tr} f((\Phi_2 \circ \Phi_1')[P_\psi]) \geq \sum_j p_j' \operatorname{Tr} f\left(\Phi_2\left[P_{\psi_j}\right]\right) \tag{12.206}$$

Since f is assumed strictly concave, $S \to \operatorname{Tr} f(\Phi_2[S])$ is strictly concave [40] (the amplifier Φ_2 is injective by Lemma 12.41). Also, this functional is lower semicontinuous and therefore attains the minimum on the finite-dimensional set of density operators supported by $\mathfrak{L}_n$. Assuming that P_ψ is such a minimizer for the functional (12.205), we conclude that $\Phi_2\left[P_{\psi_j}\right]$ must all coincide, otherwise the above inequality would be strict, contradicting the assumption. From Lemma 12.41 it follows that $P_{\psi_j} = P_{\psi'}$ for all j and for some $\psi' \in \mathcal{H}_B$, and hence, assuming that P_ψ is a minimizer, the output $\Phi_1[P_\psi] = P_{\psi'}$ is a pure state.

Since $\mathbf{K}_1 = \sqrt{\mathbf{I}_B - \mathbf{K}_2^{-2}}$, the condition of Lemma 12.48 is fulfilled when $\mathbf{K}_2 > \mathbf{I}_B$. In this case, if P_ψ is a minimizer, the lemma implies that P_ψ is a coherent state. In fact, since $\psi \in \mathfrak{L}_n$, it has to be the vacuum state S_0. Thus we obtain inequality (12.199) for the amplifier Φ_2 with $\mathbf{K}_2 > \mathbf{I}_B$ and strictly concave f, provided $\psi \in \mathfrak{L}_n$. By standard approximation, this fact is extended to concave f, including all concave polygonal functions. For such functions Lemma 12.50 implies continuity of the functional in question. Then arbitrary $\psi \in \mathcal{H}$ can be approximated in the norm by a sequence $\psi_n \in \mathfrak{L}_n, n \to \infty$, and using this continuity, we arrive at (12.199) for polygonal functions and all $\psi \in \mathcal{H}$. By using the monotone approximation by polygonal functions, we finally obtain (12.199) for all concave functions f satisfying $f(0) = 0$.

In the case of an amplifier Φ_2 with $\mathbf{K}_2 \geq \mathbf{I}_B$, we can take any sequence $\mathbf{K}_2^{(n)} > \mathbf{I}_B$, $\mathbf{K}_2^{(n)} \to \mathbf{K}_2$, and the corresponding amplifiers $\Phi_2^{(n)}$. Then $\operatorname{Tr} f\left(\Phi_2^{(n)}[S]\right) \to \operatorname{Tr} f(\Phi_2[S])$ for any concave polygonal function f on $[0,1]$, such that $f(0) = 0$, and any $S \in \mathfrak{S}(\mathcal{H}_B)$ by Lemma 12.50. This follows from the fact that any such function is Lipschitz, $|f(x) - f(y)| \leq \varkappa |x - y|$, and $\left\|\Phi_2^{(n)}[S] - \Phi_2[S]\right\|_1 \to 0$. It follows that (12.199) holds for all extreme amplifiers Φ_2 in the case of polygonal concave functions f. For arbitrary concave f on $[0,1]$ there is a monotonously nondecreasing sequence of concave polygonal functions f_m converging to f pointwise. Passing to the limit $m \to \infty$ gives inequality (12.199) for an arbitrary extreme amplifier, and hence, (12.197) holds for arbitrary Gaussian gauge covariant or contravariant channels.

(ii) Let f be strictly concave. Repeating the argument after equation (12.206) for the case $\mathbf{K}_2 > \mathbf{I}_B$ and $\psi \in \mathcal{H}_A$, we obtain case (a).

The "only if" statement in cases (b) and (c) are obtained from the decomposition $\Phi = \Phi_2 \circ \Phi_1$ and the relations (12.200)-(12.202). Note that the conditions on the channel Φ imply that in the decomposition $\Phi = \Phi_2 \circ \Phi_1$ the attenuator Φ_1 is defined by the matrix $\mathbf{K}_1$ such that

$0 < \mathbf{K}_1\mathbf{K}_1^* < \mathbf{I}_A$ (see Remark 12.44). Applying the argument involving (12.205) with strictly concave f to the relations (12.200)-(12.203), we obtain that for any pure minimizer P_ψ of $\operatorname{Tr} f(\Phi[P_\psi])$ the output of the extremal attenuator $\Phi_1[P_\psi]$ is necessarily a pure state. Applying Lemma 12.48 to the attenuator Φ_1 we conclude that P_ψ is necessarily a coherent state. □

Explicit Formulas and Additivity

As an immediate corollary of Theorem 12.52 we obtain the following.

Corollary 12.54. For any Gaussian gauge covariant or contravariant channel Φ,

$$\check{H}(\Phi) = H(\Phi[S_0]) = \operatorname{Sp} g(\boldsymbol{\mu} + (\mathbf{K}^*\mathbf{K} - \mathbf{I}_B)/2), \tag{12.207}$$

where S_0 is the vacuum state.

For any two Gaussian gauge covariant (contravariant) channels Φ_1 and Φ_2 the additivity (8.33) of the minimal von Neumann entropy holds.

Proof. The first equality in (12.207) follows from Theorem 12.52 by taking $f(x) = -x\log x$.

From the definitions of gauge covariant/contravariant channels (12.169), (12.173), it follows that the state $\Phi[S_0]$ is gauge invariant Gaussian with the correlation matrix $\boldsymbol{\mu} + \mathbf{K}^*\mathbf{K}/2$, and hence, by using formula (12.109) for the entropy, we obtain

$$\check{H}(\Phi) = \operatorname{Sp} g(\boldsymbol{\mu} + (\mathbf{K}^*\mathbf{K} - \mathbf{I}_B)/2). \tag{12.208}$$

If Φ_1 and Φ_2 are both gauge covariant (contravariant), then their tensor product $\Phi_1 \otimes \Phi_2$ shares this property. The second statement then follows from the expressions (12.207) and the product property of the vacuum state $S_0 = S_0^{(1)} \otimes S_0^{(2)}$, which follows from the definition. □

We now turn to the classical capacity of the channel Φ. We refer to Section 11.5 for all relevant general definitions and results in infinite dimensions. The constrained classical capacity is given by the expression

$$C(\Phi, F, E) = \lim_{n\to\infty} \frac{1}{n} C_\chi\left(\Phi^{\otimes n}, F^{(n)}, nE\right), \tag{12.209}$$

where $C_\chi\left(\Phi^{\otimes n}, F^{(n)}, nE\right)$ is the constrained χ-capacity, F is the constraint operator, and $F^{(n)} = F \otimes I \cdots \otimes I + \cdots + I \otimes \cdots \otimes I \otimes F$.

Let Φ be a Gaussian gauge covariant channel, and consider a gauge invariant oscillator energy operator

$$F = \sum_{j,k=1}^{s_A} \epsilon_{jk} a_j^\dagger a_k, \tag{12.210}$$

where $\boldsymbol{\epsilon} = [\epsilon_{jk}]$ is a Hermitian positive definite matrix, $a_j = \frac{1}{\sqrt{2}}(q_j + ip_j)$ - the annihilation operator for the j th mode. For any state S satisfying $\operatorname{Tr} SF < \infty$, the first moments $\operatorname{Tr} Sa_j$ and the second moments $\operatorname{Tr} Sa_j^\dagger a_k, \operatorname{Tr} Sa_j a_k$ are well-defined. For a Gaussian gauge invariant state (12.97) we have $\operatorname{Tr} Sa_j = 0$ and $\operatorname{Tr} Sa_j a_k = 0$, while (see (12.98))

$$\boldsymbol{\alpha} - \mathbf{I}/2 = \left[\operatorname{Tr} a_j S a_k^\dagger\right]_{j,k=1,\ldots,s}.$$

For this choice of the channel and the constraint, the conditions of Corollary 11.24 are fulfilled, and the χ-capacity is in general given by the relation (11.38).

Theorem 12.55. The constrained classical capacity of the Gaussian gauge covariant channel Φ is

$$
\begin{aligned}
C(\Phi;F,E) =& C_\chi(\Phi;F,E)\\
=& \max_{\boldsymbol{v}:\mathrm{Sp}\,\boldsymbol{v}\boldsymbol{\epsilon}\le E} \mathrm{Spg}\left(\mathbf{K}^*\boldsymbol{v}\mathbf{K}+\boldsymbol{\mu}+\left(\mathbf{K}^*\mathbf{K}-\mathbf{I}_B\right)/2\right)\\
&-\mathrm{Spg}\left(\boldsymbol{\mu}+\left(\mathbf{K}^*\mathbf{K}-\mathbf{I}_B\right)/2\right). \qquad (12.211)
\end{aligned}
$$

The optimal ensemble π which attains the maximum in (11.38) consists of coherent states $S_{\mathbf{z}}=D_A(\mathbf{z})S_0D_A(\mathbf{z})^*, \mathbf{z}\in\mathbf{Z}_A$, distributed with gauge invariant Gaussian probability distribution $Q_{\boldsymbol{v}}\left(d^{2s}z\right)$ on $\mathbf{Z}_A$ having zero mean and the correlation matrix $\boldsymbol{v}$ which solves the maximization problem in (12.211).

Proof. Consider a Gaussian ensemble $\pi_{\boldsymbol{v}}$ consisting of coherent states $S_{\mathbf{z}}=D_A(\mathbf{z})\times S_0D_A(\mathbf{z})^*, \mathbf{z}\in\mathbf{Z}_A$, with gauge invariant Gaussian probability distribution $Q_{\boldsymbol{v}}\left(d^{2s}z\right)$ on $\mathbf{Z}_A$ having zero mean and some correlation matrix $\boldsymbol{v}$. It is defined by the classical characteristic function

$$
\int_{\mathbf{Z}_A}\exp\left(2i\,\mathrm{Im}\,\mathbf{w}^*\mathbf{z}\right)Q_{\boldsymbol{v}}\left(d^{2s}w\right)=\exp\left(-\mathbf{z}^*\mathbf{v}\mathbf{z}\right).
$$

By using the covariance property (12.140) of Gaussian channels, we have

$$
H\left(\Phi\left[S_{\mathbf{z}}\right]\right)=H\left(\Phi\left[D_A(\mathbf{z})S_{\mathbf{0}}D_A(\mathbf{z})^*\right]\right)=H\left(\Phi\left[S_0\right]\right)=\mathrm{Spg}\left(\boldsymbol{\mu}+\left(\mathbf{K}^*\mathbf{K}-\mathbf{I}_B\right)/2\right),
$$

which does not depend on $\mathbf{z}$, and hence it gives the value of the integral term in (11.35). Integration of the characteristic functions of the coherent states gives for the average state of the ensemble (cf. (12.100))

$$
\mathrm{Tr}\,\bar{S}_{\pi_v}D_A(\mathbf{z})=\exp\left(-\mathbf{z}^*\left(\boldsymbol{v}+\mathbf{I}_A/2\right)\mathbf{z}\right).
$$

Then $\boldsymbol{v}=\left[\mathrm{Tr}\,a_j\bar{S}_{\pi_v}a_k^\dagger\right]_{j,k=1,\ldots,S_A}$ (see (12.98)), and

$$
\mathrm{Tr}\,\bar{S}_{\pi_v}F=\sum_{j,k=1}^{s_A}\epsilon_{jk}\,\mathrm{Tr}\,\bar{S}_{\pi_v}a_j^\dagger a_k=\mathrm{Sp}\,\boldsymbol{\epsilon}\boldsymbol{v}^\top=\mathrm{Sp}\,\boldsymbol{v}\boldsymbol{\epsilon},
$$

where we used $\boldsymbol{\epsilon}^\top=\boldsymbol{\epsilon}$. The state $\Phi\left[\bar{S}_{\pi_v}\right]$ is gauge invariant Gaussian with the correlation matrix

$$
\mathbf{K}^*\left(\boldsymbol{v}+\mathbf{I}_A/2\right)\mathbf{K}+\boldsymbol{\mu},
$$

hence it has the entropy

$$
\mathrm{Sp}\,g\left(\mathbf{K}^*\boldsymbol{v}\mathbf{K}+\boldsymbol{\mu}+\left(\mathbf{K}^*\mathbf{K}-\mathbf{I}_B\right)/2\right).
$$

Thus for the Gaussian ensemble π_v

$$
\chi\left(\pi_{\boldsymbol{v}}\right)=\mathrm{Sp}\,g\left(\mathbf{K}^*\boldsymbol{v}\mathbf{K}+\boldsymbol{\mu}+\left(\mathbf{K}^*\mathbf{K}-\mathbf{I}_B\right)/2\right)-\mathrm{Spg}\left(\boldsymbol{\mu}+\left(\mathbf{K}^*\mathbf{K}-\mathbf{I}_B\right)/2\right). \qquad (12.212)
$$

Summarizing, we need to show

$$
C(\Phi;F,E)=C_\chi(\Phi;F,E)=\sup_{v:\mathrm{Sp}\,v\in\le E}\chi\left(\pi_v\right). \qquad (12.213)
$$

Let us denote by $\mathcal{G}$ the set of Gaussian gauge invariant states in $\mathcal{H}_A$.

Lemma 12.56. Let Φ be a Gaussian gauge covariant channel and the constraint operator F is given by (12.210). Then

$$\max_{S^{(n)}:\mathrm{Tr}\, S^{(n)}F^{(n)}\le nE} H\left(\Phi^{\otimes n}\left[S^{(n)}\right]\right) \le n \max_{S:S\in\mathcal{G},\mathrm{Tr}\, SF\le E} H(\Phi[S]). \tag{12.214}$$

Proof. We first note that Lemma 11.20 implies

$$\sup_{S^{(n)}:\mathrm{Tr}\, S^{(n)}F^{(n)}\le nE} H\left(\Phi^{\otimes n}\left[S^{(n)}\right]\right) \le n \sup_{S:\mathrm{Tr}\, SF\le E} H(\Phi[S]). \tag{12.215}$$

By using gauge covariance of the channel Φ, we can then reduce maximization in the right-hand side of (12.215) to gauge invariant states. Indeed, for a given state S, satisfying the constraint $\mathrm{Tr}\, SF \le E$, the averaging

$$S_{av} = \frac{1}{2\pi}\int_0^{2\pi} U_\phi S U_\phi^* d\phi$$

also satisfies the constraint, while $H(\Phi[S]) \le H\left(\Phi\left[S_{av}\right]\right)$ by concavity of the entropy. Finally, we use the maximum entropy principle which says that among states with fixed second moments the Gaussian state has maximal entropy (see Lemma 12.26). This proves (12.214). □

We have

$$\max_{S:S\in\mathcal{G},\mathrm{Tr}\, SF\le E} H(\Phi[S]) = \max_{\boldsymbol{v}:\mathrm{Sp}\,\boldsymbol{v}\boldsymbol{\epsilon}\le E} \mathrm{Spg}\left(\mathbf{K}^*\boldsymbol{v}\mathbf{K} + \boldsymbol{\mu} + \left(\mathbf{K}^*\mathbf{K} - \mathbf{I}_B\right)/2\right)\Big]. \tag{12.216}$$

Now let $\boldsymbol{v}$ be the solution of the maximization problem in the right-hand side. To prove (12.211) observe that

$$\begin{aligned} n\chi\left(\pi_\nu\right) &\le nC_\chi(\Phi, F, E) \le C_\chi\left(\Phi^{\otimes n}, F^{(n)}, nE\right) \\ &\le \max_{S^{(n)}:\mathrm{Tr}\, S^{(n)}F^{(n)}\le nE} H\left(\Phi^{\otimes n}\left[S^{(n)}\right]\right) - \min_{S^{(n)}} H\left(\Phi^{\otimes n}\left[S^{(n)}\right]\right) \end{aligned}$$

By using Lemma 12.56 and Corollary 12.54 we see that this is less than or equal to

$$n\left[\max_{S:S\in\mathcal{G},\mathrm{Tr}\, SF\le E} H(\Phi[S]) - H\left(\Phi\left[S_0\right]\right)\right] = n\chi\left(\pi_v\right),$$

where the equality follows from (12.216) and (12.212).
Thus the additivity $C_\chi\left(\Phi^{\otimes n}, F^{(n)}, nE\right) = nC_\chi(\Phi, F, E)$ holds, and hence the constrained classical capacity (12.209) of the Gaussian gauge covariant channel is given by the expression (12.211). □

A similar argument applies to the Gaussian gauge contravariant channel (12.173), giving the expression (12.211) with $\boldsymbol{\epsilon}$ replaced by $\overline{\boldsymbol{\epsilon}}$. Indeed, in this case the state $\Phi\left[\bar{S}_{\pi_v}\right]$ is gauge invariant Gaussian with the characteristic function

$$\begin{aligned} \mathrm{Tr}\,\Phi\left[\bar{S}_{\pi_v}\right] D(\mathbf{z}) &= \exp\left(-\left(\overline{\mathbf{K}\mathbf{z}}\right)^*\left(\boldsymbol{v} + \mathbf{I}_A/2\right)\overline{\mathbf{K}\mathbf{z}} - \mathbf{z}^*\boldsymbol{\mu}\boldsymbol{z}\right) \\ &= \exp\left(-\left(\mathbf{K}\mathbf{z}\right)^*\left(\overline{\boldsymbol{v}} + \mathbf{I}_A/2\right)\mathbf{K}\mathbf{z} - \mathbf{z}^*\boldsymbol{\mu}\boldsymbol{z}\right), \end{aligned}$$

with the correlation matrix $\mathbf{K}^*\left(\overline{\boldsymbol{v}} + \mathbf{I}_A/2\right)\mathbf{K} + \boldsymbol{\mu}$. Redefining $\overline{\boldsymbol{v}}$ as $\boldsymbol{v}$ and noting that $\mathrm{Sp}\,\overline{\boldsymbol{v}}\boldsymbol{\epsilon} = \mathrm{Sp}\,\boldsymbol{v}\overline{\boldsymbol{\epsilon}}$ since $\boldsymbol{v}, \boldsymbol{\epsilon}$ are Hermitian, we get the statement.

The maximization in (12.211) is a finite-dimensional optimization problem which is a quantum analog of the "water-filling" problem in classical information theory; see, e. g., [47]. Apart from the case of a single mode considered in the next section, it can be solved explicitly only in some special cases, e.g., when $\mathbf{K}, \boldsymbol{\mu}, \boldsymbol{\epsilon}$ commute, and it is a subject of separate study.

10.12.26 12.6 The Case of Single Mode

10.12.27 12.6.1 Classification of Gaussian Channels

In this section we will be interested in the problem of reducing an arbitrary quantum Gaussian channel to the simplest "normal" form which can be obtained by applying suitable unitary operators, corresponding to symplectic transformations T_1, T_2 via formula (12.67), to the input and the output of the channel, i.e.,

$$\Phi^{*\prime}[W(z)] = U_{T_1}^* \Phi^* \left[U_{T_2}^* W(z) U_{T_2}\right] U_{T_1},$$

that is,

$$\Phi^{*\prime}[W(z)] = W\left(T_1 K T_2 z\right) f\left(T_2 z\right). \tag{12.217}$$

Here we give a complete solution of this problem in one mode, $s = 1$.
Let Z be the two-dimensional symplectic space, i. e., the real linear space of vectors $z = \left[\begin{array}{cc} x & y \end{array}\right]^\top$ with the symplectic form

$$\Delta\left(z, z'\right) = xy' - x'y. \tag{12.218}$$

A basis e, h in Z is symplectic if $\Delta(e, h) = 1$, i. e., if the area of the oriented parallelogram based on e, h is equal to 1 . Recall that a linear transformation T in Z is symplectic if it maps a symplectic basis into a symplectic basis.

According to formula (12.137), a Gaussian channel is characterized by the parameters (K, l, μ) satisfying

$$\mu \geq \pm \frac{i}{2}\left[\Delta - K^\top \Delta K\right]. \tag{12.219}$$

By way of a displacement transformation (12.53) we can always make $l = 0$, which we assume. Thus

$$\Phi^*[W(z)] = W(Kz) \exp\left[-\frac{1}{2} z^\top \mu z\right]. \tag{12.220}$$

The transformation (12.217) amounts to $K \to T_1 K T_2, \mu \to T_2^\top \mu T_2$ which leaves invariant the quantities

$$\det K = \Delta(Ke, Kh), \quad \det \mu, \tag{12.221}$$

as well as the rank of the matrices K and μ. It is therefore not surprising that these quantities play a special role in the classification.

In the following theorem we use the notation

$$I_2 = \left[\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array}\right].$$

Theorem 12.57. Let $\{e, h\}$ be a symplectic basis. Then, depending on the value
(A) $\Delta(Ke, Kh) = 0$;
(B) $\Delta(Ke, Kh) = 1$;
(C) $\Delta(Ke, Kh) = k^2 > 0, k \neq 1$;
(D) $\Delta(Ke, Kh) = -k^2 < 0$,
there are symplectic transformations T_1, T_2, such that the channel $\Phi^{*\prime}$ has the form (12.220) with

$$
\begin{aligned}
&(\mathrm{A}_1)\quad K=0,\\
&\mu=\left(N_0+\frac{1}{2}\right)I_2,\quad N_0\geq 0;\\
&(\mathrm{A}_2)\quad K=\begin{bmatrix}1&0\\0&0\end{bmatrix},\\
&\mu=\left(N_0+\frac{1}{2}\right)I_2;\\
&(\mathrm{B}_1)\quad K=I_2,\\
&\mu=\frac{1}{2}\begin{bmatrix}1&0\\0&0\end{bmatrix};\\
&\qquad\qquad K=I_2,\\
&\qquad\qquad \mu=N_cI_2,\quad N_c\geq 0;\\
&\qquad(\mathrm{C}_1)\quad K=kI_2,\quad 0<k<1,\\
&(\mathrm{B}_2)\qquad\quad \mu=\left(N_c+\frac{1-k^2}{2}\right)I_2;\\
&\qquad(\mathrm{C}_2)\quad K=kI_2,\quad k>1,\\
&\qquad\qquad \mu=\left(N_c+\frac{k^2-1}{2}\right)I_2;\\
&\qquad\qquad K=k\begin{bmatrix}1&0\\0&-1\end{bmatrix},\quad k>0,\\
&(\mathrm{D})\\
&\qquad\qquad \mu=\left(N_c+\frac{k^2+1}{2}\right)I_2.
\end{aligned}
$$

Apparently, in the cases $(\mathrm{A}_1), (\mathrm{B}_2), (\mathrm{C})$ the channel is gauge covariant with respect to the natural complex structure associated with multiplication by i in the complex plane x, y. In case (D) the channel is gauge contravariant. It is convenient to describe the variety of all channels with gauge symmetry by two parameters expressed in terms of the invariants (12.221), i.e.,

$$
\varkappa=\det K,\quad N_c=\sqrt{\det\mu}-\frac{1}{2}|\det K-1|. \tag{12.222}
$$

One has $-\infty<x<\infty$ ($x=k^2$ for $(\mathrm{A}_1), (\mathrm{B}_2), (\mathrm{C})$, $x=-k^2$ for (D)), and $N_c\geq 0$, so that the variety is just the upper half-plane of the variables x, N_c (Figure 12.3).

Proof. (A) $\Delta(Ke,Kh)=0$. In this case $\Delta(Kz,Kz')\equiv 0$ and either $K=0$ or K has rank one. Then inequality (12.219) is just the condition on the covariance matrix of a quantum Gaussian state. As follows from Lemma 12.12, there is a symplectic transformation T_2 such that

$$
\mu(T_2z,T_2z)=\left(N_0+\frac{1}{2}\right)\left(x^2+y^2\right). \tag{12.223}
$$

In the case $K=0$ we just have (A_1).

Let K have rank one. Then KT_2 has rank one and there is a vector e' such that $KT_2\begin{bmatrix}x&y\end{bmatrix}^\top=(k_1x+k_2y)\,e'$. Then there is a symplectic transformation T_1 such that $T_1e'=\begin{bmatrix}1&0\end{bmatrix}$ and hence $T_1KT_2\begin{bmatrix}x&y\end{bmatrix}^\top=\begin{bmatrix}k_1x+k_2y&0\end{bmatrix}^\top$. By making a rotation T_2' which leaves μ unchanged, we can transform this vector to $[k_1'x\quad 0]^\top$ with $k_1'\neq 0$, and then by a symplectic scaling (squeezing) T_1' we arrive to case (A_2).

(B), (C) $\Delta(Ke,Kh)=k^2>0$. Then $T=k^{-1}K$ is a symplectic transformation and

$\Delta(Kz, Kz') = k^2\Delta(z, z')$. Let $T_1 = (TT_2)^{-1}$, where T_2 will be chosen later, so that $T_1 K T_2 = kI$.

In case (B)$k = 1$ and the condition (12.219) is just positive definiteness of μ. Then we have the following subcases:

(B_2) If μ is nondegenerate, then by Lemma 12.12 there is a symplectic transformation T_2 such that

$$\mu(T_2 z, T_2 z) = N_c\left(x^2 + y^2\right),$$

where $N_c > 0$. Also if $\mu = 0$, we have a similar formula with $N_c = 0$.

(B_1) On the other hand, if μ is degenerate of rank one, then $\mu(z, z) = (k_1 x + k_2 y)^2$ for some k_1, k_2 simultaneously not equal to zero, and then for arbitrary $N_c > 0$ there is a symplectic transformation T_2 such that

$$\mu(T_2 z, T_2 z) = N_c x^2,$$

in particular, we can take $N_c = \frac{1}{2}$.

In case (C) $k \neq 1$, and the condition (12.219) implies that $\mu/|k^2 - 1|$ is a covariance matrix of a quantum Gaussian state, hence there exists a symplectic transformation T_2 such that

$$\mu(T_2 z, T_2 z) = \left|k^2 - 1\right|\left(N_0 + \frac{1}{2}\right)\left(x^2 + y^2\right) = \left(N_c + \frac{|k^2 - 1|}{2}\right)\left(x^2 + y^2\right),$$

where $N_0 \geq 0, N_c = |k^2 - 1| N_0$.

(D) $\Delta(Ke, Kh) = -k^2 < 0$. Then $T = k^{-1}K$ is an antisymplectic transformation, which means that $\Delta(Tz, Tz') = -\Delta(z, z')$ and $\Delta(Kz, Kz') = -k^2\Delta(z, z')$. Similar to cases (B) and (C), we obtain

$$\mu(T_2 z, T_2 z) = \left(k^2 + 1\right)\left(N_0 + \frac{1}{2}\right)\left(x^2 + y^2\right) = \left(N_c + \frac{(k^2 + 1)}{2}\right)\left(x^2 + y^2\right)$$

with $N_0 \geq 0, N_c = (k^2 + 1) N_0$. Letting $T_1 = \Lambda(TT_2)^{-1}$, where $\Lambda \begin{bmatrix} x & y \end{bmatrix}^\top = \begin{bmatrix} x & -y \end{bmatrix}^\top$, we obtain the first equation in (D). Note that T_1 is symplectic since both T and Λ are antisymplectic.

As explained in Section 12.4.1, a Gaussian channel Φ can be dilated to a linear dynamics of open bosonic system described by symplectic transformation of canonical variables q, p and ancillary canonical variables $q_E, p_E, \ldots$ in a Gaussian state S_E; moreover this linear dynamics provides also a description of the weak complementary channel Φ_E mapping initial state of the system q, p into the final state of the environment $q'_E, p'_E, \ldots$; in the case where the state S_E is pure, Φ_E is just the complementary channel $\widetilde{\Phi}$, which is determined by Φ up to isometric equivalence. Note that the environment may have more than one mode (which is reflected by introducing ... in the environment variables).

Let us give such a description in terms of an input-output relation in each of the cases of Theorem 12.57.

(A_1) This is the completely depolarizing channel

$$q' = q_E,$$
$$p' = p_E,$$

where q_E, p_E describe the environment in the quantum thermal state S_E with mean number of quanta N_0. Its weak complementary is the ideal channel Id.

(A_2) The input-output relation is

$$q' = q + q_E \tag{12.224}$$
$$p' = p_E$$

where q_E, p_E are again in the quantum thermal state S_E with mean number of quanta N_0. The equation describes the degenerate classical signal q with additive quantum Gaussian noise. The weak complementary to this channel is described by the transformation

$$q'_E = q \tag{12.225}$$
$$p'_E = p - p_E$$

where p_E can be regarded as a classical real Gaussian variable with variance $N_0 + \frac{1}{2}$.
(B_1) The equation of the channel has the form (12.225), where p_E has variance $\frac{1}{2}$, so that the mode q_E, p_E is in pure (vacuum) state, and the complementary channel is given by (12.224). This is quantum signal plus degenerate (two-dimensional) classical Gaussian noise.
(B_2) For a channel with (nondegenerate) additive classical Gaussian noise,

$$q' = q + \xi$$
$$p' = p + \eta$$

where ξ, η are i. i. d. Gaussian random variables with zero mean and variance N_c.

Exercise 12.58 Check that the Stinespring dilation for this channel can be obtained by adding environment with two bosonic modes $q_j, p_j, j = 1, 2$, in pure Gaussian state having zero means, zero covariances, and the variances

$$\mathrm{D}q_1 = \mathrm{D}q_2 = N_c, \quad \mathrm{D}p_1 = \mathrm{D}p_2 = \frac{1}{4N_c},$$

so that $\xi = q_1, \eta = q_2$ and with the following dynamics for the canonical observables

$$q' = q + q_1,$$
$$p' = p + q_2,$$
$$q'_1 = q_1,$$
$$p'_1 = p_1 - p - q_2/2,$$
$$q'_2 = q_2,$$
$$p'_2 = p_2 + q + q_1/2.$$

(C) Attenuation/amplification channel with coefficient k and quantum noise with mean number of quanta N_0. In the attenuation case ($k < 1$) the input-output relation is

$$q' = kq + \sqrt{1 - k^2} q_E,$$
$$p' = kp + \sqrt{1 - k^2} p_E,$$

where q_E, p_E are in the quantum thermal state S_E with mean number of quanta N_0. The weak complementary is given by the equations

$$q'_E = \sqrt{1 - k^2} q - k q_E \tag{12.226}$$
$$p'_E = \sqrt{1 - k^2 p} - k p_E \tag{12.227}$$

and is again an attenuation channel (with coefficient $k' = \sqrt{1-k^2}$).

In the amplification case ($k > 1$) we have

$$q' = kq + \sqrt{k^2-1}q_E$$
$$p' = kp - \sqrt{k^2-1}p_E$$

with the weak complementary

$$q'_E = \sqrt{k^2-1}q + kq_E$$
$$p'_E = -\sqrt{k^2-1}p + kp_E$$

(see case (D)).

D) The input-output relation is

$$q' = kq + \sqrt{k^2+1}q_E$$
$$p' = -kp + \sqrt{k^2+1}p_E$$

which is the same as the weak complementary to an amplification channel with coefficient $k' = \sqrt{k^2+1}$ and quantum noise with mean number of quanta N_0. This channel describes attenuation/amplification with phase conjugation, i.e., $q, p \to q, -p$.

Finally, let us show how the c-q channel considered in Section 12.1.4 fits into the general description of quantum Gaussian channels. Since the input is twodimensional classical, one has to use two bosonic input modes q_1, p_1, q_2, p_2 to describe it quantum mechanically, so that, e.g., $m_q = q_1, m_p = q_2$. The environment is one mode q, p in the Gaussian state S_0 so the output is given by the equations

$$q' = q_1 + q = q + m_q,$$
$$p' = q_2 + p = p + m_p,$$

and the channel parameters are

$$K = \begin{bmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad \mu = \left(N_0 + \frac{1}{2}\right) I_2. \tag{12.228}$$

In this case the full set of the Heisenberg equations is the same as in case (B_2), with the roles of input modes and environmental modes interchanged.

10.12.28 12.6.2 Entanglement-Breaking Channels

Let us apply Theorem 12.36 to the case of one bosonic mode $A = B$, where $\Delta_A(z, z') = \Delta_B(z, z')$ is given by the relation (12.218). As shown above, any one-mode Gaussian channel can be transformed to one of the normal forms.

We only have to find the form $K^\top \Delta_A K$ and check the decomposability (12.146) in each of these cases. We rely upon the following fact.

Exercise 12.59 Show that

$$\left(N + \frac{1}{2}\right) I_2 \geq \pm \frac{i}{2}\Delta$$

if and only if $N \geq 0$.

With this we proceed to a consideration of each class:

(A) $K^\top \Delta K = 0$, hence Φ is a c-q (in fact essentially classical) channel;

(B) $K^\top \Delta K = \Delta$, hence the necessary condition of decomposability (12.146) requires $\mu \geq i\Delta$; this is never fulfilled in case (B_1) due to the degeneracy of μ. Thus the channel is not entanglement-breaking (in fact it has infinite quantum capacity as shown in [120]); on the other hand, in case (B_2) the condition (12.146) is fulfilled with $\alpha_B = \alpha_A = \mu/2$ if and only if $N_c \geq 1$, hence Φ is entanglement-breaking in this case;
(C) $K^\top \Delta K = k^2 \Delta$; it is clear that in this case the decomposability condition holds if and only if $\mu \geq \pm\frac{i}{2}(1+k^2)\Delta$, which is equivalent to $N_c + \frac{|1-k^2|}{2} \geq \frac{(1+k^2)}{2}$ or

$$N_c \geq \min\left(1, k^2\right) \tag{12.229}$$

this gives the condition for the entanglement breaking (which also formally includes case (B_2);
(D) $K^\top \Delta K = -k^2 \Delta$; again the decomposability condition holds if and only if $\mu \geq \pm\frac{i}{2}(1+k^2)\Delta$, which is always the case, hence the channel is entanglement-breaking for all $N_c \geq 0$.

Thus the additivity property (11.33) holds for one-mode Gaussian channels of the form (A), (D) with arbitrary parameters, and (B_2), (C) with parameters satisfying (12.229). In general, entanglement-breaking channels have zero quantum capacity, $Q(\Phi) = 0$ (see Corollary 10.28). However, in Section 12.6.4 a broader domain of zero quantum capacity will be demonstrated basing on degradability analysis.

Exercise 12.60 Use Exercise 12.59 to show that in the case of one mode the condition (12.153) implies (12.146), hence every PPT channel is entanglement-breaking.

10.12.29 12.6.3 Attenuation/Amplification/Classical Noise Channel

From the point of view of applications the gauge covariant cases (C), (B_2) are the most interesting. The action of the channel Φ in these cases can be described by a single formula, i. e.,

$$\Phi^*[D(\mathbf{z})] = D(k\mathbf{z}) \cdot \exp\left[-\left(N_c + \left|k^2 - 1\right|/2\right)|\mathbf{z}|^2\right], \tag{12.230}$$

where the parameter $N_c \geq 0$ is the power of the environment noise and $k > 0$ is the coefficient of attenuation/amplification in case (C). Then $N_c = |k^2 - 1|\, N_0$, where N_0 is the mean photon number of the environment. Case (B_2) of additive classical Gaussian noise channel corresponds to the value $k = 1$. The channel is gauge covariant with respect to the natural complex structure associated with the multiplication by i of the complex variable $\mathbf{z} = (x + iy)/\sqrt{2} \in \mathbb{C}$. Therefore, in what follows, basing on the results of Section 12.5, we can restrict ourselves to the gauge invariant input states.

In the case of one mode the only such states are the elementary Gaussian states $S = S(N)$ with the characteristic function

$$\operatorname{Tr} S(N) D(\mathbf{z}) = \exp\left[-(N + 1/2)|\mathbf{z}|^2\right],$$

the parameter N representing the power (mean number of quanta) of the signal

$$\operatorname{Tr} S(N) a^\dagger a = N. \tag{12.231}$$

The entropy of $S(N)$ is

$$H(S(N)) = g(N). \tag{12.232}$$

From (12.230) we find that the output state $\Phi[S]$ is the Gaussian state $S(N')$ where

$$N' = k^2 N + N'_0, \tag{12.233}$$

and the total noise

$$N'_0 = \max\left\{0, \left(k^2 - 1\right)\right\} + N_c \tag{12.234}$$

is the output mean photon number corresponding to the vacuum input state $S(0)$. The first term is nonzero only in the case $k > 1$ when it represents the amplifier noise. The output entropy is equal to

$$H(\Phi[S(N)]) = g\left(N'\right). \tag{12.235}$$

Now we compute the entropy exchange $H(S(N), \Phi)$. The (pure) input state S_{12} of the extended system $\mathcal{H} \otimes \mathcal{H}_0$ is characterized by the 2×2-matrix (12.120). According to (12.154), the action of the extended channel $\Phi \otimes \mathrm{Id}$ transforms this matrix into

$$\Delta_{12}^{-1}\mu'_{12} = \begin{bmatrix} 0 & -\left(N' + 1/2\right) & k\sqrt{N^2+N} & 0 \\ N' + 1/2 & 0 & 0 & k\sqrt{N^2+N} \\ k\sqrt{N^2+N} & 0 & 0 & N + 1/2 \\ 0 & k\sqrt{N^2+N} & -(N+1/2) & 0 \end{bmatrix},$$

where N' is given by (12.233). From formula (12.110) we deduce $H(S(N), \Phi) = g\left(|\lambda_1| - \frac{1}{2}\right) + g\left(|\lambda_2| - \frac{1}{2}\right)$, where $\pm\lambda_1, \pm\lambda_2$ are the eigenvalues of the matrix on the right-hand side. Solving the characteristic equation we obtain

$$\lambda_{1,2} = \frac{i}{2}\left(\left(N' - N\right) \pm D\right), \tag{12.236}$$

where

$$D = \sqrt{\left(N + N' + 1\right)^2 - 4k^2 N(N+1)}.$$

Hence

$$H(S(N), \Phi) = g\left(\frac{D + N' - N - 1}{2}\right) + g\left(\frac{D - N' + N - 1}{2}\right). \tag{12.237}$$

Let us consider the classical capacities of the channel Φ under the additive input energy constraint (11.28) corresponding to the operator $F = a^\dagger a$. According to Corollary 12.38, the entanglement-assisted classical capacity

$$C_{ea}(\Phi, F, E) = \max_{S:\mathrm{Tr}\, Sa^+a \le E} I(S, \Phi)$$

is attained on a gauge invariant Gaussian state. Since the condition (11.42) is obviously fulfilled for our channel, $\mathrm{Tr}\, \mathrm{S}a^\dagger a = E$ for this state, which is thus the elementary Gaussian state $S(E)$. Hence the maximum is equal to

$$C_{ea}(\Phi, F, E) = I(S(E), \Phi) = H(S(E)) + H(\Phi[S(E)]) - H(S(E), \Phi), \tag{12.238}$$

where the entropies are given by the relations (12.232), (12.235), and (12.237) with N replaced by E.

Considering $C_{ea}(\Phi, F, E)$ as a function of the parameters E, k, N_c, it is interesting to compare it with the classical capacity $C(\Phi, F, E)$ computed in Theorem 12.55. In the case of one mode the maximum in formula (12.211) with $\boldsymbol{\epsilon} = 1$ is attained for $\boldsymbol{v} = E$. Hence the optimal

ensemble consists of coherent states $S_\zeta = |\zeta\rangle\langle\zeta|; \zeta \in \mathbb{C}$, with the Gaussian probability density $p(\zeta) = (\pi E)^{-1} \exp(-|\zeta|^2/E)$, giving the value

$$C(\Phi, F, E) = g\left(k^2 E + N_0'\right) - g\left(N_0'\right), \tag{12.239}$$

where N_0' is given by (12.234), so that

$$C(\Phi, F, E) = g\left(k^2 E + N_c + \max\left\{0, \left(k^2 - 1\right)\right\}\right) - g\left(N_c + \max\left\{0, \left(k^2 - 1\right)\right)\right.\right.\right.

The entanglement-assisted classical capacity can be computed via formula (12.238) in which the entropies are calculated with $N' = k^2 E + N_0'$, but N_0' is given by (12.243). We leave the detail to the interested reader.

10.12.30 12.6.4 Estimating the Quantum Capacity

In this section the quantum capacity of the one-mode channel will be computed in several cases, basing on the (anti)degradability property (see Sections 10.3.3, 12.5.3). We use the fact that composition of one-mode Gaussian channels is again a one-mode Gaussian channel. In particular, the general rule (12.139) implies the following relations.

Denote by $\Phi_{C,k}$ (resp. $\Phi_{D,k}$) a channel of class C (resp. D) with coefficient k and a fixed value of parameter N_c. Then

$$\begin{array}{ll} \Phi_{C,k_2} \circ \Phi_{C,k_1} = \Phi_{C,k_1 k_2}, & \text{if } k_1, k_2 < 1, \\ \Phi_{D,k_2} \circ \Phi_{C,k_1} = \Phi_{D,k_1 k_2}, & \text{if } k_1 > 1. \end{array} \tag{12.246}$$

Proposition 12.62. For attenuators with $k \leq \frac{1}{\sqrt{2}}$ the quantum capacity $Q(\Phi_{C,k}) = 0$. For attenuation/amplification channels with $k \geq \frac{1}{\sqrt{2}}$ and $N_c = 0$

$$Q(\Phi_{C,k}) = Q_G(\Phi_{C,k}) = \log \frac{k^2}{|k^2 - 1|}. \tag{12.247}$$

Here

$$Q_G(\Phi) = \sup_{N \geq 0} I_c(S(N), \Phi),$$

where the supremum of the coherent information $I_c(S, \Phi) = H(\Phi[S]) - H(S, \Phi)$ is taken over all gauge invariant Gaussian input states $S(N)$.

Proof. The proof will follow from Proposition 12.40 if we show that attenuators with $k < \frac{1}{\sqrt{2}}$ are antidegradable while attenuation/amplification channels with $k \geq \frac{1}{\sqrt{2}}$ and $N_c = 0$ are degradable.

Let $k < \frac{1}{\sqrt{2}}$. Then $k_1 = \frac{k}{\sqrt{1-k^2}} < 1$ and taking into account that the weak complementary of $\Phi_{C,k}$ is

$$\widetilde{\Phi}^W_{C,k} = \Phi_{C,\sqrt{1-k^2}} \tag{12.248}$$

(see (12.226)), the relation (12.245) takes the form

$$\Phi_{C,k} = \Phi_{C,\frac{k}{\sqrt{1-k^2}}} \circ \widetilde{\Phi}^W_{C,k}, \tag{12.249}$$

which implies that $\Phi_{C,k}$ is antidegradable, since the weak complementary can be dilated to complementary by purifying the environment state. Hence its quantum capacity is equal to zero by Proposition 10.27.

In the case $N_c = 0$, when the environment state is pure, the complementary channel coincides with the weakly complementary, i. e., $\widetilde{\Phi}_{C,k} = \widetilde{\Phi}^w_{C,k} = \Phi_{C,k'}$, where $k' = \sqrt{1-k^2} > \frac{1}{\sqrt{2}}$, and the relation (12.249) is the same as

$$\widetilde{\Phi}_{C,k'} = \Phi_{C,\frac{k}{\sqrt{1-k^2}}} \circ \Phi_{C,k'},$$

which means that $\Phi_{C,k'}$ is degradable for $\frac{1}{\sqrt{2}} < k' < 1$. Therefore Proposition 12.40 applies implying

$$Q(\Phi_{C,k}) = Q_G(\Phi_{C,k}). \tag{12.250}$$

Similarly in the amplifier case ($k > 1, N_c = 0$) the relation (12.246) implies

$$\widetilde{\Phi}_{C,k} = \Phi_{D,\frac{\sqrt{k^2-1}}{k}} \circ \Phi_{C,k},$$

whence $\Phi_{C,k}$ is degradable, and (12.250) continues to hold. It remains to compute $Q_G(\Phi_{C,k})$.

Since the channels are gauge covariant, Proposition 12.40 implies that in looking for the maximum of the coherent information over Gaussian input states it is sufficient to restrict to the one-mode gauge invariant states $S(N)$.

In the general case where $N_c \geq 0$, the coherent information

$$I_c(S(N), \Phi) = g(N') - g\left(\frac{D + N' - N - 1}{2}\right) - g\left(\frac{D - N' + N - 1}{2}\right) \tag{12.251}$$

is a complicated function of the input power N. We have $I_c(S(0), \Phi) = 0$ and

$$\lim_{N\to\infty} I_c(S(N), \Phi) = \log k^2 - \log\left|k^2 - 1\right| - g\left(N_c/\left|k^2 - 1\right|\right), \quad k \neq 1.$$

Whenever positive, this gives a lower bound $\underline{Q}(\varkappa, N_c), \varkappa = k^2$, for the quantum capacity $Q(\Phi_{C,k})$.

Let us now consider the case $N_c = 0$. The behavior of the entropies $H(\Phi[S(N)])$, $H(S(N), \Phi)$ as functions of k for $N_c = 0$ is shown in Figure 12.1. Note that for all N the coherent information $H(\Phi[S(N)]) - H(S(N), \Phi)$ turns out to be positive for $k^2 > \frac{1}{2}$ and negative otherwise. It tends to $-H(S(N))$ for $k \to 0$, is equal to $H(S(N))$ for $k = 1$, and quickly tends to zero as $k \to \infty$.

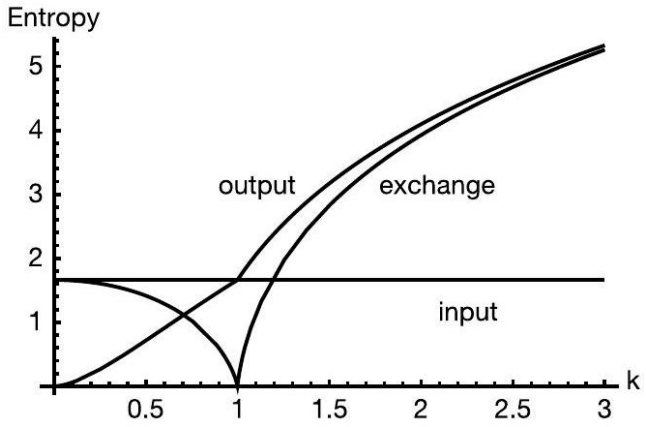


Figure 12.1: Entropies: the output entropy (12.235), the entropy exchange (12.237) in the case $N_{c} =0$.

If $k < 1$ (ideal attenuator), then $N' = k^2 N, D = (1 - k^2) N + 1$ and

$$I_c(S(N), \Phi) = g\left(k^2 N\right) - g\left(\left(1 - k^2\right) N\right).$$

Exercise 12.63 Show that $I_c(S(N), \Phi)$ is a convex decreasing function of N for $k^2 < \frac{1}{2}$ (correspondingly, a concave increasing function for $k^2 > \frac{1}{2}$), hence

$$\sup_N I_c(S(N), \Phi) = \begin{cases} I_c(S(N), \Phi)|_{N=0} = 0, & k^2 < \frac{1}{2}, \\ \lim_{N\to\infty} I_c(S(N), \Phi) = \log \frac{k^2}{1-k^2}, & k^2 > \frac{1}{2}. \end{cases}$$

In the case $k > 1$ (ideal amplifier), using (12.233), we have $N' = k^2(N + 1) - 1, D = k^2(N + 1) - N$, and

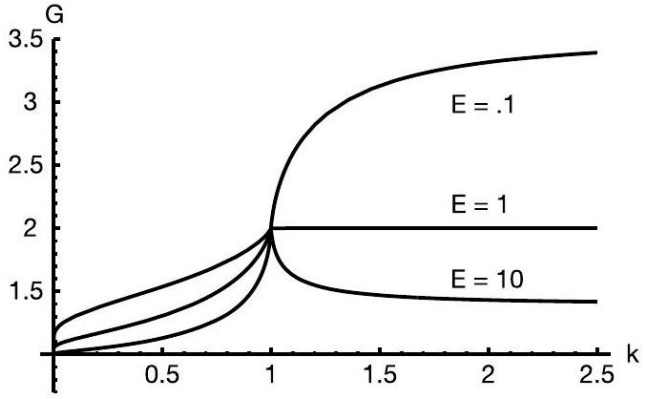


Figure 12.2: The entanglement-assistance gain (12.240) as a function of k for $N_{c =0$. Parameter = the input energy E.}

$$I_c(S(N),\Phi) = g\left(k^2(N+1)-1\right) - g\left(\left(k^2-1\right)(N+1)\right).$$

Exercise 12.64 Show that $I_c(S(N),\Phi)$ is a concave increasing function of N and therefore

$$\sup_N I_c(S(N),\Phi) = \lim_{N\to\infty} I_c(S(N),\Phi) = \log\frac{k^2}{k^2-1}.$$

Summarizing we get the general expression (12.247) for the quantum capacity of the attenuator/amplifier with $N_c = 0$. □

In view of an appropriate infinite-dimensional generalization of Proposition 10.31, a similar expression is obtained for the properly defined private classical capacity C_p of extreme attenuator/amplifier channels.

A vast area of zero quantum capacity, containing the domain (12.229) of the entanglement-breaking channels, is given by the following proposition.

Proposition 12.65. Let $k \geq \frac{1}{\sqrt{2}}$. Then $Q\left(\Phi_{C,k}\right) = 0$ for

$$N_c \geq \frac{1}{2}\left(k^2 - \left|k^2-1\right|\right) = \min\left\{k^2, 1\right\} - \frac{1}{2}. \tag{12.252}$$

Proof. Consider the concatenation $\Phi = \Phi_2 \circ \Phi_1$, where

$$\Phi_1^*[D(\mathbf{z})] = D(\sqrt{2}k\mathbf{z}) \exp\left[-\left(2k^2-1\right)\left(N_1+\frac{1}{2}\right)|\mathbf{z}|^2\right],$$
$$\Phi_2^*[D(\mathbf{z})] = D\left(\frac{\mathbf{z}}{\sqrt{2}}\right) \exp\left[-\frac{1}{2}\left(N_2+\frac{1}{2}\right)|\mathbf{z}|^2\right],$$

so that $Q\left(\Phi_2\right) = 0$ by Proposition 12.62 and hence $Q\left(\Phi_2 \circ \Phi_1\right) = 0$ by (10.35). Then

$$\Phi_1^* \circ \Phi_2^*[D(\mathbf{z})] = D(k\mathbf{z}) \exp\left[-\left(\frac{|k^2-1|}{2} + N_c\right)|\mathbf{z}|^2\right],$$

where

$$\frac{|k^2-1|}{2} + N_c = \frac{1}{2}\left(N_2+\frac{1}{2}\right) + \frac{(2k^2-1)}{2}\left(N_1+\frac{1}{2}\right).$$

By varying $N_1, N_2 \geq 0$ one gets all the values N_C satisfying (12.252). □

In cases (A) and (D) the channel Φ is antidegradable [120] and hence also $Q(\Phi) = 0$ (see Figure 12.3).

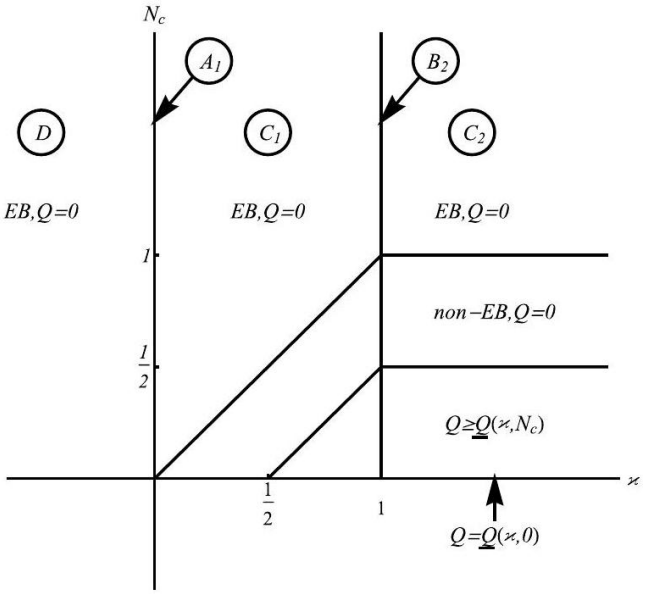


Figure 12.3: The chart of the variety of one-mode gauge-symmetric channels in the invariant coordinates (12.222). EB = entanglement-breaking channel.

The behavior of the capacities $C, C_{ea}, Q = C_p$ of extreme ($N_c = 0$) attenuation/amplification channel as functions of $x = k^2$ is shown in Figure 12.4.

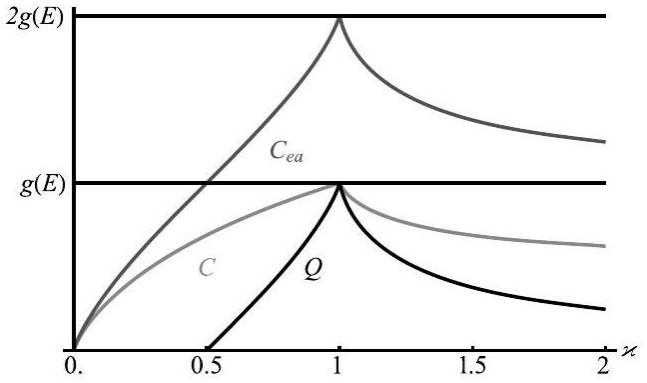


Figure 12.4: Capacities of extreme (quantum-limited, $N_{c =0$) attenuation/amplification channel (signal power $E = 1$)).}

10.12.31 12.7 Notes and References

1. The spectral theorem for self-adjoint operators, Stone's theorem, and related questions are considered in detail in the book of Reed and Simon [193].

The quantum harmonic oscillator, first studied by Dirac [64], underlies many mathematical models in quantum optics and quantum electronics. In particular, useful symbolic calculus leading to algebraic identities following from CCRs such as (12.15) was developed in the book of Louisell [169]. Analysis based on coherent states was developed in the classical work of Glauber [84]. The relation (12.22) is the famous P-representation widely used in quantum optics. Representation of the radiation field as an ensemble of quantum oscillators introduced by Dirac is discussed in the books of Klauder and Sudarshan [155] and Helstrom [103] in the

form suitable for use in quantum optics. For applications of results of the present chapter in lightwave communication see the comprehensive monograph of Papen and Blahut [185].

By using overcompleteness of the system of coherent vectors (Exercise 12.6), one can define the unsharp observable with values in $\mathbb{C} \simeq \mathbb{R}^2$

$$M(B) = \frac{1}{\pi} \int_B |\zeta\rangle\langle\zeta| d^2\zeta, \tag{12.253}$$

which plays a key role in the description of "approximate joint measurement" of observables q and p. A detailed discussion and further references can be found in the books of Davies [56] and Holevo [122].

The formula for the capacity of c-q Gaussian channels was conjectured by Gordon [86]. In our proof we follow [114], where one can also find a consideration of the multimode Gaussian c-q channel including a realistic stochastic process model of classical signals against a background of colored quantum noise. The capacity of channels with squeezed Gaussian noise was computed by Holevo, Sohma, and Hirota in [133]. Much more detailed information concerning the rate of convergence of the error probability for pure state Gaussian channels can be obtained by modifying the estimates from Section 5.7 to channels with infinite alphabets and constrained input [134].

2. The usefulness of the symmetric description (12.48) of CCRs was stressed by Segal [204]. For the proof of the following theorem see, e. g., [122].

Stone-von Neumann uniqueness theorem. Let $V_x, U_y, x, y \in \mathbf{R}^s$ be two strongly continuous families of unitary operators in a separable Hilbert space $\mathcal{H}$ satisfying the Weyl CCR (12.45). Then V_x, U_y are unitarily equivalent to a direct sum of an at most countable number of copies of the Schrödinger representation arising from (12.44). In particular, any irreducible representation is unitarily equivalent to the Schrödinger representation.

The paper of Williamson [252] contains general results concerning normal forms of classical not necessarily positive quadratic Hamiltonians. For the proof of Lemma 12.12 see also Chapter V of the book [122].

Many physical applications of linear dynamics of systems with quadratic Hamiltonians are considered in the book of Malkin and Man'ko [173]. A detailed review of the group of real symplectic transformations with applications to quantum optics and mechanics is given by Arvind, Dutta, Mukunda, and Simon [11].

3. In our exposition of quantum Gaussian states we follow Chapter V of the book [122], where the proofs of Exercises 12.15, 12.16, 12.19 and of sufficiency of the condition (12.80) can be found. In [122] one can find also an accurate treatment of expectations of unbounded operators and moments of a quantum state. The approach to quantum Gaussian states via characteristic functions is based on apparent analogies with probability theory and is perhaps the most direct and transparent. An alternative way used in physical papers is via the Wigner distribution function; see, e.g., [220].

The formulas for entropy of general quantum states were obtained in [133]. The maximum entropy characterization of the Gaussian states (Lemma 12.26) is a particular case of the maximum entropy principle in statistical mechanics (see, e. g., [169], Section 6.6); a similar property with respect to the conditional quantum entropy (Lemma 12.27) was observed by Eisert and Wolf [66].

The separability criterion for Gaussian states was obtained in the paper of Werner and Wolf [244]. This paper also contains important results concerning Gaussian PPT states, in particular, proof that in $1 \times N$ bosonic modes PPT is sufficient for separability of Gaussians and the construction of a family of Gaussian PPT nonseparable (bound entangled) states in a 2×2 system. Purification of Gaussian states was computed in [106].

4. The general description of bosonic linear and Gaussian channels was given in Holevo and

Werner [135] (see also the survey [66]) following [108]. By making a canonical decomposition for a general bosonic Gaussian channel studied in this section, it is possible to show that an arbitrary quantum optical communication circuit can be seen as composed of basic building blocks, comprising linear multiport interferometers and a few basic single-mode "nonlinear" (mathematically - non-gauge covariant) operations, such as parametric down-converters or squeezers [35].

On the other hand, the Gaussian channels are a special case of quasi-free maps of the CCR-algebra considered by Demoen, Vanheuverzwijn, and Verbeure [59]. In [59] the problem of unitary dilation of a quasi-free map was considered under rather special restriction on the operator K. The proof of Theorem 12.32 contains the construction of the unitary dilation for arbitrary Gaussian channels; see Caruso, Eisert, Giovannetti, and Holevo [42] for more detail. Maps which leave globally invariant the set of Gaussian states were studied in [60], in particular, it is shown that a channel having this property is necessarily Gaussian. In [124] it is shown that a Gaussian channel is an extreme point of the convex set of all channels if and only if its correlation matrix is a minimal solution of inequality (12.132).

Gaussian observables are essentially Gaussian q-c channels; they are considered in Chapter VI of the book [122]. In particular, it is shown that the Naimark dilation for the unsharp observable (12.253) is given by the joint spectral measure of commuting operators $q+q_C, p-p_C$, where the mode C is in the vacuum state.

Gaussian entanglement-breaking channels were studied in the work of Holevo [121].

5. The principle "Gaussian channels have Gaussian optimizers" is well known in classical information theory. Theorem 12.38, proved in Holevo and Werner [135], extrapolates this principle to quantum Gaussian states and channels for the mutual quantum information. Proposition 12.40, expressing this principle for the quantum capacity of degradable Gaussian channels, is based on the observation of Wolf, PérezGarcía, and Giedke [258].

There are indications that confirmation of the hypothesis of optimal Gaussian ensembles should depend on the solution of the additivity problem for quantum Gaussian channels. In the paper of Wolf, Giedke, and Cirac [256] it is shown that if the additivity holds, then the average state $\bar{S}_\pi$ of the optimal ensemble should be Gaussian. A closely related conjecture of Gaussian minimizers for entanglement of formation by Wolf et al. was shown to have positive solutions for symmetric Gaussian states in 1×1 composite bosonic systems [257]. Later the condition of symmetry was relaxed; see [4] for a survey of progress in this problem.

In the paper of Giovannetti, Guha, Lloyd, Maccone, Shapiro, and Yuen [80] it was shown that the vacuum state minimizes the output entropy of the single-mode pure loss channel. In this case the minimum is zero implying the additivity. Basing on this, the constrained classical capacity of this channel is easily computed. A breakthrough in the general problem was made in the paper of Giovannetti, Holevo, and GarciaPatron [81], where both hypotheses were proved to hold for a broad class of multimode gauge covariant or contravariant channels. Such channels are of main interest in quantum optics, where they are called phase-insensitive channels.

In our exposition of the solution we follow the survey [125]. Proposition 12.42 generalizes to many modes the decomposition of single-mode channels, the usefulness of which was emphasized and exploited in the paper [79] (see also [41] on concatenations of single-mode channels). Lemma 12.53 is based on a key observation by Giovannetti.

The basic Theorem 12.52 for one mode was obtained in [174]. Here we present a complete proof in the multimode case, a sketch of which was given in [82].

A mathematical model of quantum communication channels with time-continuous additive stationary Gaussian noise was considered in [128]. The multimode capacity formula (12.211) was applied to compute the classical capacity of quantum Gaussian "broadband" gauge covariant channels in spectral terms.

By taking $f(x) = -x^p, p > 1$, Theorem 12.52 implies the multiplicativity property of the (

$1 \to p$)-norms of the Gaussian channels, defined as

$$\|\Phi\|_{1\to p} = \sup_{X\neq 0} \|\Phi[X]\|_p / \|X\|_1 = \sup_{\|X\|_1\leq 1} \|\Phi[X]\|_p,$$

where $\|\cdot\|_p$ is the Schatten p-norm, and hence the additivity of the output Rényi entropies of arbitrary order $p > 1$. The problem of Gaussian maximizers for similarly defined ($q \to p$)-norms, $q < p$, remains in general open, while for $q = p$ the norm is attained asymptotically on a sequence of Gaussian states for arbitrary (not necessarily gauge covariant) Gaussian channels [71], [127]. For a survey of partial results in these directions as well as other related hypotheses, see [61].

6. The classification of one-mode Gaussian channels was obtained by Holevo [121]; see also [41]. A detailed study of their structure based on explicitly described Kraus decompositions is given in the paper of Ivan, Sabapathy, and Simon [143]. On the other hand, in the case of more than one mode the structure of nongauge covariant Gaussian channels is far from clear; see, e. g., [126].

The capacities of the attenuation/amplification channel were considered by Holevo and Werner [135], where formula (12.239) for the classical capacity was conjectured. The fact that the quantum capacity is given by the Gaussian expression obtained in [135] was proved by Wolf, Pérez-García, and Giedke [258]. The regions of zero quantum capacity were described in Caruso, Giovannetti, and Holevo [41]. Solutions of the exercises from Section 12.6.4 and additional information on the channel with additive classical Gaussian noise are given in the paper [120]. In the case $N_c > 0$ (thermal noise in the environment) bounds on the quantum capacity of attenuation/amplification channels were developed in [250], [207], [195]; see also references therein. Smith, Smolin, and Yard [223] demonstrated superactivation of quantum capacity for the couple of zero-capacity Gaussian channels: one-mode attenuators with $k^2 = 1/2$ and an explicitly constructed two-mode PPT channel.

Numerous physical applications of continuous-variable (in particular bosonic Gaussian) information processing systems, including experimental realizations, are discussed in the surveys [36], [241].

10.12.32 Bibliography

[1] A. Abeyesinghe, I. Devetak, P. Hayden and A. Winter, The mother of all protocols: restructuring quantum information's family tree, Proc. R. Soc. A 465(2108) (2009), pp. 2537-63; arXiv:quant-ph/0606225 (2006).

[2] C. Adami and N. J. Cerf, Capacity of noisy quantum channels, Phys. Rev. A 56 (1997), pp. 3470-85.

[3] R. Ahlswede and I. Csiszár, Common randomness in information theory and cryptography Part II: CR capacity, IEEE Trans. Inform. Theory 44 (1998), pp. 225-40.

[4] Y. Akbari-Kourbolagh and H. Alijanzadeh-Boura, On the entanglement of formation of two-mode Gaussian states: a compact form, Quantum Information Processing 14(11) (2015), pp. 4179-99; arXiv:1402.3321v2.

[5] R. Ahlswede and A. Winter, Strong converse for identification via quantum channels, IEEE Trans. Inf. Theory 48 (2002), pp. 569-79.

[6] G. Alber, T. Beth, M. Horodecki, P. Horodecki, R. Horodecki, M. Rötteler, H. Weinfurter and R. F. Werner, Quantum Information. An Introduction to Basic Theoretical Concepts and Experiments, Springer, Berlin, 2001.

[7] R. Alicki, Isotropic quantum spin channels and additivity questions, arXiv:quant-ph/0402080 (2004).

[8] H. Araki, On a characterization of the state space in quantum mechanics, Commun.Math.

Phys. 75 (1980), pp. 1-24.
[9] P. K. Aravind, Quantum misteries revisited again, Am. J. Phys. 72 (2004), pp. 1303-7.
[10] W. B. Arveson, Subalgebras of C*-algebras, Acta Math. 123 (1969), pp. 141-224.
[11] Arvind, B. Dutta, N. Mukunda, and R. Simon, The real symplectic groups in quantum mechanics and optics, Pramana 45 (1995), pp. 471.
[12] G. Aubrun and S. Szarek, Alice and Bob Meet Banach: The Interface of Asymptotic Geometric Analysis and Quantum Information Theory, AMS Mathematical Surveys and Monographs, 223, 2017, 414 pp.
[13] G. Aubrun, S. Szarek and E. Werner, Hastings' additivity counterexample via Dvoretzky's theorem, Comm. Math. Phys. 305 (2011), pp. 85-97; arXiv:1003.4925 [quant-ph] (2010).
[14] K. M. R. Audenaert, A sharp Fannes-type inequality for the von Neumann entropy, J. Phys. A 40 (2007), pp. 8127-36; arXiv:quant-ph/0610146 (2006).
[15] K. M. R. Audenaert and S. L. Braunstein, On strong superadditivity of the entanglement of formation, Commun. Math. Phys. 246 (2004), pp. 443-52.
[16] P. A. Bakut and S. S. Shchurov, Optimal detection of quantum signal, Probl. Inform. Transmission 4 (1968), pp. 61-5.
[17] H. Barnum, E. Knill and M. A. Nielsen, On quantum fidelities and channel capacities, IEEE Trans. Inform. Theory 46 (1998), pp. 1317-29; arXiv:quant-ph/9809010.
[18] H. Barnum, M. A. Nielsen and B. Schumacher, Information transmission through a noisy quantum channel, Phys. Rev. A 57 (1998), pp. 4153-75.
[19] S. Beigi, Sandwiched Renyi Divergence Satisfies Data Processing Inequality, J. Math. Phys. 54 (2013) 122202; arXiv:1306.5920.
[20] V. P. Belavkin, Optimal multiple quantum statistical hypotheses testing, J. Stoch. 1 (1975), pp. 315-45.
[21] J. S. Bell, On the Einstein-Podolsky-Rosen paradox, Physics 1 (1964), pp. 195-200.
[22] C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A Peres and W. K. Wootters, Teleporting an unknown quantum state via dual classical and EPR channels, Phys. Rev. Lett. 70 (1993), pp. 1855-9.
[23] C.H. Bennett, I. Devetak, A. W. Harrow, P. W. Shor and A. Winter, Quantum Reverse Shannon Theorem, IEEE Trans. Inf. Theory. 60(5) (2014), pp. 2926-59; arXiv:0912.5537.
[24] C. H. Bennett, I. Devetak, P. W. Shor and J. A. Smolin, Inequalities and separations among assisted capacities of quantum channels, arXiv:quant-ph/0406086 (2004).
[25] C.H. Bennett, D. P. DiVincenzo, J. A. Smolin and W. K. Wootters, Mixed state entanglement and quantum error correction, Phys. Rev. A 54 (1996), pp. 3824-51; arXiv:quant-ph/9604024 (1996).
[26] C. H. Bennett, C. A. Fuchs and J. A. Smolin, Entanglement-enhanced classical communication on a noisy quantum channel, in Quantum Communication, Computing and Measurement, Proc. QCM96, ed. by O. Hirota, A. S. Holevo and C. M. Caves, Plenum, New York, 1997, pp.79-88; arXiv:quant-ph/9611006.
[27] C. H. Bennett and P. W. Shor, Quantum information theory, IEEE Trans. Inform. Theory 44 (1998), pp. 2724-42.
[28] C.H. Bennett, P. W. Shor, J. A. Smolin and A. V. Thapliyal, Entanglement-assisted classical capacity of noisy quantum channel, Phys. Rev. Lett. 83 (1999), pp. 3081; arXiv:quant-ph/9904023.
[29] C.H. Bennett, P. W. Shor, J. A. Smolin and A. V. Thapliyal, Entanglement-assisted capacity and the reverse Shannon theorem, IEEE Trans. Inform. Theory 48 (2002), pp. 2637-55; arXiv:quant-ph/0106052.
[30] C.H. Bennett and S. J. Wiesner, Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states, Phys. Rev. Lett. 69 (1992), pp. 2881-4.
[31] R. Bhatia, Matrix Analysis, Springer, New York, 1997.

[32] I. Bjelaković and R. Siegmund-Schultze, Quantum Stein's lemma revisited, inequalities for quantum entropies, and a concavity theorem of Lieb, arXiv:quant-ph/0307170v2.
[33] G. Bowen, Quantum Feedback Channels, IEEE Trans. Inform. Theory 50 (2004), pp. 2429-33.
[34] F. G. L. S. Brandão, M. Horodecki, On Hastings' counterexample to the minimum output entropy additivity conjectures, Open Syst. Inf. Dyn. 17 (2010), pp. 31; arXiv:0907.3210.
[35] S. L. Braunstein, Squeezing as an irreducible resource, Phys. Rev. A 71 (2005) 055801; arXiv:quant-ph/9904002v2.
[36] S. L. Braunstein and P. van Loock, Quantum information with continuous variables, Rev. Mod. Phys. 77 (2005), pp. 514-77.
[37] M. V. Burnashev and A. S. Holevo, On reliability function of quantum communication channel, Probl. Inform. Transm. 34 (1998), pp. 97-107.
[38] N. Cai, A. Winter and R. W. Yeung, Quantum privacy and quantum wiretap channels, Probl. Inform. Transmission 40 (2004), pp. 318-36.
[39] R. Calderbank and P. W. Shor, Good quantum error-correcting codes exist, Phys. Rev. A 54 (1996), pp. 1098-105.
[40] E. A. Carlen, Trace inequalities and quantum entropy. An introductory course, Contemp. Math. 529 (2010), 73.
[41] F. Caruso, V. Giovannetti and A. S. Holevo, One-mode Bosonic Gaussian channels: a full weak-degradability classification, New J. Phys. 8 (2006), 310; arXiv:quant-ph/0609013.
[42] F. Caruso, J. Eisert, V. Giovannetti, A. S. Holevo, Multi-mode bosonic Gaussian channels, New J. Phys. 10 (2008), 083030, 33 pp.; arXiv:0804.0511 [quant-ph].
[43] C. M. Caves and P. B. Drummond, Quantum limits of bosonic communication rates, Rev. Mod. Phys. 66 (1994), pp. 481-538.
[44] N. N. Chentsov, Selected works. Mathematics. Part IV. Geometrostatistics and noncommutative probability, Fizmatlit, Moscow, 2001. (in Russian).
[45] G. Chiribella, G. M. D'Ariano and P. Perinotti, Informational derivation of quantum theory, Phys. Rev. A 84 (2011), 012311; arXiv:1011.6451 [quant-ph].
[46] M.-D. Choi, Completely positive maps on complex matrices, Linear Alg. and Its Appl. 10 (1975), pp. 285-90.
[47] T. M. Cover and J. A. Thomas, Elements of Information Theory, 2nd edition, John Wiley & Sons, New York, 1996.
[48] T.Cubitt, D.Elkouss, W.Matthews, M.Ozols, D. Perez-Garcia and S. Strelchuk Unbounded number of channel uses are required to see quantum capacity, Nat. Commun. 6 (2015), 7739; arXiv:1408.5115.
[49] T. S. Cubitt, M.-B. Ruskai and G. Smith, The structure of degradable quantum channels, J. Math. Phys. 49 (2008) 102104; arXiv:0802.1360 [quant-ph] (2008).
[50] I. Cziszár and J. Körner, Information Theory. Coding Theorems for Discrete Memoryless Systems, Akadémiai Kiadó, Budapest, 1981.
[51] M. Dalai, Sphere packing and zero-rate bounds to the reliability of classical-quantum channel, arXiv:1201.5411 [cs.IT] (2012).
[52] M. Dalai, Lower bounds on the probability of error for classical and classical-quantum channels, IEEE IT Trans. 51 (2013), pp. 8027-56.
[53] M. Dall'Arno, G. M. D'Ariano and M. F. Sacchi, Informational power of quantum measurements, Phys. Rev. A 83 (2011) 062304; arXiv:1103.1972.
[54] G. M. D'Ariano, G. Chiribella and P. Perinotti, Quantum Theory from First Principles : An Informational Approach, Cambridge University Press, 2017.
[55] E. B. Davies, Information and quantum measurement, IEEE Trans. Inform. Theory 24 (1978), pp. 596-9.
[56] E. B. Davies, Quantum Theory of Open Systems, Academic Press, London, 1976.

[57] N. Davis, M. E. Shirokov and M. M. Wilde, Energy-constrained two-way assisted private and quantum capacities of quantum channels, Phys. Rev. A 97(6) (2018) 062310; arXiv:1801.08102.
[58] G. F. Dell'Antonio, On the limits of sequences of normal states, Commun. Pure Appl. Math. 20 (1967), pp. 413-30.
[59] B. Demoen, P. Vanheuverzwijn and A. Verbeure, Completely positive quasi-free maps on the CCR algebra, Rep. Math. Phys. 15 (1979), pp. 27-39.
[60] G. De Palma, A. Mari, V. Giovannetti and A. S. Holevo, Normal form decomposition for Gaussian-to-Gaussian superoperators, J. Math. Phys. 56(5) (2015), 052202.
[61] G. De Palma, D. Trevisan, V. Giovannetti and L. Ambrosio, Gaussian optimizers for entropic inequalities in quantum information, J. Math. Phys. 59(8) (2018), 081101.
[62] I. Devetak, The private classical information capacity and quantum information capacity of a quantum channel, arXiv:quant-ph/0304127v6.
[63] I. Devetak and P. Shor, The capacity of a quantum channel for simultaneous transition of classical and quantum information, arXiv:quant-ph/0311131v3.
[64] P. A. M. Dirac, The Principles of Quantum Mechanics, 4th edition, Oxford Univ. Press, Oxford, 1958, (1930).
[65] D. Di Vincenzo, P. W. Shor, J. Smolin, Quantum channel capacities of very noisy channels, Phys. Rev. A 57 (1998), pp. 830-9.
[66] J. Eisert and M. M. Wolf, Gaussian quantum channels, in Quantum Information with Continuous Variables of Atoms and Light, Imperial College Press, London, 2007, pp. 23-42; arXiv:quant-ph/0505151.
[67] E. G. Effros, A matrix convexity approach to some celebrated quantum inequalities, Proc. Natl. Acad. Sci. USA 106 (2009), pp. 1006-8; arXiv:math-ph/0802.1234.
[68] L. D. Faddeev and O. A. Yakubovskii, Lectures on Quantum Mechanics for Mathematics Students (Student Mathematical Library), AMS, 2009.
[69] M. Fannes, A continuity property of quantum entropy for spin lattice systems, Commun. Math.
Phys. 31 (1973), pp. 291-4.
[70] R. P. Feynman, R. B. Leighton and M. Sands, The Feynman Lectures on Physics, vol. 3, Addison-Wesley Publishing Company, Inc., Reading, Massachusetts, Paolo Alto, London, 1965.
[71] Frank R. L., Lieb E. H. Norms of quantum Gaussian multi-mode channels, arXiv:1704.08720v3.
[72] G. D. Forney, Jr., M.S. Thesis, MIT, 1963.
[73] A. Hartkamper, H. Neumann, Foundations of Quantum Mechanics and Ordered Linear Spaces. Lect. Notes Phys. 29, Springer-Verlag, New York-Heidelberg-Berlin, 1974.
[74] C.A. Fuchs, Distinguishability and accessible information in quantum theory, Ph.D. Dissertation, University of New Mexico; arXiv:quant-ph/9601020.
[75] C.A. Fuchs, Quantum mechanics as quantum information (and only a little more), arXiv:quant-ph/0205039v1.
[76] M. Fukuda, C. King and D. Moser, Comments on Hastings' additivity counterexamples, Commun. Math. Phys. 296 (2010), pp. 111-43; arXiv:0905.3697.
[77] M. Fukuda and M. M. Wolf, Simplifying additivity problems using direct sum constructions, J. Math. Phys. 48 (2007), 072101.
[78] R. Gallager, Information Theory and Reliable Communications, Wiley, New York, 1968.
[79] R. García-Patrón, C. Navarrete-Benlloch, S. Lloyd, J. H. Shapiro and N. J. Cerf, Majorization theory approach to the Gaussian channel minimum entropy conjecture, Phys. Rev. Lett. 108 (2012), 110505.
[80] V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, J. H. Shapiro and H. P. Yuen, Classical

capacity of the lossy bosonic channel: the exact solution, Phys. Rev. Lett. 92 (2004), 027902; arXiv:quant-ph/0308012.
[81] V. Giovannetti, A. S. Holevo and R. Garcia-Patron, A solution of Gaussian optimizer conjecture for quantum channels, Commun. Math. Phys. 334(3) (2015), 1553-71.
[82] V.Giovannetti, A. S.Holevo and A.Mari, Majorization and additivity for multimode bosonic Gaussian channels, Theor. Math. Phys., 182:2 (2015).
[83] I. M. Glazman and Ju. I. Ljubich, Finite-Dimensional Linear Analysis: A Systematic Presentation in Problem Form, MIT Press, Cambridge, Massachusetts, 1974.
[84] R. J. Glauber, The quantum theory of optical coherence, Phys. Rev. 130 (1963), pp. 2529-39.
[85] J. P. Gordon, Quantum effect and communications systems, Proc. IRE 50 (1962), pp. 1898-908.
[86] J. P. Gordon, Noise at optical frequencies; information theory, in Quantum Electronics and Coherent Light, Proc. Int. School Phys. "Enrico Fermi", Course XXXI, ed. by P. A. Miles, Academic Press, New York, 1964, pp. 156-81.
[87] D. Gottesman, Stabilizer codes and quantum error correction, Ph. D. Thesis, Caltech, 1997; arXiv:quant-ph/9705052.
[88] A. Grudka, M. Horodecky and L. Pankowski, Constructive counterexamples to additivity of minimum output Rényi entropy of quantum channels for all $p > 2$, J. Phys. A: Math. Theor. 43 (2010) 425304; arXiv:0911.2515v2.
[89] M. J. W. Hall, Quantum information and correlation bounds, Phys. Rev. A 55 (1997), pp.1050-2947.
[90] M. J. W. Hall, Entropic Heisenberg limits and uncertainty relations from the Holevo information bound, J. Phys. A 51 (2018) 364001; arXiv:1804.01343.
[91] R. Hanson et al., Experimental loophole-free violation of a Bell inequality using entangled electron spins separated by 1.3 km, arXiv:1508.05949.
[92] L. Hardy, Reformulating and reconstructing quantum theory, arXiv:1104.2066v3.
[93] M. B. Hastings, A counterexample to additivity of minimum output entropy, Nature Phys. 5 (2009), 255; arXiv:quant-ph/0809.3972.
[94] P. Hausladen, R. Jozsa, B. Schumacher, M. Westmoreland and W. Wootters: Classical information capacity of a quantum channel, Phys. Rev. A 54 (1996), pp. 1869-76.
[95] M. Hayashi, Quantum Information: an Introduction, Springer, Berlin, 2006.
[96] M. Hayashi and H. Nagaoka, General formulas for capacity of classical-quantum channels, IEEE Trans. Inform. Theory 49 (2003), pp. 1753-68; arXiv:quant-ph/0206186.
[97] P. Hayden, The maximal p-norm multiplicativity conjecture is false, arXiv:0707.3291.
[98] P. Hayden, Entanglement in random subspaces, in Proc. of QCMC04. AIP Conference Proceedings, 734, pp. 226-9, 2004; arXiv:quant-ph/0409157.
[99] P. Hayden, D. Leung, P. W. Shor and A. Winter, Randomizing quantum states: constructions and applications, Communications in Mathematical Physics 250 (2004), pp. 371-91.
[100] P. Hayden and A. Winter, Counterexamples to the maximal p-norm multiplicativity conjecture for all $p > 1$, Comm. Math. Phys. 284 (2008), pp. 263-80; arXiv:0807.4753.
[101] P. Hayden, P. W. Shor and A. Winter, Random quantum codes from Gaussian ensembles and an uncertainty relation, Open Syst. Inf. Dyn. 15 (2008), pp. 71-89; arXiv:quant-ph/0712.0975.
[102] C. W. Helstrom, Detection theory and quantum mechanics, Inform. and Control 10 (1967), pp. 254-91.
[103] C. W. Helstrom, Quantum Detection and Estimation Theory, Academic Press, New York, 1976.
[104] U. Herzog, Optimum state discrimination with a fixed rate of inconclusive results:

Analytical solutions and relation to state discrimination with a fixed error rate, arXiv:1206.4412 [quant-ph].
[105] W. Hoeffding, Probability inequalities for sums of bounded random variables, J. Amer. Statist. Assoc. 58 (1963), pp. 13-30.
[106] A. S. Holevo, Generalized free states of the C^*-algebra of the CCR. Theor. Math. Phys. 6(1) (1971), pp. 1-12.
[107] A. S. Holevo, Statistical problems in quantum physics, in 2nd Japan-USSR Symp. on Probability Theory 1, Kyoto (1972), pp. 22-40.
[108] A. S. Holevo, Towards a mathematical theory of quantum communication channels, Probl. Inform. Transm. 8 (1972), pp. 63-71.
[109] A. S. Holevo, On quasiequivalence of locally normal states, Theor. Math. Phys., 13 (1972), pp. 184-99.
[110] A. S. Holevo, Information-theoretic aspects of quantum measurement, Probl. Inform. Transm. 9 (1973), pp. 31-42.
[111] A. S. Holevo, Some estimates for the information content transmitted by a quantum communication channel, Probl. Inform Transm. 9 (1973), pp. 3-11.
[112] A. S. Holevo, Statistical definition of observable and the structure of statistical models, Rep. Math. Phys. 22 (1985), pp. 385-407.
[113] A. S. Holevo, The capacity of quantum communication channel with general signal states, IEEE Trans. Inform. Theory 44 (1998), pp. 269-72; arXiv:quant-ph/9611023 (1996).
[114] A. S. Holevo, Quantum coding theorems, Russian Math. Surveys 53 (1998), pp. 1295-331; arXiv:quant-ph/9809023.
[115] A. S. Holevo, Statistical Structure of Quantum Theory, Lect. Notes Phys. m67 Springer, Berlin, 2001.
[116] A. S. Holevo, On entanglement-assisted classical capacity, J. Math. Phys. 43, (2002), pp. 4326-33; arXiv:quant-ph/0106075.
[117] A. S. Holevo, Classical capacities of quantum channels with constrained inputs, Probab. Theory and Appl. 48 (2003), pp. 359-74; arXiv:quant-ph/0211170.
[118] A. S. Holevo, On complementary channels and the additivity problem, Probab. Theory and Appl. 51 (2006), pp. 133-4; arXiv:quant-ph/0509101.
[119] A. S. Holevo, The additivity problem in quantum information theory, in Proc. ICM, Madrid, Spain, 2006, pp. 999-1018.
[120] A. S. Holevo, One-mode quantum Gaussian channels, Probl. Inform. Transmission 43 (2007), pp. 1-11; arXiv:quant-ph/0607051.
[121] A. S. Holevo, Entanglement-breaking channels in infinite dimensions, Probl. Inform. Transmission 44 (2008), pp. 3-18; arXiv:quant-ph/0802.0235.
[122] A. S. Holevo, Probabilistic and Statistical Aspects of Quantum Theory, 2nd edition, Edizioni della Normale, Pisa, 2011.
[123] A. S. Holevo, Information capacity of quantum observable, Probl. Inform. Transmission, 48(1) (2012), pp. 1-10; arXiv:1103.2615 [quant-ph].
[124] A. S. Holevo, Extreme bosonic linear channels, Theor. Math. Phys., 174(2) (2013), pp. 288-97.
[125] A. S. Holevo, Gaussian optimizers and the additivity problem in quantum information theory, Russian Math. Surveys, 70(2) (2015), 331-67.
[126] A. S. Holevo, On the constrained classical capacity of infinite-dimensional covariant quantum channels, J. Math. Phys. 57(1) (2016), pp. 15203, 11 pp.
[127] A. S. Holevo, On the quantum Gaussian optimizers conjecture in the case $q = p$, Russian Math. Surveys, 72(6) (2017), pp. 1177-9.
[128] A. S. Holevo, On the classical capacity of a channel with stationary quantum gaussian noise, Theory Probab. Appl., 62(4) (2018), pp. 534-51.

[129] A. S. Holevo, M. E. Shirokov, On Shor's channel extension and constrained channels, Commun. Math. Phys. 249 (2004), pp. 417-30; arXiv:quant-ph/0306196.
[130] A. S. Holevo and M. E. Shirokov, Continuous ensembles and the x-capacity of infinite dimensional channels, Probab. Theory and Appl. 50 (2005), pp. 98-114.
[131] A. S. Holevo and M. E. Shirokov, On the entanglement-assisted classical capacity of infinite-dimensional quantum channels, Probl. Inform. Transmission 49(1) (2013), pp. 15-31; arXiv:1210.6926v2.
[132] A. S. Holevo, M. E. Shirokov and R. F. Werner, On the notion of entanglement in infinite dimensional spaces, Russian Math. Surveys 60 (2005), pp. 153-4.
[133] A. S. Holevo, M. Sohma and O. Hirota, Capacity of quantum Gaussian channels, Phys. Rev. A 59 (1999), pp. 1820-8.
[134] A. S. Holevo, M. Sohma, O. Hirota, Error exponents for quantum channels with constrained inputs, Rep. Math. Phys. 46 (2000), pp. 343-58.
[135] A. S. Holevo and R. F. Werner, Evaluating capacities of Bosonic Gaussian channels, Phys. Rev. A 63 (2001), 032312; arXiv:quant-ph/9912067 (1999).
[136] M. Horodecki, P. Horodecki and R. Horodecki, Separability of mixed states: necessary and sufficient conditions, Phys. Lett A 223 (1996), pp. 1-8.
[137] P. Horodecki, Separability criterion and inseparable mixed states with positive partial transposition, Phys.Lett. A 232 (1997), pp. 333; arXiv:quant-ph/9703004 (1997).
[138] M. Horodecki, P. Horodecki and R. Horodecki, Unified approach to quantum capacities:towards quantum noisy coding theorem, Phys. Lett. 85 (2000), pp. 433-6.
[139] P. Horodecki, M. Horodecki and R. Horodecki Binding entanglement channels, J. Mod. Opt. 47 (2000), pp. 347-54.
[140] R. Horodecki, P. Horodecki, M. Horodecki and K. Horodecki, Quantum entanglement, Rev. Mod. Phys. 81 (2009), pp. 865-942.
[141] M. Horodecki, J. Oppenheim and A. Winter, Quantum state merging and negative information, Comm. Math. Phys. 269 (2006), pp. 107; arXiv:quant-ph/0512247.
[142] M. Horodecki, P. W. Shor and M. B. Ruskai, General entanglement breaking channels, Rev. Math. Phys. 15 (2003), pp. 629-41; arXiv:quant-ph/0302031.
[143] J. S. Ivan, K. Sabapathy and R. Simon, Operator-sum representation for Bosonic Gaussian channels, Phys. Rev. A 84 (2011), 042311.
[144] A. Jamiolkowski, Linear transformations which preserve trace and positive semidefiniteness
of operators, Rep. Math. Phys. 3 (1972), 275-8.
[145] R. Jozsa, D. Robb and W. K. Wootters, Lower bound for accessible information in quantum mechanics, Phys. Rev. A 9 (1994), pp. 668-77.
[146] R. Jozsa and B. Schumacher: A new proof of the quantum noiseless coding theorem, J. Modern Optics 41 (1994), pp. 2343-9.
[147] K. Kato, M. Osaki and O. Hirota, Derivation of classical capacity of quantum channels for discrete information sources, arXiv:quant-ph/9811085v1.
[148] K. Kato, M. Osaki, T. Suzuki, M. Ban and O. Hirota, Upper bound of the accessible information and lower bound of the Bayes cost in quantum signal detection processes, Phys. Rev. A 54 (1996), 2718-27.
[149] M. Keyl, Fundamentals of quantum information theory Phys. Rep. 369 (2002), pp. 431-548, arXiv:quant-ph/0202122.
[150] C. King, Additivity for unital qubit channels, J. Math. Phys. 43 (2002), pp. 4641-3; arXiv:quant-ph/0103156.
[151] C. King, The capacity of quantum depolarizing channel, IEEE Trans. Inf. Th. 49 (2003), pp. 221-9; arXiv:quant-ph/0204172.
[152] C. King, K. Matsumoto, M. Natanson and M. B. Ruskai, Properties of conjugate

channels with applications to additivity and multiplicativity, Markov Process and Related Fields 13 (2007), pp. 391-423; arXiv:quant-ph/0509126.
[153] E. Knill and R. Laflamme, Theory of quantum error-correcting codes, Phys. Rev. A 55 (1997), pp. 900-11.
[154] A. Yu. Kitaev, Quantum computations: algorithms and error-correction, Russian Math. Surveys 52 (1997), pp. 1191-249.
[155] J. R. Klauder and E. C. G. Sudarshan, Fundamentals of Quantum Optics, Benjamin, New York, 1968.
[156] A.I. Kostrikin and Yu.I. Manin, Linear Algebra and Geometry, Gordon and Breach Scientific Publications, 1989.
[157] K. Kraus, States, Effects and Operations, Springer Lecture Notes in Physics 190, 1983.
[158] D. Kretschmann and R. Werner, Tema con variazioni: quantum channel capacities, New J. Phys. 6 (2004), 26; arXiv:quant-ph/0311037.
[159] D. Kretschmann, R. Werner, Quantum channels with memory Phys. Rev. A 72 (2005), 062323; arXiv:quant-ph/0502106.
[160] D. S. Lebedev and L. B. Levitin, The maximal amount of information transmissible by an electromagnetic field, Doklady AN SSSR 149 (1963), pp. 1299-303.
[161] A. Lesniewski and M. B. Ruskai, Monotone Riemannian metrics and relative entropy on noncommutative probability spaces, J. Math. Phys. 40 (1999), pp. 5702-24.
[162] L. B. Levitin, Optimal quantum measurement for two pure and mixed states, in Quantum Communications and Measurement, Proc. QCM94, ed. by V. P. Belavkin, O. Hirota, R. L. Hudson, Plenum, New York 1995, pp. 439-48.
[163] E. H. Lieb and M. B. Ruskai, Proof of the strong subadditivity of quantum mechanical entropy, J. Math. Phys., 14 (1973), pp. 1938-41.
[164] G. Lindblad, Entropy, information and quantum measurements, Commun. Math. Phys. 33 (1973), pp. 305-22.
[165] G. Lindblad, Expectations and entropy inequalities for finite quantum systems, Commun. Math. Phys. 39 (1974), pp. 111-9.
[166] G. Lindblad: Completely positive maps and entropy inequalities, Commun. Math. Phys. 40 (1975), pp. 147-51.
[167] G. Lindblad, Quantum entropy and quantum measurements, in Quantum Aspects of Optical Communication, ed. by C. Benjaballah, O. Hirota, S. Reynaud, Lect. Notes Phys., 378, 1991,
pp. 71-80.
[168] S. Lloyd, Capacity of noisy quantum channel, Phys. Rev. A 55 (1997), pp. 1613-22.
[169] W. Louisell, Radiation and Noise in Quantum Electronics, McGraw-Hill, New York, 1964.
[170] G. Ludwig, Foundations of Quantum Mechanics I, Springer, Berlin-Heidelberg-New York, 1983.
[171] G. W. Mackey, Mathematical Foundations of Quantum Mechanics, Benjamin, New York, 1963.
[172] G. G. Magaril-Ilyaev and V. M. Tikhomirov, Convex Analysis: Theory and Applications, Translations of Mathematical Monographs 222, AMS, 2003.
[173] I. A. Malkin and V. I. Man'ko, Dynamical Symmetries and Coherent States of Quantum Systems, Nauka, Moscow, 1979 (in Russian).
[174] A.Mari, V.Giovannetti and A. S.Holevo, Quantum state majorization at the output of bosonic Gaussian channels, Nature Communications, 5 (2014), 3826.
[175] LI. Masanes and M. P. Müller, A derivation of quantum theory from physical requirements, New J. Phys. 13 (2011), 063001.
[176] K. Matsumoto, T. Shimono and A. Winter, Remarks on the additivity of the Holevo

channel capacity and of the entanglement of formation, Commun. Math. Phys. 246 (2004), pp. 427-42; arXiv:quant-ph/0206148 (2002).
[177] M. Mosonyi and T. Ogawa, Strong converse exponent for classical-quantum channel coding, Commun. Math. Phys. 355(1) (2017), pp. 373-426; arXiv:1409.3562.
[178] A. Müller-Hermes and D. Reeb, Monotonicity of the Quantum Relative Entropy Under Positive Maps, Ann. H. Poincare 18 (2017), pp. 1777-88; arXiv:1512.06117.
[179] M. A. Nielsen and I. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, 2000.
[180] M. A. Naimark, Spectral functions of a symmetric operator, Izv. Acad. nauk SSSR Ser. Mat. 4 (1940), pp. 277-318. (in Russian).
[181] T. Ogawa and H. Nagaoka, Strong converse and Stein's lemma in quantum hypothesis testing, IEEE Trans. Inf. Theory, 46 (2000), pp. 2428-33.
[182] M. Ohya and D. Petz, Quantum Entropy and Its Use, Texts and Monographs in Physics, Springer, New York, 1993.
[183] M. Ozawa, On information gain by quantum measurement of continuous observable, J. Math. Phys. 27 (1986), pp. 759-63.
[184] M. Ozawa, Quantum measuring process of continuous observables, J. Math. Phys. 18 (1987), pp. 412-21.
[185] G. C. Papen and R. E. Blahut, Lightwave communication, Cambridge University Press, 2019.
[186] K. R. Parthasarathy, Probability Measures on Metric Spaces, Academic Press, New York and London, 1967.
[187] A. Peres, Phys. Lett. A 128 (1988), pp. 19.
[188] A. Peres, Phys. Rev. Lett. 76 (1997), pp. 1413.
[189] D. Petz, Quasi-entropies for finite quantum systems, Rep. Math. Phys. 21 (1986), pp. 57-65.
[190] D. Petz, Quantum Information Theory and Quantum Statistics, Springer, Berlin, 2008.
[191] R. T. Powers and E. Störmer, Free states on the canonical anticommutation relations, Commun. Math. Phys. 16 (1970), pp. 1-33.
[192] E. M. Rains, Bound on distillable entanglement, Phys. Rev. A 60 (1999), 179-84.
[193] M. Reed and B. Simon, Methods of Modern Mathematical Physics, Vol. 1. Functional Analysis, Academic Press, London, 1980.
[194] R. T. Rockafellar, Convex Analysis, Princeton University Press, Princeton, NJ, 1970.
[195] M. Rosati, A. Mari and V. Giovannetti Narrow Bounds for the Quantum Capacity of Thermal Attenuators, Nature Commun. 9 (2018), pp. 4339; arXiv:1801.04731.
[196] M. B. Ruskai, Inequalitues for quantum entropy: A review with conditions for equality, J. Math. Phys. 43 (2002), pp. 4358-75.
[197] M. B. Ruskai, S. Szarek and E. Werner, An analysis of completely-positive trace-preserving maps on 2×2 matrices, Lin. Alg. Appl. 347 (2002), pp. 159-87; arXiv:quant-ph/0101003v2.
[198] T. A. Sarymsakov, Introduction to Quantum Probability Theory, FAN, Tashkent, 1985. (in Russian).
[199] M. Sasaki, S. M. Barnett, R. Jozsa, M. Osaki and O. Hirota, Accessible information and optimal strategies for real symmetric quantum sources, Phys. Rev. A 59 (1999), 3325; arXiv:quant-ph/9812062.
[200] B. Schumacher and M. D. Westmoreland, Sending classical information via noisy quantum channel, Phys. Rev. A. 56 (1997), pp. 131-8.
[201] B. Schumacher and M. D. Westmoreland, Quantum privacy and quantum coherence, Phys. Rev. Lett. 80 (1998), pp. 5695-7; arXiv:quant-ph/9709058.
[202] B. Schumacher and M. D. Westmoreland, Optimal signal ensembles,

arXiv:quant-ph/9912122.
[203] B. Schumacher and M. D. Westmoreland, Approximate quantum error correction, arXiv:quant-ph/0112106.
[204] I. Segal, Mathematical Problems of Relativistic Physics, AMS, Providence, RI, 1963.
[205] L. K. Shalm et al., A strong loophole-free test of local realism, Phys. Rev. Lett. 115 (2015) 250402; arXiv:1511.03189v2.
[206] C. Shannon and W. Weaver, The Mathematical Theory of Communication, Univ. Illinois Press, Urbana III., 1949.
[207] K. Sharma, M. M. Wilde, S. Adhikari and M. Takeoka, Bounding the energy-constrained quantum and private capacities of phase-insensitive bosonic Gaussian channels, New J. Phys. 20 (2018) 063025; arXiv:1708.07257.
[208] M. E. Shirokov, Entropic characteristics of subsets of states, Izvestiya Math. 70 (2006), pp. 1265-92; 71 (2007), pp. 181-218.
[209] M. E.Shirokov, On entropic quantities related to the classical capacity of infinite dimensional quantum channels, Theory Probab. and Appl. 52 (2007), pp. 250-76.
[210] M. E. Shirokov, The Holevo capacity of infinite dimensional channels and the additivity problem, Commun. Math. Phys. 262 (2006), pp. 137-59; arXiv:quant-ph/0408009.
[211] M. E. Shirokov, Entropy reduction of quantum measurements, J. Math. Phys. 52 (2011), 052202; arXiv:1011.3127.
[212] M. E. Shirokov, A criterion for coincidence of the entanglement-assisted classical capacity and the Holevo capacity of a quantum channel, Probl. Inform. Transmission. 48 (2012), pp. 3-19; arXiv:1202.3449v2 [quant-ph] (2012).
[213] M. E. Shirokov and T. Shulman, On superactivation of one-shot zero-error quantum capacity and the related property of quantum measurements, Probl. Inform.Transmission. 50(3) (2014), pp. 232-46; arXiv:1312.3586.
[214] M. E.Shirokov, On channels with positive quantum zero-error capacity having vanishing n-shot capacity, Quantum Inf. Process. 14(8) (2015), pp. 3057-74.
[215] P. W. Shor, Additivity of the classical capacity of entanglement-breaking quantum channels, J. Math. Phys. 43 (2002), pp. 4334-40; e-print quant-ph/0201149.
[216] P. W. Shor, The quantum channel capacity and coherent information, Lecture Notes, MSRI Workshop on Quantum Computation, Berkeley, 2002.
[217] P. W. Shor, The adaptive classical capacity of a quantum channel, or information capacity of 3 symmetric pure states in three dimensions, arXiv:quant-ph/0206058v3 (2002).
[218] P. W. Shor, Equivalence of additivity questions in quantum information theory, Commun. Math. Phys. 246 (2004), pp. 453-72; arXiv:quant-ph/0305035.
[219] P. W. Shor, The classical capacity achievable by a quantum channel assisted by limited entanglement, in Quantum Information, Statistics, Probability, ed. by O. Hirota, Rinton Press, Inc., Princeton, New Jersey, 2004; quant-ph/0402129.
[220] R. Simon, M. Selvadoray and G. S. Agarwal, Gaussian states for finite number of Bosonic degrees of freedom, Preprint, 1998.
[221] G. Smith, The private classical capacity with a symmetric side channel and its applications to quantum cryptography, Phys. Rev. A 78 (2008) 022306; arXiv:0705.3838.
[222] G. Smith and J. A. Smolin, Detecting incapacity, Phys. Rev. Lett. 108 (2012) 230507; arXiv:1108.1807.
[223] G. Smith, J.A. Smolin and J. Yard, Gaussian bosonic synergy: quantum communication via realistic channels of zero quantum capacity, Nature Photonics 5 (2011), pp. 624-7; arXiv:1102.4580.
[224] G. Smith and J. Yard, Quantum communication with zero-capacity channels, Science 321 (2010), pp. 1812.
[225] A. Steane: Quantum computing, Rept. Prog. Phys. 61 (1997), pp. 117-73.

[226] W. F. Stinespring, Positive functions on C*-algebras, Proc. Amer. Math. Soc. 6 (1955), pp. 211-316.
[227] R. L. Stratonovich, The amount of information transmitted by a quantum channel. I, II, Izv. VUZ. Radiophysics 8 (1965), pp. 116-41 (in Russian).
[228] R. L. Stratonovich, The quantum generalization of optimal statistical estimation and testing hypothesis, J. Stoch. 1 (1973), pp. 87-126.
[229] R. L. Stratonovich and A. G. Vantsjan, On asymptotically errorless decoding in pure quantum channels, Probl. Control Inform. Theory, 7 (1978), pp. 161-74.
[230] E. C. G. Sudarshan, P. M. Mathews and J. Rau, Stochastic dynamics of quantum-mechanical systems, Phys. Rev. 121 (1961), pp. 920-4.
[231] M. Tomamichel and V. Y. F. Tan, Second-Order Asymptotics for the Classical Capacity of Image-Additive Quantum Channels, Commun. Math. Phys. 338(1) (2015), pp. 103-37; arXiv:1308.6503v3.
[232] J. A. Tropp, User-friendly tail bounds for sums of random matrices, Found. Comput. Math.. 12(4) (2012), pp. 389-434; arXiv:1004.4389v7.
[233] A. Uhlmann, The "transition probability" in the state space of a $*$-algebra, Rep. Math. Phys. 9 (1976), pp. 273-9.
[234] A. Uhlmann, Relative entropy and the Wigner-Yanase-Dyson-Lieb concavity in an interpolation theory, Commun. Math. Phys. 54 (1977), pp. 21-32.
[235] K.A. Valiev, Quantum computers and quantum computations, Physics-Uspekhi 48 (2005), pp. 1-36.
[236] S. Verdú, Fifty years of Shannon theory, IEEE Trans. Inform. Theory 44 (1998), pp. 2057-78.
[237] J. von Neumann, Mathematical Foundations of Quantum Mechanics, Princeton University Press, Princeton, NJ, 1955, (1932).
[238] F. Verstraete and H. Verschelde, On quantum channels, arXiv:quant-ph/0202124v2.
[239] L. Wang and R. Renner, One-Shot Classical-Quantum Capacity and Hypothesis Testing, Phys. Rev. Lett. 108 (2012), 200501; arXiv:1007.5456v3.
[240] J. Watrous, The theory of quantum information, Cambridge University Press, 2018; http: //cs.uwaterloo.ca/~watrous/TQI/TQI.pdf.
[241] C. Weedbrook, S. Pirandola, R. Garcia-Patron, N. J. Cerf, T. C. Ralph, J. H. Shapiro and S. Lloyd, Gaussian quantum information, Rev. Modern Physics 84 (2012), pp. 621; arXiv:1110.3234.
[242] A. Wehrl, General properties of entropy, Rev. Mod. Phys. 50 (1978), pp. 221-60.
[243] R.A. Werner and A. S. Holevo, Counterexample to an additivity conjecture for output purity of quantum channels, J. Math. Phys. 43 (2002), pp. 4353-7.
[244] Werner R. F. and Wolf M. M., Bound entangled Gaussian states, Phys. Rev. Lett. 86 (2001), pp. 3658; arXiv:quant-ph/0009118.
[245] H. Weyl, The Theory of Groups and Quantum Mechanics, Dover, New York, 1931, (1928).
[246] A. S. Wightman, Hilbert's sixth problem: mathematical treatment of the axioms of physics, in Proc. Symp. in pure math. 28 (1977), pt. 1, pp. 147-240.
[247] E. P. Wigner, Group Theory, Academic Press, New York, 1959.
[248] M. M. Wilde, Quantum Information Theory, 2nd edition, Cambridge University Press, Cambridge, 2017; arXiv:1106.1445.
[249] M. M. Wilde, N. Datta, Min-Hsiu Hsieh and A. Winter Quantum rate distortion coding with auxiliary resources, IEEE IT Trans. 59(10) (2013), pp. 6755-73; arXiv:1704.02903.
[250] M. M. Wilde and H. Qi, Energy-constrained private and quantum capacities of quantum channels, IEEE IT Trans. 64(12) (2018), pp. 7802-27; arXiv:1609.01997.
[251] M. M. Wilde, Andreas Winter and Dong Yang, Strong converse for the classical capacity

of entanglement-breaking and Hadamard channels via a sandwiched Renyi relative entropy, Commun. Math. Phys. 331 (2014), pp. 593-622; arXiv:1306.1586v4.
[252] J. Williamson, On the algebraic problem concerning the normal forms of linear dynamical systems, Am. J. Math 58 (1936), pp. 141; 59 (1937), pp. 599; 61 (1939), pp. 897.
[253] A. Winter, Coding theorem and strong converse for quantum channels, IEEE Trans. Inform. Theory, 45 (1999), pp. 2481-5.
[254] A. Winter, Compression of sources of probability distributions and density operators, arXiv:quant-ph/0208131 (2002).
[255] A. Winter, The maximum output p-norm of quantum channels is not multiplicative for any $p > 2$, arXiv:0707.0402.
[256] M. Wolf, G. Giedke and J. I. Cirac, Extremality of Gaussian quantum states, Phys. Rev. Lett. 96 (2006), 080502; arXiv:quant-ph/0509154.
[257] M. M. Wolf, G. Giedke, O. Krueger, R. F. Werner and J. I. Cirac, Gaussian entanglement of formation, Phys. Rev. A 69 (2004), 052320; arXiv:quant-ph/0306177.
[258] M. Wolf, D. Pérez-Garsía, G. Giedke, Quantum capacities of Bosonic channels, Phys. Rev. Lett. 98 (2007), 130501; quant-ph/0606132.
[259] S. L. Woronowicz, On the purification map, Commun. Math. Phys. 30 (1973), pp. 55-67.
[260] H. P. H Yuen and M. Lax, Multiple-parameter quantum estimation and measurement of non-selfadjoint observables, IEEE Trans. Inform. Theory 19 (1973), pp. 740-50.
[261] C. Zu, Y-X. Wang, X-Y. Chang, Z-H. Wei, S-Y. Zhang and L-M. Duan, Experimental demonstration of quantum gain in a zero-sum game, New J. Phys. 14 (2012), 033002.
[262] A. Zeilinger et al., Significant-loophole-free test of Bell's theorem with entangled photons, Phys. Rev. Lett. 115 (2015) 250401; arXiv:1511.03190v2.

11 Quantum supremacy using a programmable superconducting processor by Google AI Quantum

11.1 Device design and architecture

The Sycamore device was designed with both the quantum supremacy experiment [1] and small noisy intermediate scale quantum (NISQ) applications in mind. The architecture is also suitable for initial experiments with quantum error correction based on the surface code. While we are targeting 0.1% error two-qubit gates for error correction, a quantum supremacy demonstration can be achieved with 0.3-0.6% error rates.

For decoherence-dominated errors, a 0.1% error means a factor of about 1000 between coherence and gate times. For example, a 25 μs coherence time implies a 25 ns gate. A key design objective in our architecture is achieving short two-qubit gate time, leading to the choice of tunable transmon qubits with direct, tunable coupling.

A difficult challenge for achieving a high-performance two-qubit gate is designing a sufficiently strong coupling when the gate is active, which is needed for fast gates, while minimizing the coupling otherwise for low residual control errors. These two competing requirements are difficult to satisfy with a fixed-coupling architecture: our prior processors [2] used large qubit-qubit detuning ($\sim$1 GHz) to turn off the effective interaction, requiring relatively high-amplitude precise flux pulses to tune the qubit frequencies to implement a CZ gate. In the Sycamore device, we use adjustable couplers [3] as a natural solution to this control problem, albeit at the cost of more wiring and control signals. This means that the qubits can idle at much smaller relative detuning. We chose a capacitor-coupled design [3, 4], which is simpler to layout and scale, over the inductor-based coupler of previous gmon devices [5, 6]. In Sycamore,

the coupling g is tunable from 5 MHz to -40 MHz. The experiment uses 'on' coupling of about -20 MHz.

By needing only small frequency excursions to perform a two-qubit gate, the tunable qubit can be operated much closer to its maximum frequency, thus greatly reducing flux sensitivity and dephasing from $1/f$ flux noise. Additionally, the coupling can be turned off during measurement, reducing the effect of measurement crosstalk, a phenomenon that has shown to be somewhat difficult to understand and minimize [7].

The interaction Hamiltonian of a system of on-resonance transmons with adjustable coupling (truncated to the qubit levels) has the following approximate form,

$$H_{\text{int}}(t) \approx \sum_{\langle i,j \rangle} g_{ij}(t) \left(\sigma_i^+ \sigma_j^- + \sigma_i^- \sigma_j^+\right) + \frac{g_{ij}^2(t)}{|\eta|} \sigma_i^z \sigma_j^z \,, \tag{11.1}$$

where g_{ij} is the nearest neighbor coupling, η is the non-linearity of the qubits (roughly constant), i and j index nearest-neighbor qubit pairs, and $\sigma^\pm = (\sigma^x \pm i\sigma^y)/2$. We pulse the coupling in time to create coupling gates.

Our two-qubit gate can be understood using Cartan decomposition [8], which enables an arbitrary two-qubit gate to be decomposed into four single-qubit gates around a central two-qubit gate that can be described by a unitary matrix describing only XX, YY and ZZ interactions, with 3 parameters indicating their strengths. For the physical interaction describing our hardware, we see a swapping interaction between the $|01\rangle$ and $|10\rangle$ qubits states, corresponding to an XX+YY interaction. Interaction of the qubit $|11\rangle$ state with the $|2\rangle$ states of the data transmons produce a phase shift of that state, corresponding to a ZZ interaction. By changing the qubit frequencies and coupling strength we can vary the magnitude of these interactions, giving net control of 2 out of the 3 possible parameters for an arbitrary gate.

11.2 Fabrication and layout

Our Sycamore quantum processor is configured as a diagonal array of qubits as seen in the schematic of Fig. 1 in the main text. The processor contains 142 transmon qubits, of which 54 qubits have individual microwave and frequency controls and are individually read out (referred to as qubits). The remaining 88 transmons are operated as adjustable couplers remaining in their ground state during the algorithms (referred to as couplers).

The qubits consist of a DC SQUID sandwiched between two metal islands, operating in the transmon regime. An on-chip bias line is inductively coupled to the DC SQUID, which allows us to tune qubit frequency by applying control fluxes into the SQUID loop. For regular operations, we tune qubits through a small frequency range (< 100 MHz). This corresponds to a relatively small control signal and makes qubit operation less sensitive to flux crosstalk.

Each pair of nearest-neighbor qubits are coupled through two parallel channels: direct capacitive coupling and indirect coupling mediated by coupler [3, 9, 4]. Both channels result in qubit-qubit coupling in the form of $\sigma_i^x \sigma_j^x + \sigma_i^y \sigma_j^y$ in the rotating frame, although with different signs. The indirect coupling is negative, given it is a second-order virtual process. The strength of the indirect coupling is adjusted by changing the coupler frequency with an additional on-chip bias line, giving a net zero qubit-qubit coupling at a specific flux bias.

The Sycamore processor consists of two die that we fabricated on separate high resistivity silicon wafers. The fabrication process, using aluminum on silicon, requires a total of 14 lithography layers utilizing both optical and electron beam lithography. Crosstalk and dissipation are mitigated through ground plane shielding [10]. After fabrication and die singulation, we use indium bump bonding [11, 12] of the two separate dies to form the Sycamore processor.

The Sycamore processor is connected to a 3-layer Al-plated circuit board with Al wirebonds [13]. Each line is routed through a microwave connector to an individual coax cable. We shield

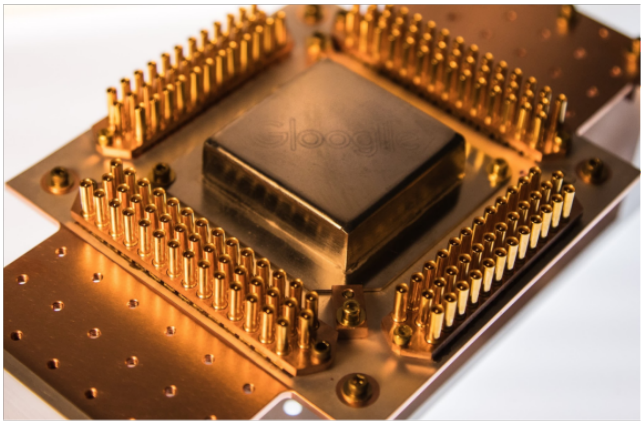


Figure S1: **A photograph of a packaged Sycamore processor.** The processor is shielded from the electromagnetic environment by a mu-metal shield (middle) and a superconducting aluminum cap, inside the mu-metal shield. The processor control wires are routed, through PCB circuit board, to coaxial connectors shown around the edge.

the processor from stray light using a superconducting Al lid with black coating, and from magnetic fields using a mu-metal shield as shown in Fig. S1.

11.3 Qubit control and readout

11.3.1 Control

Operating the device requires simultaneous synchronized control waveforms for each of the qubits and couplers. We use 54 coherent microwave control signals for qubit XY rotations, 54 fast flux bias lines for qubit frequency tuning, and 88 fast flux biases for the adjustable couplers. Dispersive readout requires an additional 9 microwave signals and phase sensitive receivers. A schematic of the room temperature electronics is shown in Fig. S2, and the cryogenic wiring is shown in Fig. S3.

Waveform generation is based on a custom-built multi-channel digital to analog converter (DAC) module. Each DAC module provides 8 DACs with 14-bit resolution and 1 GS/s sample rate. Each DAC sample clock is synchronized to a global 10 MHz reference oscillator, and their trigger is connected by a daisy chain to synchronize all modules used in the experiment. This set of DAC modules forms a >250-channel, phase-synchronous waveform generator. We have measured 20 ps of jitter between channels. The modules are mounted in 14-slot 6U rackmount chassis. A single chassis, shown in FIG. S4, can control approximately 15 qubits including their associated couplers and readout signals. A total of 4 chassis are used to control the entire Sycamore chip.

The DAC outputs are used directly for fast flux biasing the qubits and couplers required for two-qubit gates. Microwave control for single-qubit XY rotations and dispersive readout combine two DAC channels and a mixer module to form a microwave arbitrary waveform generator (Microwave AWG) via single-sideband upconversion in an IQ mixer as shown in Figure S2 a. The microwave AWG provides signals with arbitrary spectral content within ±350 MHz of the local oscillator (LO). A single LO signal is distributed to all IQ mixers so that all qubits' XY controls are phase coherent. The mixer modules are mounted in the same chassis as the DAC modules. Each mixer's I and Q port DC offsets are calibrated for minimum carrier leakage and the I and Q amplitudes and phases are calibrated to maximize image rejection.

Each DAC module contains an FPGA that provides a gigabit ethernet interface, SRAM to store waveform patterns, and sends the waveform data to the DAC module's 8 DACs. To

optimize the use of SRAM, the FPGA implements a simple jump table to allow reusing or repeating waveform segments. A computer loads the desired waveforms and jump table onto each FPGA using a UDP-based protocol and then requests the first (master) FPGA to start. The start pulse is passed down the daisy chain causing the remainder (slave) DACs and ADCs to start.

11.3.2 Readout

Qubit state measurement and readout (hereafter "readout") are done via the dispersive interaction between the qubit and a far-detuned harmonic resonator [14, 15, 16]. A change in the qubit state from $|0\rangle$ to $|1\rangle$ causes a frequency shift of the resonator from $\omega_{|0\rangle}$ to $\omega_{|1\rangle}$. A readout probe signal applied to the resonator at a frequency in between $\omega_{|0\rangle}$ and $\omega_{|1\rangle}$ reflects with a phase shift $\phi_{|0\rangle}$ or $\phi_{|1\rangle}$ that depends on the resonator frequency and therefore on the qubit state. By detecting the phase of the reflected probe signal we infer the qubit state. The readout probe signal is generated with the same microwave AWG as the XY control signals, but with a separate local oscillator, and is received and demodulated by the circuit shown in Figure S2 c.

The readout probe intensity is typically set to populate the readout resonator with only a few photons to avoid readout-induced transitions in the qubit [17]. Detecting this weak signal at room temperature with conventional electronics requires 100 dB of amplification. To limit the integration time to a small fraction of the qubit coherence time, the amplification chain must operate near the quantum noise limit [18, 19].

Inside the cryostat the signal is amplified by an impedance matched lumped element Josephson parametric amplifier (IMPA) [20] on the mixing chamber stage followed by a Low Noise Factory cryogenic HEMT amplifier at 3 K. At room temperature the signal is further amplified before it is mixed down with an IQ mixer producing a pair of intermediate frequency (IF) signals $I(t)$ and $Q(t)$. The IF signals are amplified by a pair of variable gain amplifiers to fine-tune their level, and then digitized by a pair of custom 1 GS/s, 8-bit analog to digital converters (ADC). The digitized samples I_n and Q_n are processed in an FPGA which combines them into a complex phasor

$$z_n = I_n + iQ_n = E_n \exp(i(\omega n dt + \phi))$$

where dt is the sample spacing, ω is the IF frequency, ϕ is the phase that depends on the qubit state, and E_n is the envelope of the reflected readout signal. The envelope is measured experimentally once and then used by the FPGA in subsequent experiments as the optimal demodulation window w_n to extract the phase of the reflected readout signal [21, 22]. The FPGA multiplies z_n by $w_n \exp(-i\omega n dt)$, and then sums over time to produce a final complex value $\exp(i\phi)$

$$\sum_{n=0}^{N-1} z_n w_n \exp(-i\omega n dt) \propto \exp(i\phi)$$

In the absence of noise, the final complex value would always be one of two possible values corresponding to the qubit states $|0\rangle$ and $|1\rangle$. However, the noise leads to Gaussian distributions centered at those two points. The size of the clouds is determined mostly by the noise of the IMPA and cryogenic HEMT amplifier, while the separation between the clouds' centers is determined by the resonator probe power and duration. The signal to noise ratio of the measurement is determined by the clouds' separation and width [22, 23].

The 54 qubits are divided into nine frequency multiplexed readout groups of six qubits each. Within a group, each qubit is coupled to its own readout resonator, but all six resonators are coupled to a shared bandpass Purcell filter [24, 25, 22]. All qubits in a group can be readout simultaneously by frequency-domain multiplexing [26, 2] in which the total probe signal

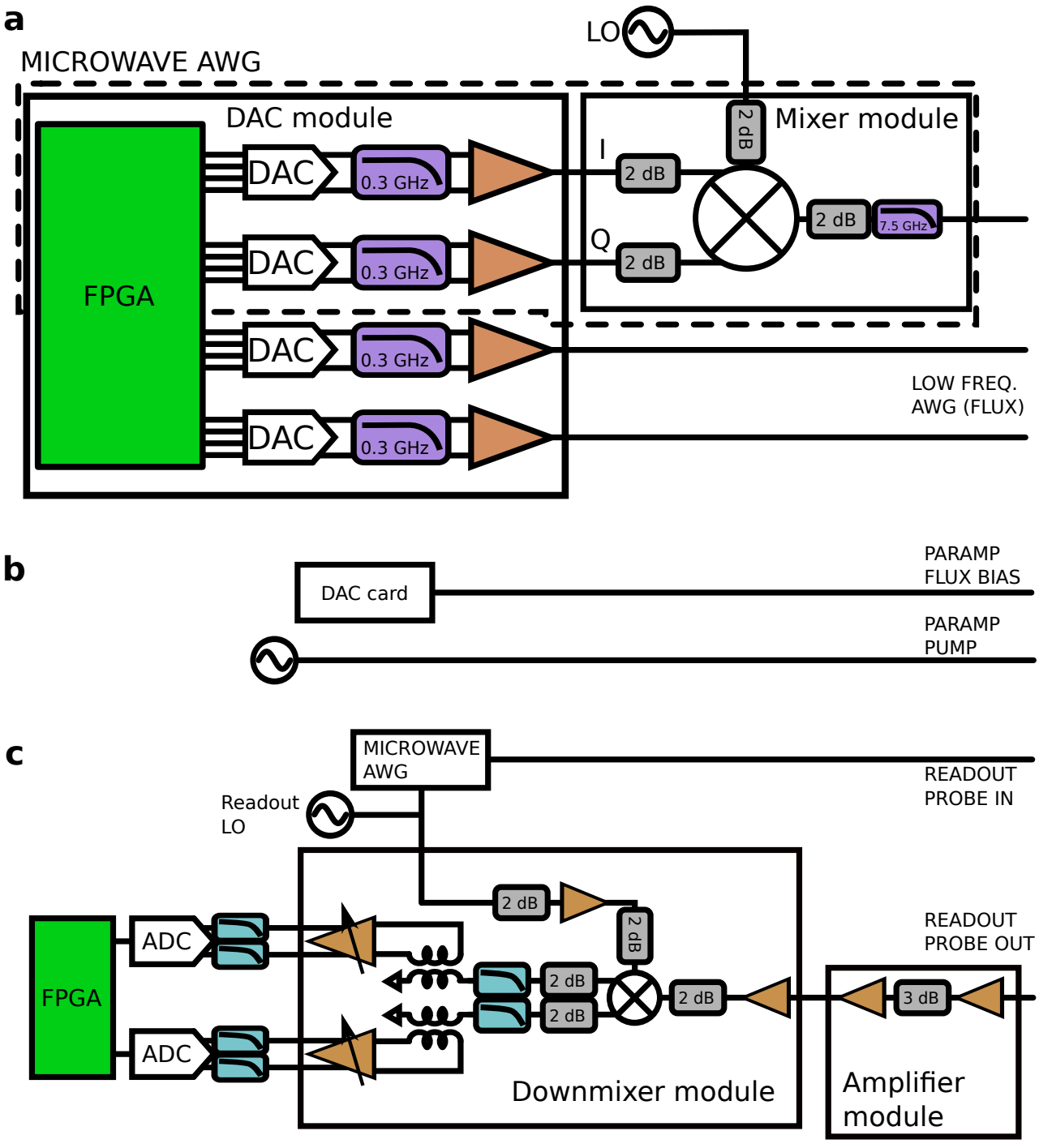


Figure S2: **Control electronics. a,** The custom DAC module provides 8 DAC channels (4 shown). DACs are used individually for flux pulses or in pairs combined with a mixer module to comprise a microwave AWG channel (dashed box). **b,** A single DAC channel and a microwave source are used to bias and pump the parametric amplifier for readout. **c,** Readout pulses are generated by a microwave AWG. The reflected signal is amplified, mixed down to IF, and then digitized in a pair of ADCs. The digital samples are analyzed in the FPGA.

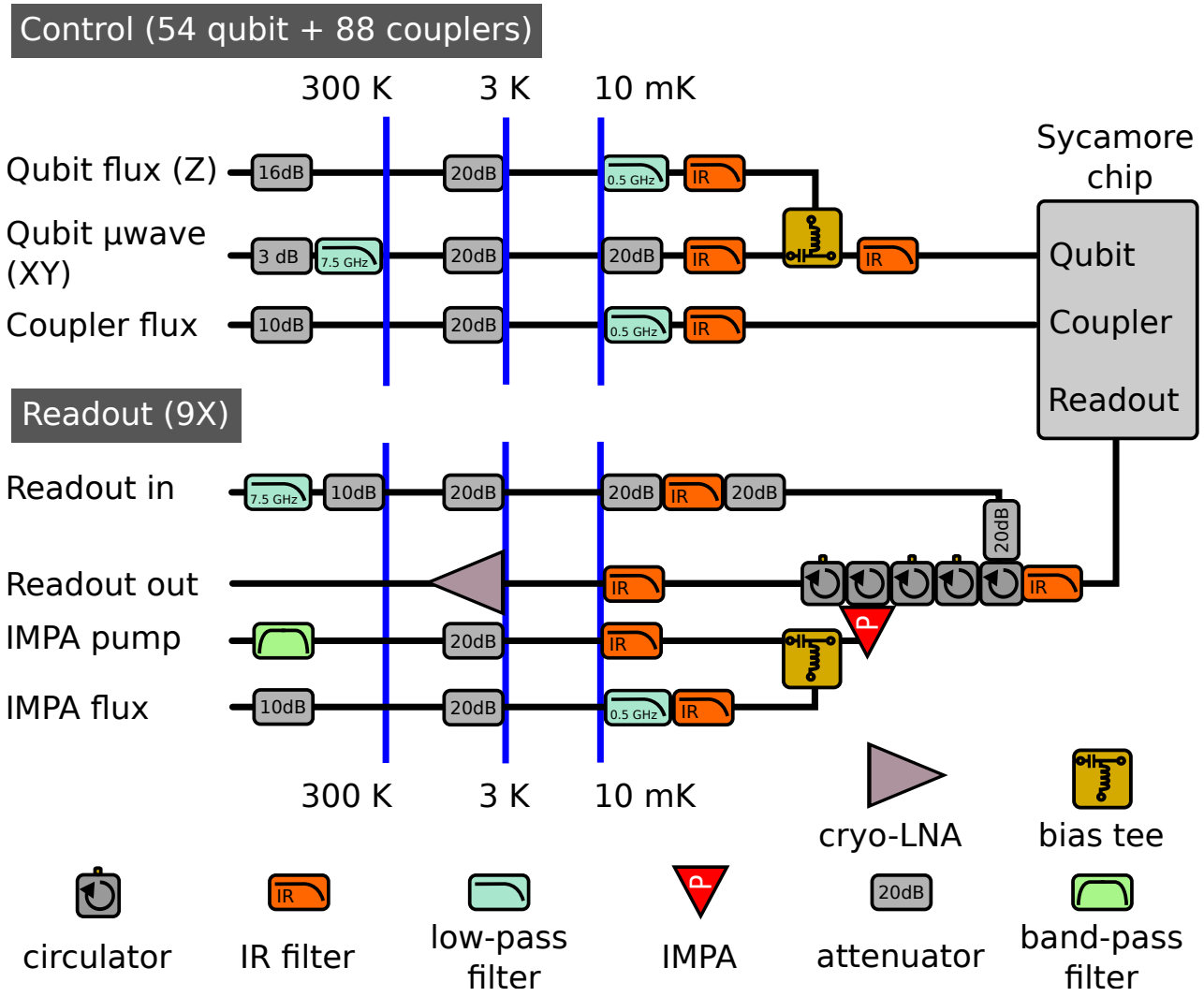


Figure S3: **Cryogenic wiring.** Control and readout signals are carried to and from the Sycamore chip with a set of cables, filters, attenuators, and amplifiers.

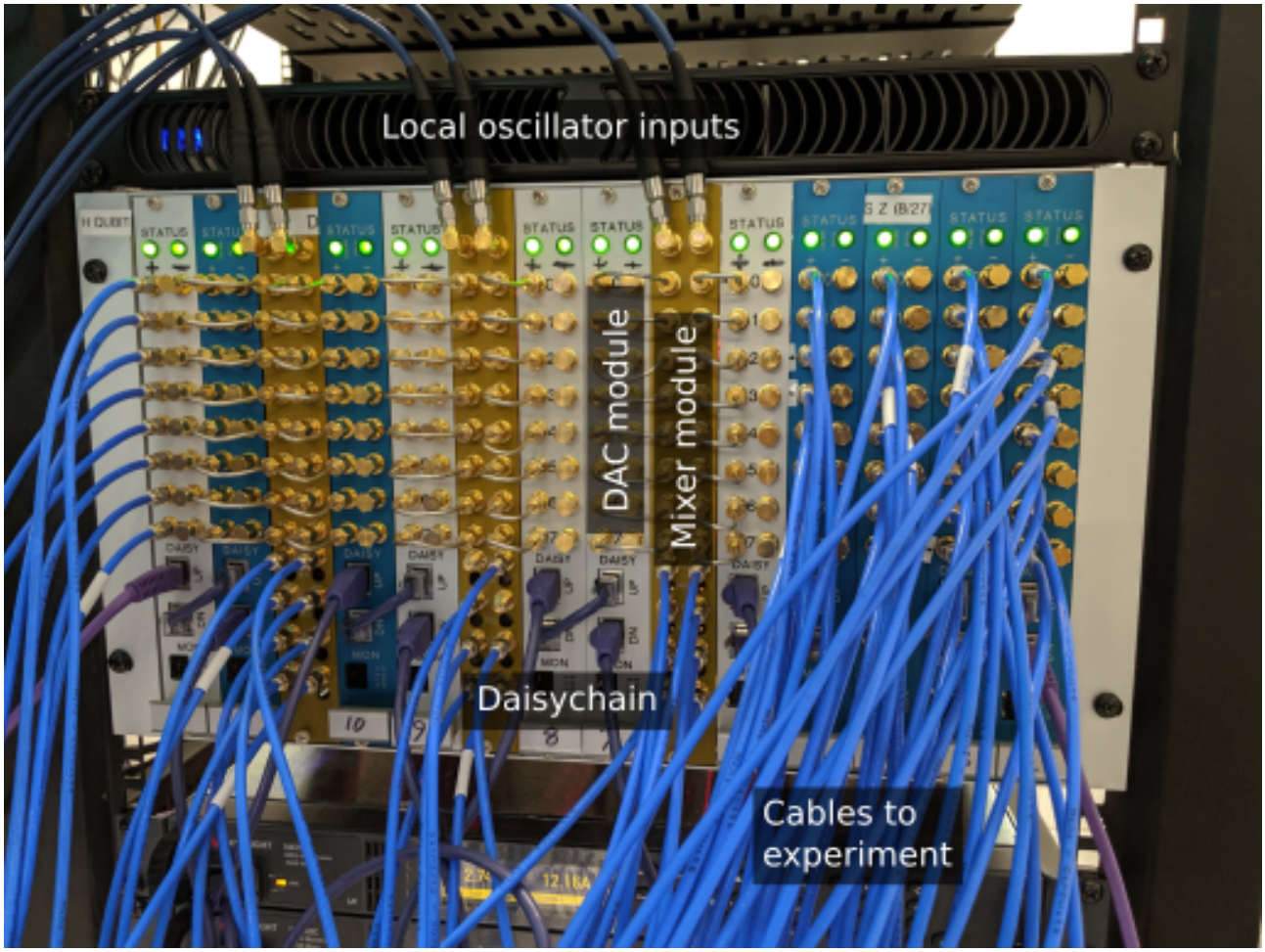


Figure S4: **Electronics chassis.** Each chassis supports 14 DAC and/or mixer modules. Local oscillators are connected at the top of each mixer module. A set of daisychain cables connects from each ADC module to the next. Control signals exit the chassis through coaxial cables.

is a superposition of probe signals at each of the readout resonators' frequencies. The phase shifts of these superposed signals are independently recovered in the FPGA by demodulating the complex IQ phasor with each intermediate frequency. In other words, we know what frequencies are in the superposed readout signal and we compute the Fourier coefficients at those frequencies to find the phase of each reflected frequency component.

11.4 XEB theory

We use cross entropy benchmarking (XEB) [27, 6] to calibrate general single- and two-qubit gates, and also to estimate the fidelity of random quantum circuits with a large number of qubits. XEB is based on the observation that the measurement probabilities of a random quantum state have a similar pattern to laser "speckles", with some bitstrings more probable than others [28, 29]. The same holds for the output state of random quantum circuits. As errors destroy the speckle pattern, this is enough to estimate the rate of errors and fidelity in an experiment. Crucially, XEB does not require the reconstruction of experimental output probabilities, which would need an exponential number of measurements for increasing number of qubits. Rather, we use numerical simulations to calculate the likelihood of a set of bitstrings obtained in an experiment according to the ideal expected probabilities. Below we describe the theory behind this technique in more detail.

11.4.1 XEB of a small number of qubits

We first consider the use of XEB to obtain the error rate for single- and two-qubit gates. As explained above, for a two-qubit XEB estimation we use sequences of cycles, each cycle consisting of two sufficiently random single-qubit gates followed by the same two-qubit gate.

The density operator of the system after application of a random circuit U with m cycles can be written as a sum of two parts

$$\rho_U = \varepsilon_m \left|\psi_U\right\rangle \left\langle\psi_U\right| + (1-\varepsilon_m)\chi_U \ , \quad D = 2^n \ . \tag{11.2}$$

Here $\left|\psi_U\right\rangle = U\left|\psi_0\right\rangle$ is the ideal output state and χ_U is an operator with unit trace that along with ε_m describes the effect of errors. For a depolarizing channel model $\chi_U = I/D$ and ε_m has the meaning of the depolarization fidelity after m cycles. Nevertheless, in the case of small number of qubits, the part of the operator χ_U has nonzero matrix elements between the states with no error and the states with the error. However, if we undo the evolution of each random circuit and average over an ensemble of circuits such cross-terms are averaged out and we expect

$$\overline{U^\dagger \chi_U U} = \frac{I}{D} \ . \tag{11.3}$$

Here and below we use the horizontal bar on the top to denote averaging over the ensemble of random circuits. Because of this property it is possible to establish the connection between the quantity ε_m and the depolarization fidelity after m cycles.

From Eqs. (11.2) and (11.3) we get

$$\overline{U^\dagger \rho_U U} = \overline{\varepsilon_m} \left|\psi_0\right\rangle \left\langle\psi_0\right| + (1-\overline{\varepsilon_m})\frac{I}{D} \ . \tag{11.4}$$

This is a depolarizing channel. From this and the exponential decay of fidelity we get

$$\overline{\varepsilon_m} = p_c^m \ , \tag{11.5}$$

connecting $\overline{\varepsilon_m}$ to the depolarization fidelity p_c per cycle.

The noise model (11.2) is very general in the context of random circuits. To provide some insight about the origin of this model we consider a specific case with pure systematic error in the two-qubit gate. In this case the resulting pure state after the application of the random circuit $\tilde{U}$ with the error can be expanded into the direction of the ideal state vector and the orthogonal direction

$$\tilde{U}\,|\psi_0\rangle = \xi_m\;|\psi_U\rangle + \sqrt{1-|\xi_m|^2}\,|\varphi_{\tilde{U}}\rangle\;\;, \tag{11.6}$$

where

$$\langle\psi_U|\varphi_{\tilde{U}}\rangle = 0, \quad \langle\varphi_{\tilde{U}}|\varphi_{\tilde{U}}\rangle = 1\;. \tag{11.7}$$

For the ensemble of random circuits U the error vector is distributed completely randomly in the plane orthogonal to the ideal vector $U\,|\psi_0\rangle$ (see Fig. S5). This condition of orthogonality is the only constraint on the vector $|\varphi_{\tilde{U}}\rangle$ that involves $|\psi_U\rangle$. Therefore we expect

$$\overline{U^\dagger\,|\varphi_{\tilde{U}}\rangle\,\langle\varphi_{\tilde{U}}|\,U} = \frac{1}{D-1}(I - |\psi_0\rangle\,\langle\psi_0|)\;. \tag{11.8}$$

Also

$$\overline{U^\dagger\left(\xi_m\sqrt{1-|\xi_m|^2}\;|\psi_U\rangle\,\langle\varphi_{\tilde{U}}| + h.c\right)U} = 0\;. \tag{11.9}$$

This gives the connection between the error vector $|\varphi_{\tilde{U}}\rangle$ and the operator χ_U

$$(1-\varepsilon_m)\chi_U - \frac{1-\varepsilon_m}{D}\,|\psi_U\rangle\,\langle\psi_U| = (1-|\xi_m|^2)\,|\varphi_{\tilde{U}}\rangle\,\langle\varphi_{\tilde{U}}| + \left(\xi_m\sqrt{1-|\xi_m|^2}\;|\psi_U\rangle\,\langle\varphi_{\tilde{U}}| + h.c\right)\;. \tag{11.10}$$

The resulting equation

$$\overline{|\xi_m|^2} = \overline{\varepsilon_m} + \frac{1-\overline{\varepsilon_m}}{D} \tag{11.11}$$

is to be expected, because $|\xi_m|^2$ is the average state fidelity while $\overline{\varepsilon_m}$ is the depolarization fidelity (see Sec. 11.5). Note that Eqs. (11.8)–(11.11) lead to Eq. (11.4). This result can also be derived assuming that single qubit gates form a 2-design in the Hilbert space of each qubit.

We demonstrate the above findings by numerically simulating the random circuits for 2 qubits that contains single qubit gates randomly sampled from Haar measure and ISWAP-like gate

$$V(\theta) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos\theta & -i\sin\theta & 0 \\ 0 & -i\sin\theta & \cos\theta & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}\;. \tag{11.12}$$

The systematic error $\Delta\theta = \theta - \pi/2$ corresponds to the deviation of the swap angle from $\pi/2$. Then assuming that the single qubit gates are error free the depolarizing channel model gives the prediction for the depolarizing fidelity per cycle

$$\begin{aligned} p_c &= \frac{|\mathrm{tr}(V(\theta)V^\dagger(\pi/2))|^2 - 1}{D^2-1} \\ &= \frac{1}{15}(8\cos(\Delta\theta) + 2\cos(2\Delta\theta) + 5)\;. \end{aligned} \tag{11.13}$$

As shown in Fig. S6 the depolarizing fidelity p_c^m for the circuit of depth m based on Eq. (11.13) closely matches the corresponding quantity obtained by the averaging of the squared overlap over the ensemble of random circuits (cf. (11.11)

$$\overline{\varepsilon_m} = \frac{D\,\overline{|\xi_m|^2} - 1}{D-1}\;. \tag{11.14}$$

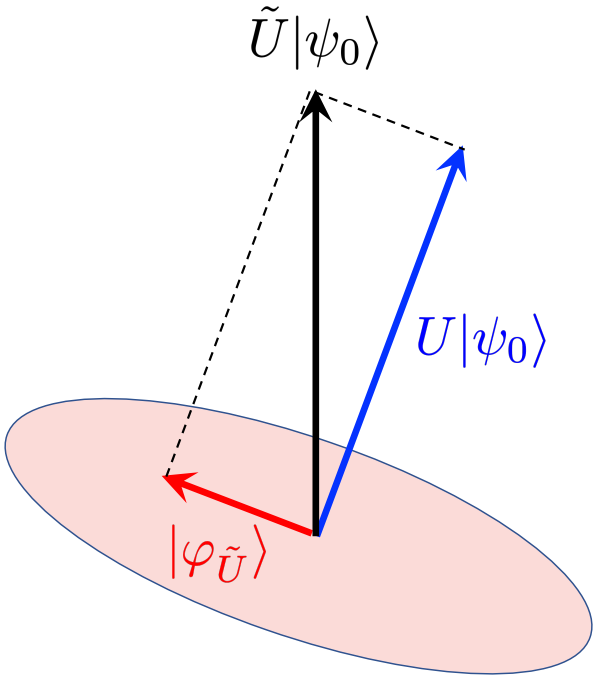


Figure S5: **Cartoon: decomposition of the quantum state into the vector aligned with the ideal quantum state and its orthogonal complement**

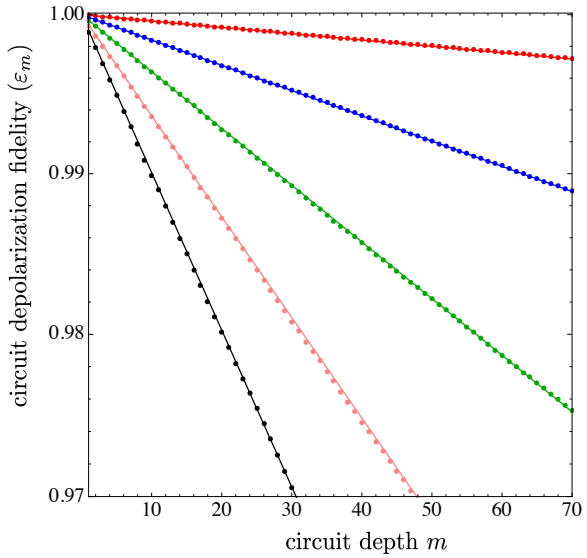


Figure S6: **Plots of the circuit depolarizing fidelity** *vs* **the circuit depth.** Solid lines corresponds to the predictions from the depolarizing channel model (11.13) and points correspond to $\overline{\varepsilon_m}$ (11.14) obtained by the averaging of the squared overlap over the ensemble of random circuits. Different colored pots correspond to different values of the swap error $\Delta\theta =$ 0.01(red), 0.02(blue), 0.03 (green), 0.04 (pink), 0.05 (black).

Returning to the generic case, property (11.3) can be extended so that for any smooth function $f(u)$ the following relation holds

$$\overline{\sum_{q\in\{0,1\}^n} f(p_s(q))\,\langle q|\,\chi_U\,|q\rangle} = \sum_{q\in\{0,1\}^n} \frac{\overline{f(p_s(q))}}{D} + \epsilon\ , \tag{11.15}$$

where $|q\rangle$ is a computational basis state corresponding to bitstring q, and $p_s(q) = \langle q|\,U\rho_0 U^\dagger\,|q\rangle$ is the simulated (computed) ideal probability of q. If the average is performed over a sample of random circuits of size S then the correction is $\epsilon \in O(1/\sqrt{S})$. We tested numerically for the case of $n = 2$ that relation (17.6) holds even for purely systematic errors in the case of a sufficiently random set of single qubit gates.

We now make the critical step of estimating the parameter p_c^m from a set of experimental realizations of random circuits with m cycles. We map each measured bitstring q with a function $f(p_s(q))$ and then average this function over the measured bitstrings. The standard XEB [27, 6] uses the natural logarithm, $f(p_s(q)) = \log(p_s(q))$. In the main text we use the linear version of XEB, for which $f(p_s(q)) = Dp_s(q)-1$. Both these functions give higher values to bitstrings with higher simulated probabilities. Another closely related choice is the Heavy Output Generation test [30], for which f is a step-function.

Under the model (11.2), in an experiment with ideal state preparation and measurement, we obtain the bitstring q with probability

$$p_c^m\ p_s(q) + (1 - p_c^m)\,\langle q|\,\chi_U\,|q\rangle\ , \tag{11.16}$$

For the linear XEB, the average value of $Dp_s(q) - 1$ when sampling with probabilities given by Eq. (11.16) is

$$\overline{\langle Dp_s(q) - 1\rangle} = p_c^m \left(D \sum_q \overline{p_s(q)^2} - 1 \right)\ . \tag{11.17}$$

Similarly to Eq. (17.6), the horizontal bar denotes averaging over the random circuits.

The sum on the right hand side of (11.17) goes over all bitstrings in the computational basis, and can be obtained with numerical simulations. It can also be found analytically assuming that the random circuit ensemble approximates the Haar measure where for a given q the quantity $p_s(q)$ is distributed with the beta distribution function $(D-1)(1-p_s)^{D-2}$. In this case the right hand side in (11.17) equals $p_c^m(2D/(D+1) - 1)$.

The experimental average on the left hand side of (11.17) can be estimated with accuracy $1/\sqrt{SN_s}$ using S random circuit realizations with N_s samples each

$$\frac{1}{SN_s} \sum_{j=1}^{S} \sum_{i=1}^{N_s} \left(Dp_s^j(q_{i,j}) - 1\right) = \overline{\langle Dp_s(q) - 1\rangle} + O\left(\frac{1}{\sqrt{SN_s}}\right)\ . \tag{11.18}$$

This gives an estimate of p_c^m.

This estimate can be justified using Bayes rule. The log-likelihood for a set of experimental measurements $\{q_{i,j}\}$ assuming that the experimental probabilities are given by Eq. (11.16) is proportional to

$$\sum_{j=1}^{S} \sum_{i=1}^{N_s} \log\left(1 + p_c^m(Dp_s^j(q_{i,j}) - 1)\right)\ , \tag{11.19}$$

where $p_s^j(q)$ is a simulated probability corresponding to the j-th circuit realization. We want to maximize the log-likelihood as a function of p_c^m. Taking the derivative with respect to p_c^m and equating to 0 we obtain

$$\sum_{j=1}^{S}\sum_{i=1}^{N_s}\frac{Dp_s^j(q_{i,j})-1}{1+p_c^m(Dp_s^j(q_{i,j})-1)}=0\ , \tag{11.20}$$

For $p_c^m \ll 1$ it is easy to solve this equation and obtain the estimate

$$p_c^m \simeq \frac{\sum_{j=1}^{S}\sum_{i=1}^{N_s}\left(Dp_s^j(q_{i,j})-1\right)}{\sum_{j=1}^{S}\sum_{i=1}^{N_s}\left(Dp_s^j(q_{i,j})-1\right)^2} \simeq \frac{\overline{\langle Dp_s(q)-1\rangle}}{D\sum_q \overline{p_s(q)^2}-1}\ . \tag{11.21}$$

In the spirit of the XEB method, we can use other functions $f(p_s(q))$ to estimate p_c^m. One alternative is derived from the log-likelihood of a sample $\{q_{i,j}\}$ with respect to the simulated (computed) ideal probabilities

$$\log \Pi_{j=1}^{S}\Pi_{i=1}^{N_s}p_s^j(q_{i,j})=\sum_{j=1}^{S}\sum_{i=1}^{N_s}\log p_s^j(q_{i,j})\ , \tag{11.22}$$

which converges to the cross entropy between experimental probabilities and simulated probabilities. The experimental average of the function $f(p_s(q))=\log p_s(q)$ under the probabilities from Eq. (11.16) with additional averaging over random circuits is

$$\begin{aligned}\overline{\langle \log p_s(q)\rangle} \simeq p_c^m&\left(\sum_q \overline{(p_s(q)-1/D)\log p_s(q)}\right)\\ &+\frac{1}{D}\sum_q \overline{\log p_s(q)}\ .\end{aligned} \tag{11.23}$$

As before, the sums on the right hand side can be obtained with numerical simulations and the average value on the left hand side can be estimated experimentally. This also gives an estimate of p_c^m.

Both Eq. (11.17) and Eq. (11.23) give a linear equation, from which we can obtain an estimate of the total polarization p_c^m for an experimental implementation of one quantum circuit with m cycles. We normally use mutiple circuits with the same number of cycles m to estimate p_c^m, which we can do using the least squares method. Finally, we obtain an estimate of p_c from a fit of the estimates p_c^m as an exponential decay in m. This is standard in randomized benchmarking [31, 32]. One advantage of this method is that it allows us to estimate the cycle polarization p_c independently of the state preparation and measurement errors (SPAM). See also below.

11.4.2 XEB of a large number of qubits

We now consider the case of a large number of qubits $n \gg 1$. We are typically interested in estimating the fidelity F of each of a set of circuits with a given number of qubits and depth. As above, we write the output of an approximate implementation of the random quantum circuit U as

$$\rho_U = F\left|\psi_U\right\rangle\left\langle\psi_U\right| + (1-F)\chi_U\ , \tag{11.24}$$

where $|\psi_U\rangle$ is the ideal output and $F=\langle\psi_U|\,\rho_U\,|\psi_U\rangle$ is the fidelity. We do not necessarily assume $\chi_U = I/D$, and we will ignore the small difference, of order 2^{-n}, $n \gg 1$, between the fidelity F and the depolarization fidelity p.

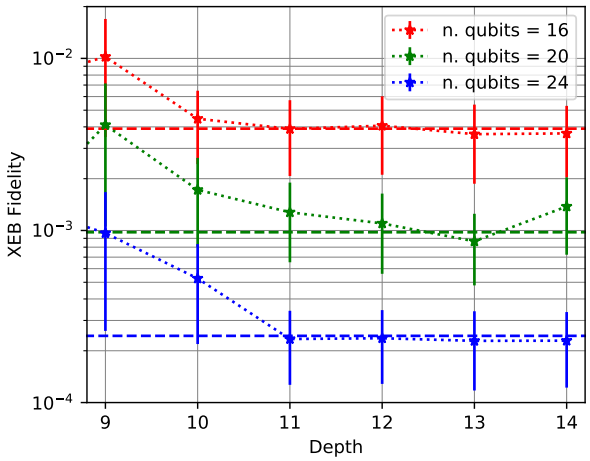


Figure S7: Absolute value of the XEB fidelity between a random quantum circuit and the same circuit with a single Pauli error. Markers show the median over all possible positions in the circuit for both bit-flip and phase-flip errors. Error bars correspond to the first and third quartile. The dashed lines are the $1/\sqrt{D}$ theory prediction.

As for the case of small number of qubits n, we map each output bitstring q with a function $f(p_s(q))$. Given that the values $\langle q|\,\chi_U\,|q\rangle$ resulting from errors are typically uncorrelated with the chaotic "speckles" of $p_s(q)$, we make our main assumption

$$\sum_q \langle q|\,\chi_U\,|q\rangle\, f(p_s(q)) = \frac{1}{D}\sum_q f(p_s(q)) + \epsilon\ . \tag{11.25}$$

This equation is trivial if we assume a depolarizing model, $\chi_U = I/D$. More generally, it can be understood in the geometric context of concentration of measure [33, 34, 35, 36] for high dimensional spaces, and from Levy's lemma [37] we expect a typical statistical fluctuation $\epsilon \in O(1/\sqrt{D})$ with $D = 2^n$. We will only require $\epsilon \ll F$. We check Eq. (11.25) numerically for the output $\rho_e = |\psi_e\rangle\langle\psi_e|$ where $|\psi_e\rangle$ is the wave function obtained after a single phase-flip or bit-flip error is added somewhere in the circuit, see Fig. S7 and Ref. [27]. We have also tested this assumption numerically comparing the fidelity with the XEB estimate for a pure state $\sqrt{F}\,|\psi_U\rangle + \sqrt{1-F}\,|\psi_\perp\rangle$, see also Ref. [38] and Section 11.10.

From Eqs. (11.24) and (11.25) we obtain Eq. (11.17) for linear XEB, $f(p_s(q)) = Dp_s(q) - 1$ ($\mathcal{F}_{\rm XEB}$ in the main text). We also obtain Eq. (11.23) for XEB, $f(p_s(q)) = \log p_s(q)$, with p_c^m replaced by fidelity F. As before, the sums on the right hand side can be obtained with numerical simulations and the average value on the left hand side can be estimated experimentally with accuracy $1/\sqrt{N_s}$ using N_s samples. This gives an estimate of F.

In practice, circuits of enough depth (as in the experiments reported here) exhibit the Porter-Thomas distribution for the measurement probabilities $p = \{p_s(q)\}$, that is

$$\Pr(p) = De^{-Dp}\ . \tag{11.26}$$

In this case the linear cross entropy Eq. (11.17) gives

$$F = \langle Dp_s(q) - 1\rangle\ . \tag{11.27}$$

The standard deviation of the estimate of F with N_s samples from the central limit theorem is $\sqrt{(1+2F-F^2)/N_s}$. The cross entropy Eq. (11.23) gives

$$F = \langle \log Dp_s(q)\rangle + \gamma\ , \tag{11.28}$$

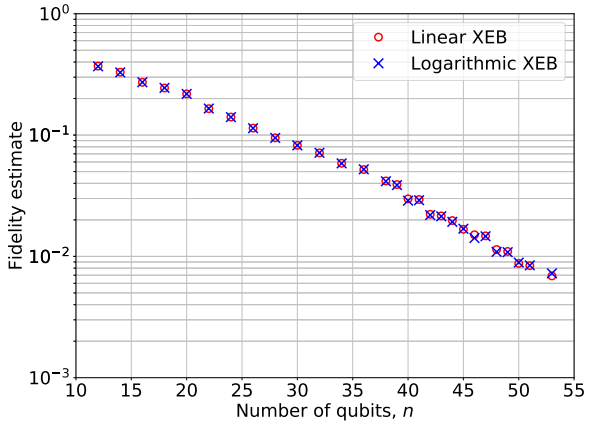


Figure S8: Comparison of fidelity estimates obtained using linear XEB, Eq. (11.27) and logarithmic XEB, Eq. (11.28) from bitstrings observed in our experiment using elided circuits (see Section 11.7.7). Standard deviation smaller than markers.

where γ is the Euler-Mascheroni constant ≈ 0.577. The standard deviation of the estimate of F with N_s samples is $\sqrt{(\pi^2/6 - F^2)/N_s}$. The logarithmic XEB has a smaller standard deviation for $F > 0.32$ (it is the best estimate when $F \approx 1$), while for $F < 0.32$ the linear XEB has a smaller standard deviation (it is the best estimate for $F \ll 1$, where it relates to the maximum likelihood estimator). See Fig. S8 for comparison of the fidelity estimates produced by the linear and logarithmic XEB.

We note in passing another example for an estimator of F related to the HOG test [30] which counts the number of measured bitstrings with probabilities $p_s(q)$ greater than the median of the probabilities. The function $f(p_s(q))$ in this case returns 1 for $Dp_s(q) \geq \log(2)$, and 0 in the other case. The fidelity estimator uses the following normalization

$$F = \frac{1}{\log(2)} \langle 2n_s(q) - 1 \rangle \ , \tag{11.29}$$

where $n_s(q)$ is defined to be 1 if $Dp_s(q) \geq \log(2)$, and 0 otherwise. The standard deviation of this estimator is $\sqrt{[\log^{-2}(2) - F^2]/N_s}$, which is always larger than for the XEB. See Fig. S9 for comparison of the fidelity estimates produced by linear XEB and the HOG-based fidelity estimator. HOG test is also related to a definition of quantum volume [39].

11.4.3 Two limiting cases

Here, we consider two special cases of Eq. (11.27) and the formula (1) in the main paper [1]. First, suppose bitstrings q_i are sampled from the uniform distribution. In this case the sampling probability is $1/D$ for every bitstring and $\mathcal{F}_{\text{XEB}} = 0$. Therefore, if the qubits are in the maximally mixed state, the estimator yields zero fidelity, as expected.

Second, suppose that bitstrings are sampled from the theoretical output distribution of a random quantum circuit. Assume that the distribution has Porter-Thomas shape. By Eq. (11.26), the fraction of bitstrings with theoretical probability in $[p, p + dp]$ is

$$\Pr(p)\, dp = De^{-Dp} dp \tag{11.30}$$

and the total number of such bitstrings is

$$N(p)\, dp = D^2 e^{-Dp}\, dp. \tag{11.31}$$

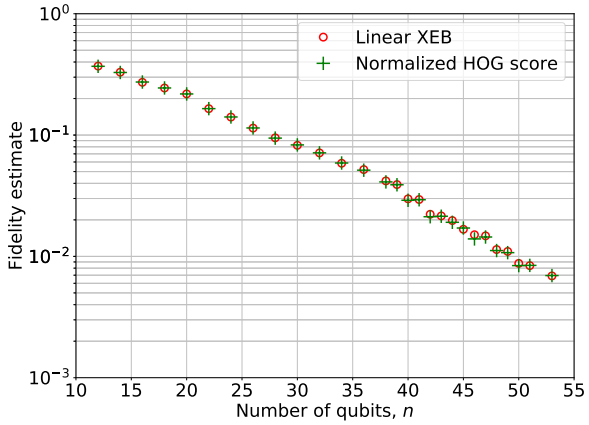


Figure S9: Comparison of fidelity estimates obtained using linear XEB, Eq. (11.27) and normalized HOG score, Eq. (11.29) from bitstrings observed in our experiment using elided circuits (see Section 11.7.7). Standard deviation smaller than markers.

Therefore, the probability that a bitstring with probability in $[p, p+dp]$ is sampled equals

$$p \cdot N(p)\, dp = pD^2 e^{-Dp}\, dp = f(p)\, dp \tag{11.32}$$

where $f(p)$ is the probability density function of the random variable defined as the ideal probability of a sampled bitstring, i.e. the random variable which is being averaged in the formula (1) of the main paper. Thus, the average probability of a sampled bitstring is

$$\begin{aligned} \langle p_s(q) \rangle &= \int_0^1 p f(p)\, dp = \int_0^1 p^2 D^2 e^{-Dp}\, dp \\ &= \frac{2}{D}\left(1 - e^{-D}\left(\frac{D^2}{2} + D + 1\right)\right) \approx \frac{2}{D}. \end{aligned} \tag{11.33}$$

Substituting into equation (1) in the main paper yields $\mathcal{F}_{\text{XEB}} = 1$. The general case of a depolarizing error can be obtained from the two limiting cases by convex combination.

11.4.4 Measurement errors

We now consider how measurement errors affect the estimation of fidelity. Let us assume uncorrelated classical measurement errors, so that if the "actual" measurement result of a qubit is 0, we can get 1 with probability e_{m0}, and similarly with probability e_{m1} we get 0 for actual result 1, i.e., $p(1|0) = e_{m0}$, $p(0|0) = 1 - e_{m0}$, $p(0|1) = e_{m1}$, $p(1|1) = 1 - e_{m1}$. In this case the probability to get measurement result $q = k_1 k_2 .. k_n$ for actual result $q' = k'_1 k'_2 .. k'_n$ is the product of the corresponding factors. The probability of correct measurement result is then

$$\begin{aligned} p_{\text{m}}(q') &= (1 - e_{m0})^{n - |q'|} (1 - e_{m1})^{|q'|} \\ &\approx (1 - e_{m0})^{n/2} (1 - e_{m1})^{n/2}, \end{aligned} \tag{11.34}$$

where $|q'|$ is the number of 1s (Hamming distance from 00..0) in the initial bitstring q', and in the second expression we approximated $|q'|$ with $n/2$ for large n.

Now let us make a natural assumption that if there was one or more measurement errors, $q' \to q$, then the resulting ideal probability $p_s(q)$ is uncorrelated with the actual ideal probability $p_s(q')$. Using this assumption we can write

$$F = F_U p_{\text{m}} \tag{11.35}$$

where F_U is the circuit fidelity and F is the complete (effective) fidelity. The complete fidelity F is estimated as before. The measurement fidelity $p_{\rm m}$ can be obtained independently. For instance, we can prepare a bistring q and measure immediately to obtain the probability of a correct measurement result for q. We obtain $p_{\rm m}$ by repeating this for a set of random bitstrings. We can therefore obtain F_U from Eq. (11.35). As explained above, fitting the depolarization fidelity per cycle p_c for different circuit depths m is also a method to separate measurement errors.

The state preparation errors can be treated similarly, assuming that a single error leads to uncorrelated resulting distribution $p_s(q)$, so that the measurement fidelity $p_{\rm m}$ in Eq. (11.35) is combined with a similar factor describing the state preparation fidelity.

11.5 Quantifying errors

An important test for this experiment is predicting XEB fidelity $\mathcal{F}_{\rm XEB}$ based on simpler measurements of single- and two-qubit errors. Here we review how this is calculated, illustrating important principles with the example of a single qubit. The general theory is described at the end of this section.

First, we assume Pauli errors describe decoherence using a depolarizing model. This model is used, for example, to compute thresholds and logical error rates for error correction. The parameter describing decoherence in a single qubit is the Pauli error e_P, giving a probability $e_P/3$ for applying an erroneous X, Y, or Z gate to the qubit after the gate, corresponding to a bit and/or phase flip.

Second, the depolarization model is assumed to describe the system state using simple classical probability. The probability of no error for many qubits and many operations, corresponding to no change to the system state, is then found by simply multiplying the probability of no error for each qubit gate. This is a good assumption for RB and XEB since a bit- or phase-flip error effectively decorrelates the state. The depolarization model assumes that when there is an error with probability e_d, the system state randomly splits to all qubits states, which has Hilbert space dimension $D = 2^n$. This is described by a change in density matrix $\rho \to (1 - e_d)\rho + e_d \times \mathbb{1}/D$. Note the depolarization term has a small possibility of the state resetting back to its original state. For a single qubit where $D = 2$, this can be described using a Pauli-error type model as a probability $e_d/4$ applying a I, X, Y, or Z gate. Comparing to the Pauli model, the error probability thus needs to be rescaled by $e_d = e_P/(1 - 1/D^2)$. This gives a net polarization p of the qubit state due to many Pauli errors as

$$p = \prod_i \left[1 - e_P(i)/\left(1 - 1/D^2\right)\right]. \tag{11.36}$$

Third, the effect of this depolarization has to be accounted for considering the measured signal. The measured signal for randomized benchmarking is given by $RB = p(1-1/D)+1/D$, which can be understood in a physical argument that a complete randomization of the state has a 1/D chance to give the correct final state. A cross-entropy benchmarking measurement gives $\mathcal{F}_{\rm XEB} = p$. A measurement of p, which can have offsets and prefactors in these formulas, also includes other scaling factors coming from state preparation and measurement errors. All of these scaling issues are circumvented by applying gates in a repeated number of cycles m such that $p = p_c^m$. A measurement of the signal versus m can then directly pull out the fractional polarization change per cycle, p_c, independent of these scale factors.

Fourth, from this polarization change we can then compute the Pauli error, which is the metric that should be reported since it is the fundamental error rate that is independent of D. Unfortunately, a fidelity $1 - e_P/(1 + 1/D)$ for RB is commonly reported, which has a D-dependent correction. We recommend this practice be changed, but note that removing the

Table 11: A "Rosetta stone" translation between error metrics. In single- and two-qubit RB or XEB experiments, we measure the per-gate (or per-cycle) depolarization decay constant p. The second column shows conversions from this rate to the various error metrics. The last two columns are representative comparisons for 0.1% Pauli error.

Error metric	Relation to depolarization decay constant p	n=1 (D=2)	n=2 (D=4)
Pauli error (e_p, r_P) [1]	$(1-p)(1-1/D^2)$	0.1%	0.1%
Average error (e_a, r)	$(1-p)(1-1/D)$	0.067%	0.08%
Depolarization error (e_d)	$1-p$	0.133%	0.107%

$1/(1+1/D)$ factor decreases the reported fidelity value. We also recommend reporting Pauli error, e_P instead of entanglement fidelity $(1-e_P)$, since it is more intuitive to understand how close some quantity is to 0 than to 1. Table 11 summarizes the different error metrics and their relations.

This general model can also account for non-depolarizing errors such as energy decay, since quantum states in an algorithm typically average over the entire Bloch sphere (as in XEB), or for example when the algorithm purposely inserts spin-echoes. Thus the average effect of energy decay effectively randomizes the state in a way compatible with Pauli errors. For a gate of length t_g with a qubit decay time T_1, averaging over the Bloch sphere (2 poles and 4 equator positions) gives (to first order) an average error probability $e_a = t_g/3T_1$. Using Table 11, this converts to a Pauli error $e_P = t_g/2T_1$.

A detailed theory of the D scaling factor is as follows. In order to arrive at a first order estimate on how error rates accumulate on random quantum circuits, the errors can be modeled via the set of Kraus operators. The density matrix of the system ρ after application of a gate is connected to the density matrix ρ_0 before the gate as follows:

$$\rho = \Lambda(\rho_0) = \sum_{k=0}^{K} A_k \rho_0 A_k^\dagger, \quad \sum_k A_k^\dagger A_k = \mathbb{1}. \tag{11.37}$$

For the closed-system quantum evolution with unitary U (no dephasing nor decay) the sum on the right hand side contains only one term with k=0 and $A_0 = U$. In general, Kraus operators describe the physical effects of many types of errors (control error, decoherence, etc.) that can explicitly depend on the gate. Knowing the Kraus operators allows us to calculate the total error budget as well as its individual components.

Conventionally, circuit fidelities are reported as a metric of its quality. To make a connection to physically observable quantities, the average fidelity can be expressed in terms of Kraus operators. In the absence of leakage errors and cross-talk the average fidelity equals

$$F = 1 - \frac{e_P}{1+1/D}, \quad e_P = 1 - \frac{1}{D^2}\sum_{k=0}^{K} |\operatorname{tr}\left(U A_k^\dagger\right)|^2 \tag{11.38}$$

where $D = 2^n$ is the dimension of the Hilbert space and the quantity e_P plays a role of a Pauli error probability in the depolarizing channel model (see below).

For random circuits the effects of errors can be described by a depolarizing channel model, with Kraus operators of the form

$$\begin{aligned} A_{\mathbf{k}} &= \sqrt{\frac{e_P}{D^2-1}}\, P_{\mathbf{k}} U, \quad \mathbf{k} \neq \mathbf{0}, \\ A_{\mathbf{0}} &= \sqrt{1-e_P}\, P_{\mathbf{0}} U, \\ P_{\mathbf{k}} &= \sigma_{k_1} \otimes \sigma_{k_2} \ldots \otimes \sigma_{k_n} \end{aligned} \tag{11.39}$$

where $P_{\mathbf{k}}$ are strings of Pauli operators σ_{k_j} for individual qubits for $k_j = 1, 2, 3$ and also identity matrices σ_0 in the qubit subspace for $k_j = 0$. This form assumes that individual Pauli errors all happen with the same probability e_P.

To make a connection to experimental measurements of the cross-entropy we substitute (11.39) into (11.37) and obtain

$$\Lambda(\rho_0) = (1 - e_P)U\rho_0 U^{-1} + \frac{e_P}{D - 1/D}\left(\mathbb{1} - \frac{U\rho_0 U^{-1}}{D}\right). \quad (11.40)$$

We compare this expression with the standard form of the depolarizing channel model

$$\Lambda(\rho_0) = pU\rho_0 U^{-1} + (1 - p)\frac{\mathbb{1}}{D}, \quad (11.41)$$

expressed in terms of the depolarization fidelity parameter p. Note the difference between the expressions. On the one hand, in (11.41) the second term corresponds to full depolarization in all directions. On the other hand, in (11.40) the second term describes full depolarization in all directions except for the direction corresponding to the ideal quantum state.

From (11.40), (11.41) one can establish the connection between the Pauli error rate and depolarizing fidelity parameter p

$$e_P = (1 - p)(1 - 1/D^2) \quad (11.42)$$

We note that the explicit assumption of connecting Pauli errors to depolarization is needed for the small D case, typically for single- and two-qubit error measurements. Once we have measured the Pauli errors, then only a simple probabilistic calculation is needed to compute $\mathcal{F}_{\text{XEB}}$ in the large D case.

11.6 Metrology and calibration

11.6.1 Calibration overview

Quantum computations are physically realized through the time-evolution of quantum systems steered by analog control signals. As quantum information is stored in continuous amplitudes and phases, these control signals must be carefully chosen to achieve the desired result. Calibration is the process of performing a series of experiments on the quantum system to learn optimal control parameters.

Calibration is challenging for a number of reasons. Analog control requires careful control-pulse shaping as any deviation from the ideal will introduce error. Qubits require individual calibration as variations in the control system and qubits necessitate different control parameters to hit target fidelities. Optimal control parameters can also drift in time, requiring calibrations to be revisited to maintain performance. Additionally, the full calibration procedure requires bootstrapping: using a series of control sequences with increasing complexity to determine circuit and control parameters to increasingly higher degrees of precision. Lastly, each qubit needs to perform a number of independent operations which are independently calibrated: single-qubit gates, two-qubit gates, and readout.

Our Sycamore processor offers a high degree of programmability: we can dynamically change the frequency of each qubit, as well as the effective qubit-qubit coupling between nearest neighbor qubits. This tunability gives us the freedom to enact many different control strategies, as well as account for non-uniformities in the processor's parameters. However, these extra degrees of freedom are a double-edged sword. Additional control knobs always introduce a source of decoherence and control errors as well as an added burden on calibration.

Our approach is to systematize and automate our calibration procedure as much as possible, thus abstracting complexity away. This automation allows us to turn calibration into a science, where we can compare calibration procedures to determine optimal strategies for time, performance, and reliability. By employing calibration science to study full-system performance with different control strategies, we have been able to improve full-system fidelities by over an order of magnitude from initial attempts while decreasing the calibration time and improving reliability. Lastly, we design our calibration to be done almost entirely at the single- or two-qubit level, rather than at the system level, in order to be as scalable as possible.

Device registry

The device registry is a database of control variables and configuration information we use to control our quantum processors. The registry stores information such as operating frequencies, control biases, gate parameters such as duration, amplitude, parameterization of circuit models, etc. The goal of calibration is to experimentally determine and populate the registry with optimal control parameters. We typically store >100 parameters per qubit to achieve high fidelity across all of the various qubit operations. The large number of parameters and subtle interdependencies between them highlights the need for automated calibration.

Scheduling calibrations: “Optimus"

We seek a strategy for identifying and maintaining optimal control parameters for a system of physical qubits given incomplete system information. To perform these tasks, we use the “Optimus" formulation as in Ref [40], where each calibration is a node in a directed acyclic graph that updates one or more registry parameters, and the bootstrapping nature of calibration sequences is represented as directed edges between nodes. Now, calibrating a system of physical qubits becomes a well-defined graph traversal problem. The calibration graph used for the Sycamore device can be see in Figure S10. This strategy is particularly useful for maintaining calibrations in the presence of drift, where we want to do the minimal amount of work to bring the system back in spec, and when extending the calibration procedure, as interdependencies are explicit. Typical timescales for bringup of a new Sycamore processor are approximately 36 hours upon first cooldown, and 4 hours per day thereafter for maintaining calibrations. These times are specific to current available technology, and can be significantly improved.

11.6.2 Calibration procedure

Device configuration

Throughout the calibration procedure, the device registry may be configured in different states in order to calibrate certain parameters. We call these different states “device configurations", and different kinds of configurations reflect our knowledge of the system at different points in the full calibration procedure. As illustrated in Figure S11, the primary difference between the different configurations is the set of “active" qubits, where active qubits are biased to an operating frequency between 5-7 GHz, and “inactive" qubits are biased near zero frequency. Following the outline above, we have three device configurations of interest:

Root config.

The root configuration is the starting state of the system immediately after cool down and basic system verification. In this configuration, we calibrate coarse frequency vs bias curves for each readout resonator, qubit, and coupler.

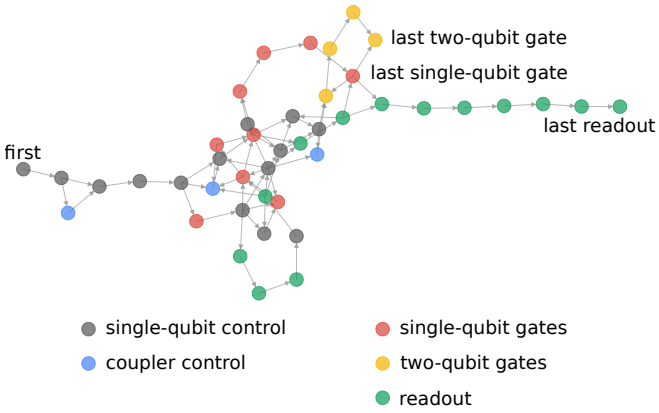


Figure S10: **Optimus calibration graph for Sycamore.** Calibration of physical qubits is a bootstrapping procedure between different pulse sequences or "experiments" to extract control and system parameters. Initial experiments are coarse and have interplay between fundamental operations and elements such as single-qubit gates, readout, and the coupler. Final experiments involve precise metrology for each of the qubit operations: single-qubit gates, two-qubit gates, and readout.

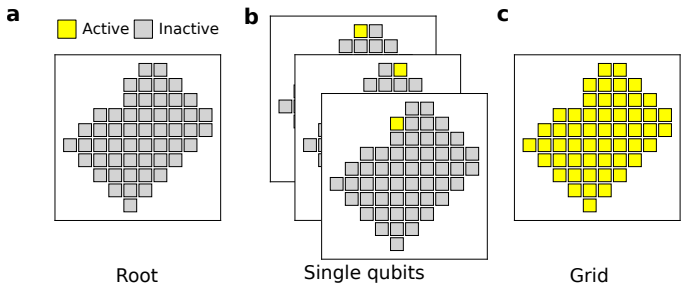


Figure S11: **Configurations of the device over the course of calibration. a,** In the root configuration, we start with no knowledge of the system and measure basic device parameters. **b,** We create a single qubit configuration for each qubit, where all qubits except the qubit of interest are biased to near zero frequency. **c,** Using knowledge learned in the single qubit configurations, we build a grid of qubits.

Single qubit config.

After completing root calibrations, we now know how to bias each qubit to its minimum and maximum frequencies. We create one configuration of the device registry for each qubit, where the qubit of interest is biased in a useful region (5-7 GHz) and the remaining qubits are biased to their minimum frequencies in order to isolate the qubit of interest. In each of these configurations, we fine tune the bias vs frequency curves for the qubit and its associated couplers and resonators, and also measure T_1 as a function of frequency, necessary due to background TLS defects and modes.

Grid config.

After completing calibrations in each isolated qubit configuration, we feed the information we learned into a frequency optimization procedure. The optimizer places the biases for each qubit and coupler in a user defined grid of any desired size up to the entire chip. We then proceed to calibrate high fidelity single qubit gates, two qubit gates, and readout.

Root config: procedure

We begin calibration with simple frequency-domain experiments to understand how each qubit and coupler responds to its flux bias line.

- Calibrate each parametric amplifier (flux bias, pump frequency, pump power).
- For each qubit, identify its readout resonator and measure the readout signal versus qubit bias ("Resonator Spectroscopy") [41]. Estimate the resonator and qubit frequency as a function of qubit bias.
- For each coupler, place one of its qubits near maximum frequency and the other near minimum frequency, then measure the readout signal of the first qubit as a function of coupler bias. The readout signal changes significantly as the coupler frequency passes near the qubit frequency. Identify where the coupler is near its maximum frequency, so the qubit-qubit coupling is small (a few MHz) and relatively insensitive to coupler bias.

Single-qubit config: procedure

After setting the biases to isolate a single qubit, we follow the procedure outlined in [42] which we will summarize here:

- Perform fixed microwave drive qubit spectroscopy while sweeping the qubit bias and detecting shifts in the resonator response, to find the bias that places the qubit at the desired resonant frequency.
- Using the avoided level crossing identified in the root config, determine the operating bias to bring the qubit on resonance with its readout resonator to perform active ground state preparation. We use a 10 μs pulse consistent with the readout resonator ringdown time.
- Perform power Rabi oscillations to find the drive power that gives a π pulse to populate the $|1\rangle$ state.
- Optimize the readout frequency and power to maximize readout fidelity.
- Fine tune parameters (qubit resonant frequency, drive power, drive detuning [43]) for π and $\pi/2$ pulses.

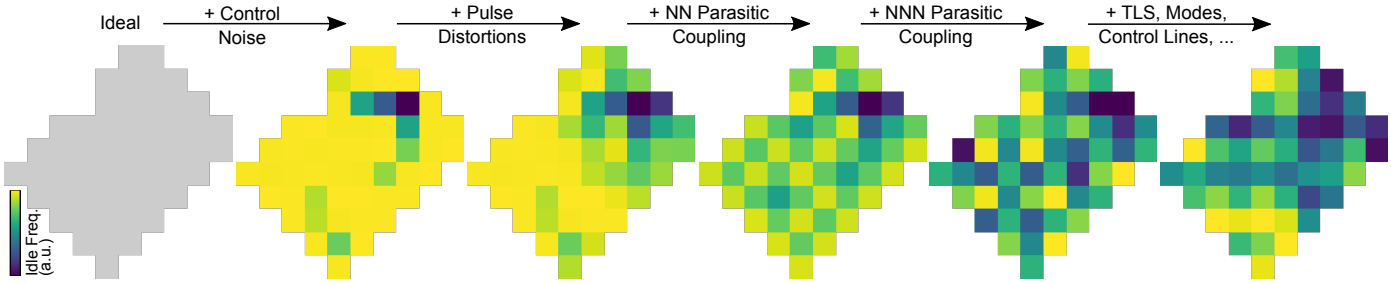


Figure S12: **Idle frequency solutions found by our Snake optimizer with different error mechanisms enabled.** The optimizer makes increasingly complex tradeoffs as more error mechanisms are enabled. These tradeoffs manifest as a transition from a structured frequency configuration into an unstructured one. Similar tradeoffs are simultaneously made in optimizing interaction and readout frequencies. Optimized idle and interaction operating frequencies are shown in Figure S13 and optimized readout frequencies are shown in Figure S20. Color scales are chosen to maximize contrast. Grey indicates that there is no preference for any frequency.

- Calibrate the timing between the qubit microwave drive, qubit bias, and coupler bias.
- Perform qubit spectroscopy as a function of qubit bias to fine tune the qubit bias vs frequency curves.
- Measure T_1 vs. frequency by preparing the qubit in $|1\rangle$ then biasing the qubit to a variable frequency for a variable amount of time, and measuring the final population [44].
- Measure the response of a qubit to a detuning pulse to calibrate the frequency-control transfer function [45, 6, 42].

With the single-qubits calibrated in isolation, we have a wealth of information on circuits parameters and coherence information for each qubit. We use this information as input to a frequency placement algorithm to identify optimal operating frequencies for when the full processor is in operation.

Optimizing qubit operating frequencies

In our quantum processor architecture, we can independently tune each qubit's operating frequency. Since qubit performance varies strongly with frequency, selecting good operating frequencies is necessary to achieve high fidelity gates. In arbitrary quantum algorithms, each qubit operates at three distinct types of frequencies: idle, interaction, and readout frequencies. Qubits idle and execute single-qubit gates at their respective idle frequencies. Qubit pairs execute two-qubit gates near their respective interaction frequencies. Finally, qubits are measured at their respective readout frequencies. In selecting operating frequencies, it is necessary to mitigate and make nontrivial tradeoffs between energy-relaxation, dephasing, leakage, and control imperfections. We solve and automate the frequency selection problem by abstracting it into an optimization problem.

We construct a quantum-algorithm-dependent and gate-dependent optimization objective that maps operating frequencies onto a metric correlated with system error. The error mechanisms embedded within the objective function are parasitic coupling between nearest-neighbor and next-nearest-neighbor qubits, spectrally-diffusing two-level-system (TLS) defects [44], spurious microwave modes, coupling to control lines and the readout resonator, frequency-control electronics noise, frequency-control pulse distortions, microwave-control pulse distortions, and microwave-carrier bleedthrough. Additional considerations in selecting readout frequencies are

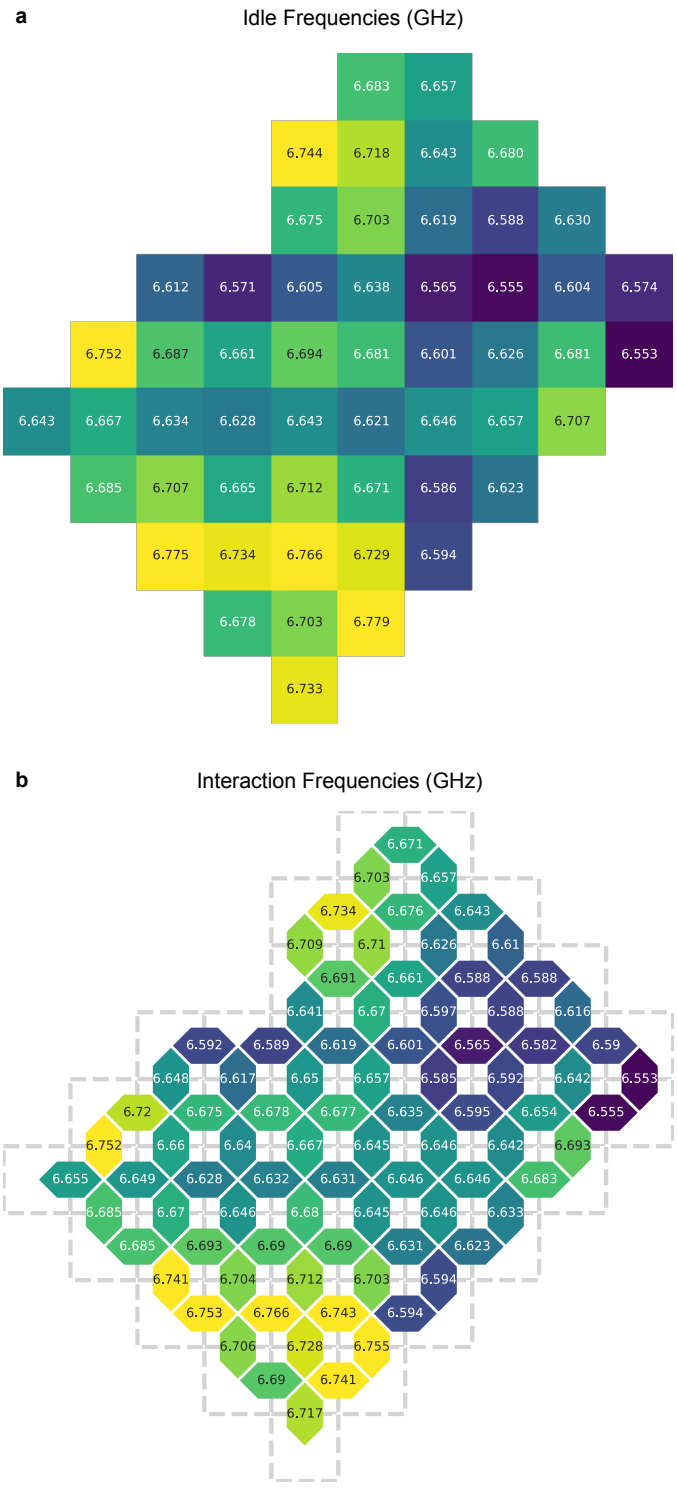


Figure S13: **Optimized idle and interaction frequencies found by our Snake optimizer. a,** Idle frequencies, **b,** interaction frequencies. Readout frequencies are shown in Figure S20. These solutions are sufficient for state-of-the-art system performance. See Figure S12 to understand some of the tradeoffs that are made during optimization. Color scales are chosen to maximize contrast.

covered in Section 11.6.4. The objective is constructed from experimental data and numerics, and the individual error mechanisms are weighted by coefficients determined either heuristically or through statistical learning.

Minimizing the objective function is a complex combinatorial optimization problem. We characterize the complexity of the problem by the optimization dimension and search space. For a processor with N qubits on a square lattice with nearest-neighbor coupling, there are N idle, N readout, and $\sim 2N$ interaction frequencies to optimize. In an arbitrary quantum algorithm, all frequencies are potentially intertwined due to coupling between qubits. Therefore, the optimization dimension is $\sim 4N$. The optimization search-space is constrained by qubits' circuit parameters and control-hardware specifications. Discretizing each qubit's operational range to 100 frequencies results in an optimization search space of $\sim 100^{4N}$. This is much larger than the dimension of the Hilbert space of an N qubit processor, which is 2^N.

Given the problem complexity, it is assumed that finding globally optimal operating frequencies is intractable. However, we have empirically verified that locally optimal solutions are sufficient for state-of-the-art system performance. To find local optima, we developed the "Snake" homebrew optimizer that combines quantum algorithm structure with physics intuition to exponentially reduce optimization complexity and take intelligent optimization steps. For the circuits used here, the optimizer exploits the time-interleaved structure of single-qubit gates, two-qubit gates, and readout. For our 53 qubit processor, it returns local optima in ~ 10 seconds on a desktop. Because of its favorable scaling in runtime versus number of qubits, we believe the Snake optimizer is a viable long-term solution to the frequency selection problem.

To illustrate how the Snake optimizer makes tradeoffs between error mechanisms, we plot idle frequency solutions with different error mechanisms enabled (Figure S12). Starting with an ideal processor with no error mechanisms enabled, there is no preference for any frequency configuration. Enabling frequency-control electronics noise, the optimizer pushes qubits towards their respective maximum frequencies, to minimize flux-noise susceptibility. Note that each qubit has a different maximum frequency due to fabrication variability. Enabling frequency-control pulse distortions forces a gradual transition between qubit frequencies to minimize two-qubit-gate frequency-sweep amplitudes. Enabling nearest-neighbor (NN) and next-nearest neighbor (NNN) parasitic coupling further lowers the degeneracy between qubit frequencies into a structure that resembles a multi-tiered checkerboard. Finally, enabling errors from TLS defects, spurious microwave modes, and all other known error mechanisms removes any obvious structure. A set of optimized idle and interaction frequencies is shown in Figure S13, and readout frequencies are shown in Figure S20.

Grid config: procedure

Calibrating a grid of qubits follows the same procedure as calibrating an isolated qubit with additional calibrations to turn off the qubit-qubit coupling.

- Achieve basic state discrimination for each qubit at its desired frequency.
- For each coupler, minimize the qubit-qubit coupling (note changing coupler biases affects qubit frequencies). For each case below, we choose the coupler bias minimizing the interaction.
  - For qubit pairs idling within 60 MHz of each other, use a resonant swapping experiment. We excite one qubit and apply flux pulses to nominally put the qubits on resonance and let the qubits interact over time [9].
  - For qubit pair idling further apart, use a conditional phase experiment. We perform two Ramsey experiments on one qubit, where the other qubit is in the ground state

and the excited state, to identify the state-dependent frequency shift of the first qubit.

- Adjust the qubit biases to restore the desired qubit frequencies and proceed with qubit calibration as in the single-qubit configurations.
- Calibrate the entangling gate.
  - Estimate the qubit pulse amplitudes to reach the desired interaction frequency with their frequency versus bias calibration.
  - Fine-tune the qubit pulse amplitudes to reach resonance, compensating for pulse undershoot.
  - Tune the coupler pulse amplitude to achieve a complete photon exchange.

In the next two sections, we describe in more detail the fine tuning required to achieve high fidelity two qubit gates and multiqubit readout.

11.6.3 Two-qubit gate metrology

High-fidelity two-qubit gates are very hard to achieve. In an effort to make this easier, we design qubits with tunable frequencies and tunable interactions. This added control allows for immense flexibility when implementing gates. In the following subsections, we discuss a simple high-fidelity control and metrology strategy for two-qubit gates in our system.

The natural two-qubit gate for transmon qubits

Consider two transmon qubits at different frequencies (say 6.0 and 6.1 GHz). Here are two potential ways of generating a multi-qubit gate in this system. If the qubits are tuned into resonance, then excitations swap back-and-forth and this interaction can be modeled as a partial-iSWAP gate [46]. If the qubits are detuned by an amount close to their nonlinearity, then the 11-state undergoes an evolution that can be modeled as a controlled-phase gate (assuming the population does not leak) [47, 48]. In fact, any two-qubit control sequence that does not leak can be modeled as a partial-iSWAP followed by a controlled-phase gate.

A typical control sequence is shown Fig. S14a. Gate times of 12 ns are chosen to trade off decoherence (too slow) and leakage to higher states of the qubit (too fast). Figure S14b depicts how this operation can be decomposed as a quantum circuit. This circuit contains Z-rotations that result from the frequency excursions of the qubits, and can be expressed by the unitary:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & e^{i(\Delta_+ + \Delta_-)}\cos\theta & -ie^{i(\Delta_+ - \Delta_{-,\mathrm{off}})}\sin\theta & 0 \\ 0 & -ie^{i(\Delta_+ + \Delta_{-,\mathrm{off}})}\sin\theta & e^{i(\Delta_+ - \Delta_-)}\cos\theta & 0 \\ 0 & 0 & 0 & e^{i(2\Delta_+ - \phi)} \end{bmatrix}. \tag{11.43}$$

These gates have an efficient mapping to interacting fermions and have been coined 'fSim' gates, short for fermionic simulation [49]. The long-term goal is to implement the entire space of gates (shown in Fig. S14c).

For quantum supremacy, the two-qubit gate of choice is the iSWAP gate. For example, CZ is less computationally expensive to simulate on a classical computer by a factor of two [38, 50]. A dominant error-mechanism when trying to implement an iSWAP is a small conditional-phase that is generated by an interaction of the $|11\rangle$-state with higher states of the transmons ($|02\rangle$ and $|20\rangle$). For this reason, the fSim gate with swap-angle $\theta \approxeq 90°$ and conditional phase $\phi \approxeq 30°$ has become the gate of choice in our supremacy experiment. Note that small deviations from

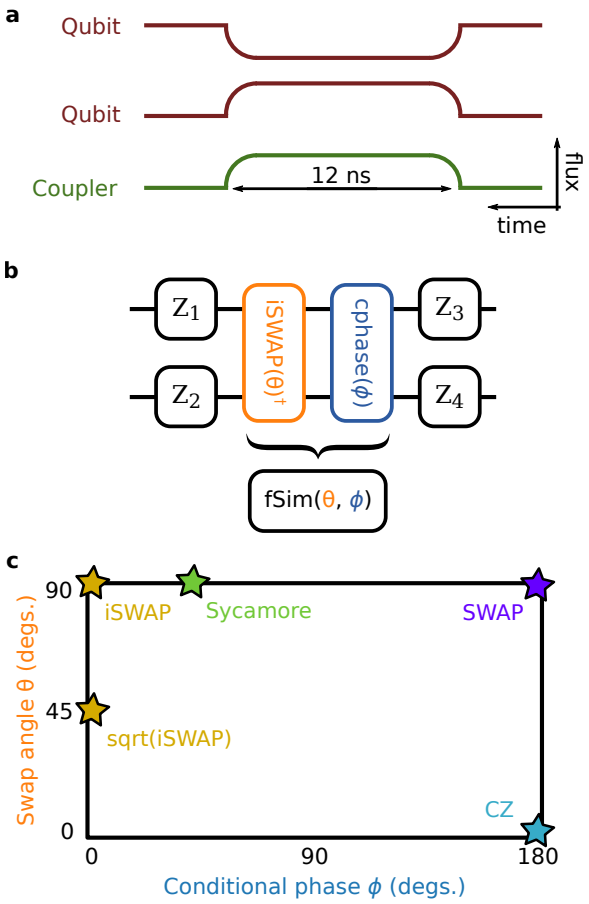


Figure S14: **Two-qubit gate strategy. a,** Control waveforms for two qubits and a coupler. Each curve represents the control flux applied to the qubit's and coupler's SQUID loops as a function of time. **b,** Generic circuit representation for an arbitrary two-qubit gate using flux pulses. This family of gates have been named "fSim" gates, short for fermionic-simulation gates. Our definition of the fSim gate uses θ with the sign opposite to the common convention for the iSWAP gate. **c,** Control landscape for fSim gates as a function of the swap angle and conditional phase, up to single qubit rotations. The coordinates of common entangling gates are marked along with the Sycamore gate fSim($\theta = 90°, \phi = 30°$).

these angles are also viable quantum supremacy gates. These gates result from the natural evolution of two qubits making them easy to calibrate, high intrinsic fidelity gates for quantum supremacy.

Using cross entropy to learn a unitary model

We have recently introduced cross-entropy as a fidelity metric for quantum supremacy experiments. Cross-entropy benchmarking (XEB) was introduced as an analog to randomized benchmarking (RB) that can be used with any number of qubits and is independent of state-preparation and measurement errors [6, 27].

A distinct advantage of XEB is that the resulting data can be analyzed to find an optimal representation of a unitary; this process is outlined in Fig. S15. The gate sequence for a two-qubit XEB experiment is shown in Fig. S15a. The sequence alternates between single-qubit gates on both qubits and a two-qubit gate between them. At the end of the sequence, both qubits are measured and the probabilities of bitstrings (00, 01, 10, 11) are estimated. This procedure is repeated for ~10-20 instances of randomly selected single-qubit gates. The measured probabilities can then be compared to the ideal probabilities using the expression for

fidelity Eq. (3) in Ref. [6].

The data from a two-qubit XEB experiment is shown in Fig. S15b (green dots). By performing additional sequences with tomography rotations prior to measurement, we can infer the decay of purity with increasing circuit depth (blue dots). For two qubits, the decay of fidelity tells us the total error of our gates while the purity decay tells us the contribution from decoherence —the difference is control error. Based on the data in green and blue, it appears that the total error is about half control and half decoherence.

So far, we have established a generic unitary model (Fig. S14b), a training dataset (Fig. S15a), and a cost-function (Fig. S15b). These three ingredients form the foundation for using optimization techniques to improve fidelity. Using a simple Nelder-Mead optimization protocol, we can maximize the XEB fidelity by varying the parameters of the unitary model. The fidelity decay curve for the optimal unitary model are shown in Fig. S15b (orange dots). The optimized results are nearly coherence limited.

The optimal control-model parameters for all pairs are shown as integrated histograms in Fig. S16a,b. Panel (a) shows the histograms for partial-iSWAP angles (∼90 degrees) and conditional phases (∼30 degrees). Panel (b) shows histograms for the various flavors of Z-rotations. While conceptually there are four possible Z-rotations (see Fig. S14b), only three of these rotations are needed to uniquely define the operation. These three rotations can be thought of as the detuning of the qubits before the iSWAP, the detuning after the iSWAP, and an overall frequency shift of both qubits which commutes with the iSWAP.

Comparison with randomized benchmarking

In Fig. S17 we show that two-qubit gate fidelity extracted using XEB agrees well with the fidelity as measured with RB, an important sanity check in validating XEB as a gate metrology tool. In two-qubit XEB, we extract the error per cycle which consists of a single-qubit gate on each qubit and a two-qubit gate between them. In Fig. S17a we show the individual RB decay curves for single-qubit gates. In panel b, we show the RB decay curve for benchmarking a CZ gate. Adding up the three errors from RB, we would expect an XEB cycle error of 0.57%. In panel c, we show the measured XEB decay curve which indicates a cycle error of 0.59% —nearly identical to the value predicted by RB.

For single-qubit gate benchmarking on the Sycamore device used in this work (see Table 12), we find that π pulse fidelities are somewhat worse than $\pi/2$ pulse fidelities, which we attribute to reflections from the imperfect microwave environment. Because the XEB gateset we have used consists only of $\pi/2$ pulses, we find that the single-qubit gate errors extracted from conventional RB, which contains π pulses, are somewhat higher than those extracted from single-qubit XEB. Using only $\pi/2$ pulses instead of π pulses in single-qubit RB brings the extracted error close to that measured via XEB.

Speckle purity benchmarking (SPB)

It is experimentally useful to be able to extract state purity from XEB experiments in order to error-budget the contribution of decoherence. Conventionally, purity estimation can be done with state tomography, where the full density matrix ρ is reconstructed and used to quantify the state purity. This involves expanding a single sequence into a collection of sequences each appended with single-qubit gates. Unfortunately, full tomographic reconstruction scales exponentially in the number of qubits, both for the number of sequences needed as well as the number of measurements needed per sequence. Here, we introduce an exponentially more efficient method to extract the state purity without additional sequences.

We use a re-scaled purity definition such that a fully-decohered state has a purity of 0, and

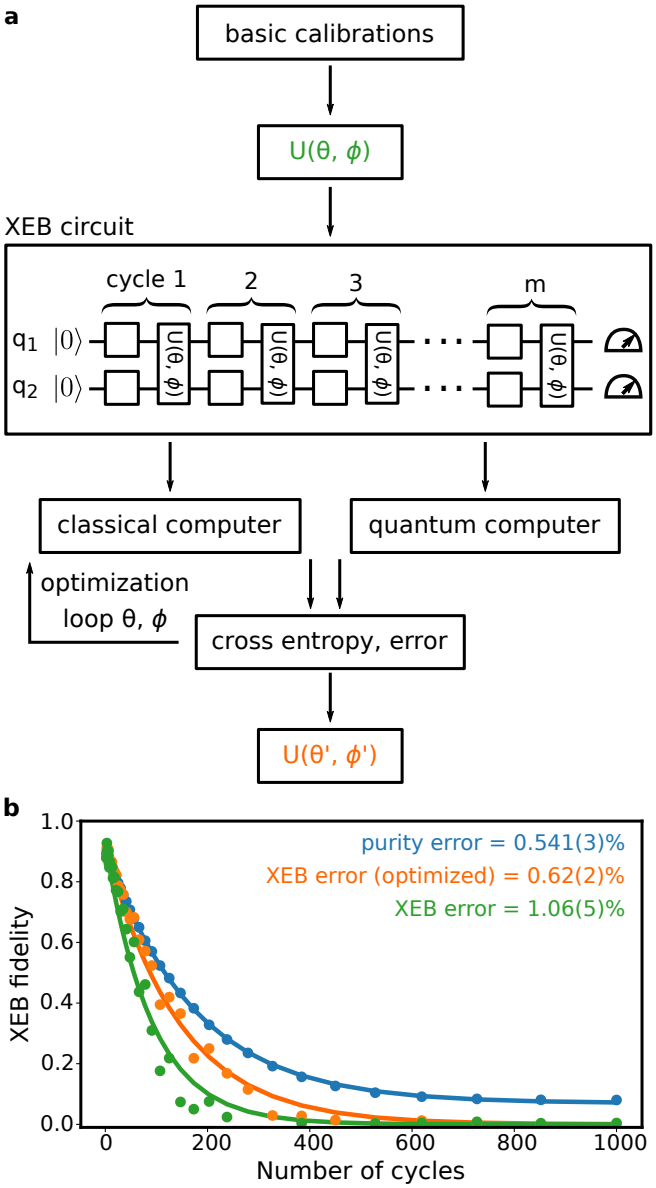


Figure S15: **Using XEB to learn a unitary model. a,** Process flow diagram for using XEB to learn a unitary model. After running basic calibrations, we have an approximate model for our two-qubit gate. Using this gate, we construct a random circuit that is fed into both the quantum computer and a classical computer. The results of both outputs can be compared using cross-entropy. Optimizing over the parameters in the two qubit model provide a high-fidelity representation of the two-qubit unitary. **b,** Data from a two-qubit XEB experiment. The two-qubit purity (blue) was measured tomographically and provides the coherence-limit of the operations. The decay of the XEB fidelity is shown in green and orange. In orange, the parameters of a generic unitary model were optimized to determine a higher-fidelity representation of the unitary. All errors are quoted as Pauli errors.

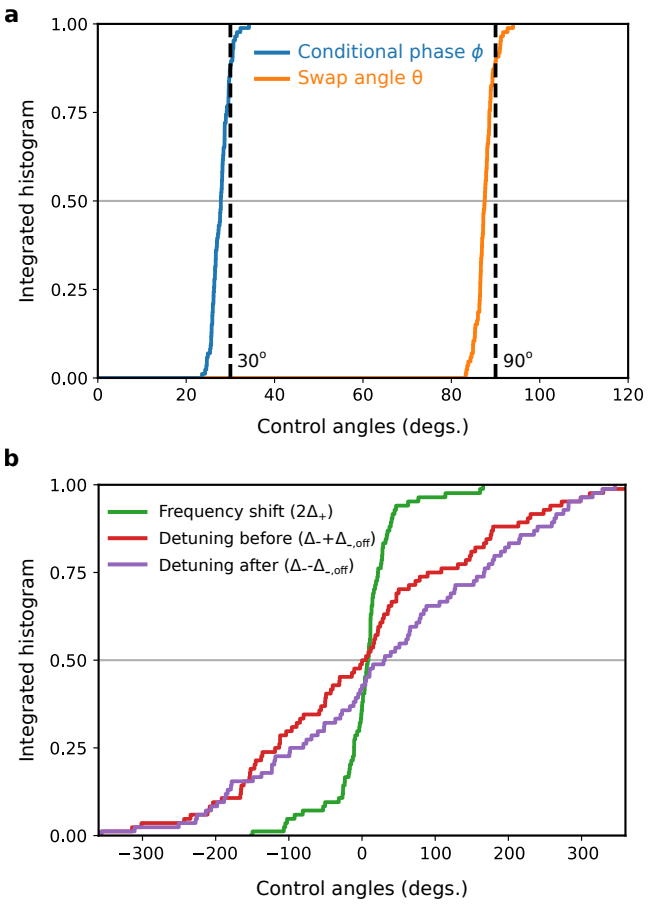


Figure S16: **Parameters of the control model.** A generic model for two-qubit gates using flux-control has five free parameters. Using XEB we can measure these parameters with high fidelity. **a,** Integrated histogram (cumulative distribution) of the control parameters that determine the interaction between the qubits. **b,** An integrated histogram of the remaining three parameters that represent different flavors of single-qubit Z-rotations. While the first two parameters (panel a) define the entangling gate, the final three parameters (panel b) are simply measured and then kept track of during an algorithm. Intuitively, these three angles correspond to a detuning before the swap, a detuning after the swap, and an overall frequency shift which commutes through the swap; these correspond to $\Delta_- + \Delta_{-,\mathrm{off}}$, $\Delta_- - \Delta_{-,\mathrm{off}}$, and $2\Delta_+$ respectively in Eq. (11.43). Note that θ and ϕ angles are 360 degrees periodic and Z-rotation angles are 720 degree periodic.

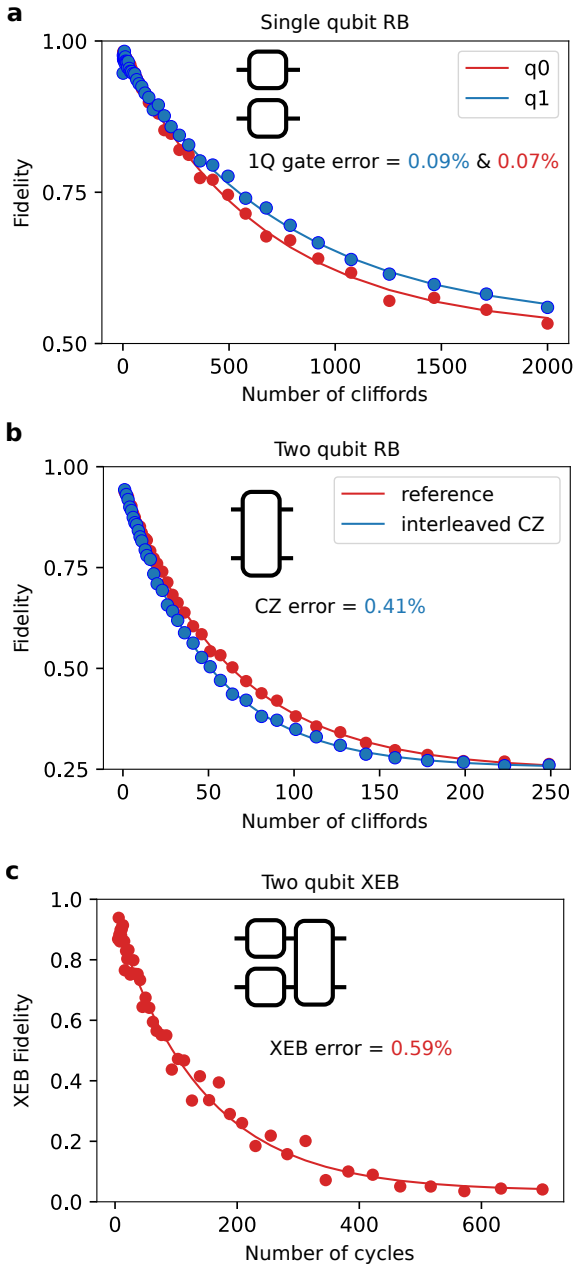


Figure S17: **Sanity check: XEB agrees with RB. a,** Single-qubit randomized benchmarking (RB) data taken separately on two qubits. **b,** Two-qubit randomized benchmarking data for a CZ on the same pair of qubits. **c,** Two-qubit cross-entropy benchmarking (XEB) on the same pair of qubits. The measured XEB error (0.59% / cycle) agrees well with the prediction from single- and two-qubit RB (0.57%). All errors are quoted as Pauli errors.

a pure state has a purity of 1. We define

$$\text{Purity} = \frac{D}{D-1}\left(\text{Tr}(\rho^2) - \frac{1}{D}\right), \tag{11.44}$$

which is consistent with what is defined in Ref. [51]. This can be understood as the squared length of the generalized Bloch vector in D dimensions (for a qubit, $D = 2$, this definition gives $\langle X\rangle^2 + \langle Y\rangle^2 + \langle Z\rangle^2$).

"Speckle" Purity Benchmarking (SPB) is the method of measuring the state purity from raw XEB data. Assuming the depolarizing-channel model with polarization parameter p, we can model the quantum state as

$$\rho = p\ |\psi\rangle\langle\psi| + (1-p)\,\frac{\mathbb{1}}{D}. \tag{11.45}$$

Here, p is the probability of a pure state $|\psi\rangle$ (which in this case is not necessarily known to us), while $1-p$ is the probability of being in the fully-decohered state ($\mathbb{1}$ is the identity operator). For the state (11.45), from the definition (11.44) it is easy to find the relation

$$\text{Purity} = p^2. \tag{11.46}$$

We will now work out how to obtain p^2 from a distribution of measured probabilities P_m of various bitstrings for a sequence, collected over many XEB sequences (Figs. S18a and S18b).

First, we note that for $p = 0$ the probabilities of all bitstrings are $1/D$, and the distribution is the δ-function located at $1/D$ (the integrated histogram is then the step-function – see Fig. S18b). In contrast, if $p = 1$, then the measured probabilities P_m follow the D-dimensional Porter-Thomas distribution [27]

$$\mathcal{P}_{\text{PT}}(P_m) = (D-1)(1-P_m)^{D-2}, \tag{11.47}$$

which has the same average $1/D$ and variance

$$\text{Var}_{\text{PT}}(P_m) = \frac{D-1}{D^2(D+1)}. \tag{11.48}$$

For the fully-decohered state all bitstrings have the same probability $1/D$, so in this case the variance of the distribution of probabilities is zero. For the state (11.45) with an arbitrary p, the histogram of probabilities P_m will be described by the distribution (11.47) shrunk towards the average $1/D$ by the factor p. Consequently, the variance of the experimental probabilities will be p^2 times the Porter-Thomas variance (11.48).

Thus, we can find p^2 by dividing the variance of experimentally measured probabilities P_m by the Porter-Thomas variance (11.48). Finally, using the relation (11.46) for the depolarization model (11.45), we can relate the variance of the experimental probabilities P_m to the average state purity

$$\text{Purity} = \text{Var}(P_m)\,\frac{D^2(D+1)}{D-1}. \tag{11.49}$$

With these convenient relations, we can directly compare the XEB fidelity $\mathcal{F}_{\text{XEB}} = p$ to $\sqrt{\text{Purity}}$ from SPB on the same scale, and check their dependence $p = p_c^m$ on the number of cycles m. Without systematic control errors, the XEB and SPB results should coincide. Experimentally, we always have control errors which lead us to incorrectly predict $|\psi\rangle$, so control errors give XEB a higher error than SPB. Thus, with a single XEB dataset we can extract the XEB error per-cycle, and the purity loss per-cycle with SPB. By subtracting these,

we are left with the control error per-cycle. Thus, with a single experiment we can error budget total error into control error and decoherence error.

These relationships can be seen experimentally in Figure S18. Amazingly, computing the speckle purity can be done with no knowledge of the specific gate sequence performed; as long as the experiment introduces sufficient randomization of the Hilbert Space, Porter-Thomas statistics apply. Practically, SPB allows us to measure the state purity from raw XEB data with exponentially fewer number of pulse sequences as compared to full state tomography. This favorable scaling allows one to extend purity measurements to larger numbers of qubits. It is important to note that an exponential number of measurements are still required to fully characterize the probability distribution for a given sequence, as in tomography, so purity measurements of the full processor are impractical.

"Per-layer" parallel XEB

To execute quantum circuits efficiently, it is helpful to run as many gates as possible in parallel. We wish to benchmark our entangling gates operating simultaneously. Resulting fidelities and optimized unitaries may differ from the isolated case, where we benchmark each pair individually, due to imperfections such as control crosstalk and stray qubit-qubit interactions. In the quantum supremacy algorithm, we partition the set of two-qubit gates into four layers, each of which can be executed in parallel. We then cycle through these layers interleaved with randomly chosen single-qubit gates (see Fig. 3a). However, it is intractable to directly use full-system XEB to benchmark our entangling gates for two reasons: we would simultaneously optimize over the unitary model parameters of every entangling gate, and the classical simulation would be exponentially expensive in system size.

We solve this problem with "per-layer" parallel XEB (see Ref. [52] for a related technique in the context of RB). Instead of alternating among the four layers of entanglers, where each qubit becomes entangled with each of its neighbors, we perform four separate experiments, one for each layer. The experiment sequences are illustrated in Fig. S19a. For each layer, we construct parallel sequences where the layer is repeated with interleaved single-qubit gates; nominally, each qubit only interacts with one other. Following each parallel XEB sequence, we measure all the qubits and extract the equivalent XEB data for each pair. Every two-qubit gate can be characterized in these four experiments, regardless of system size. The optimization and classical simulation are also efficient, as each pair can be analyzed individually.

We present experimental results of "per-layer" parallel XEB in Fig. S19b-c. In Fig. S19b, we compare the performance in the isolated and simultaneous (parallel) experiments. In both cases, the optimized XEB error is close to purity-limited. Simultaneous operation modestly increases the error, by roughly 0.003. This increase is primarily from purity error, which would arise from unintended interactions with other qubits, where coherent errors at the system scale manifest as incoherent errors when we focus on individual pairs. The unitaries we obtain in the simultaneous case differ slightly from the isolated case, which would arise from control crosstalk and unintended interactions. To quantify how these differences affect the gate error, we recalculate the error with the unitaries from the isolated optimization and the data from the simultaneous experiment, which increases the error. We also plot the distributions of the differences in unitary model parameters in Fig. S19c. The dominant change is in Δ_+, a single-qubit phase.

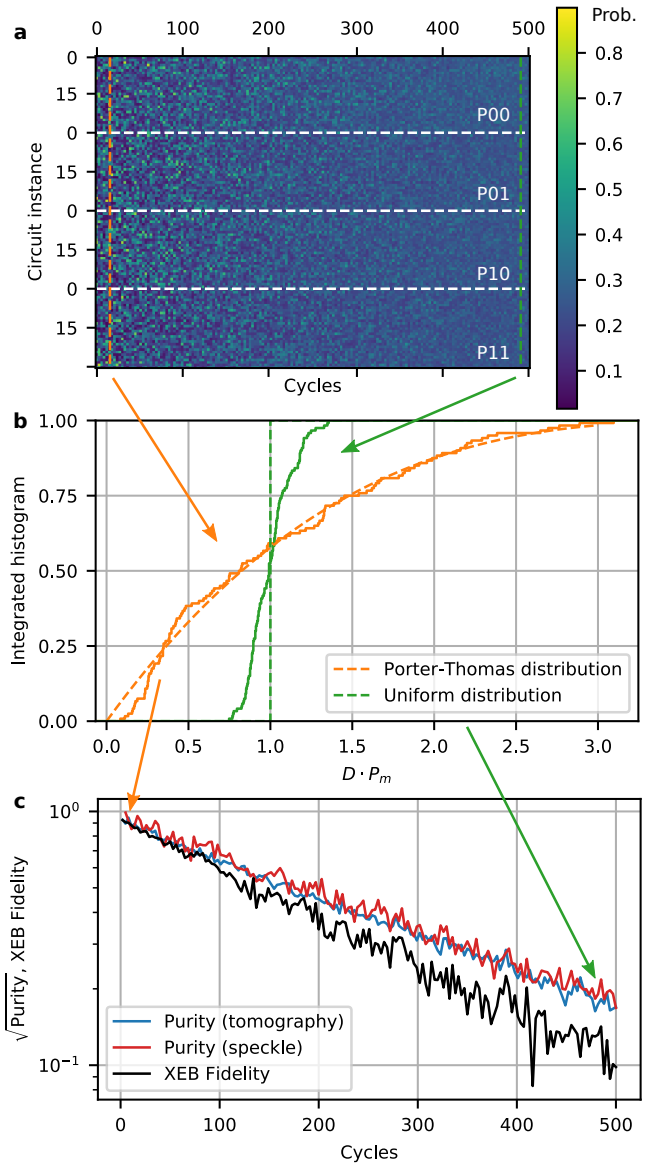


Figure S18: **"Speckle" purity extracted from XEB. a,** Measured probabilities from XEB for a two-qubit system and 30 random circuits. Raw probabilities show a speckle pattern at low cycles (orange dashed) over circuit instance and probabilities ($|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$). The speckle contrast decreases with cycles and thus decoherence (green dashed). **b,** Integrated histogram (cumulative distribution) of probabilities. The x-axis is scaled by the dimension $D = 2^2$, so the uniform distribution is a step function at 1.0. At low cycles, the distribution is well-described by Porter-Thomas, and at high cycles, the distribution approaches the uniform distribution. **c,** We can directly relate the variance of the distribution to the average state purity. We fit an exponential to the square root of Purity. We compare this purity-derived number per-cycle= 0.00276 to a similar number per-cycle=0.00282 derived from tomographic measure of purity, and see good agreement. The error of XEB, which also includes control errors, is slightly higher at error per-cycle=0.00349.

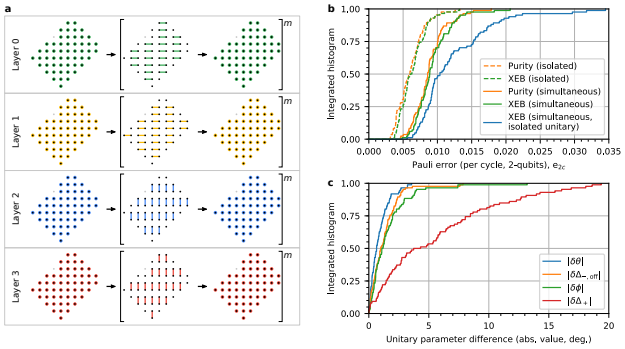


Figure S19: **Parallel XEB. a,** Schematics of four device-wide sequences, one for each entangler layer. Black points are active qubits, colored circles are single-qubit gates, and colored lines are two-qubit gates. We cycle between single- and two-qubit gates m times. Compare to Fig. 3a, main text, where the layers are interleaved. **b,** Integrated histograms of Pauli error e_{2c} (see Fig. 2a, main text). These include isolated results, where each entangler is measured in its own experiment, and simultaneous (parallel) results. Purity is "speckle" purity. **c,** Difference, δ, in unitary model parameters (Eq. 11.43) between the unitaries obtained in the isolated and simultaneous experiments. $\delta\Delta_-$ is not plotted because it has a negligible effect on the unitary when $\theta \approx 90$ degrees.

11.6.4 Grid readout calibration

Choosing qubit frequencies for readout

The algorithm described in Section 11.6.2 generally chooses qubit idling frequencies which are far detuned from the resonator to optimize for dephasing. However, these idling frequencies are not optimal for performing readout. To address this problem, we dynamically bias each qubit to a different frequency during the readout phase of the experiment. The qubit frequencies during readout are shown in Fig. S20 (compare to Fig. S13).

To choose the qubit frequencies for readout, we first measure readout fidelity as a function of qubit frequency and resonator drive frequency at a fixed resonator drive power, in each of the isolated single qubit configurations. This scan captures errors due to both non-optimal detuning between the qubit and resonator, as well as regions with low T_1 values due to TLSs. We then use the data for each qubit and a few constraints to optimize the placement of the qubit frequencies during readout, using the same optimization technique that was described in Section 11.6.2. We describe two of the important constraints and related error reduction techniques below.

First, because the coupling between qubits relies on a dispersive interaction with the coupler, the coupling would no longer be off when the qubits were detuned by a significant amount from their idling positions. Thus, we impose a constraint that qubits should not be placed near resonance during readout. Nevertheless, we found that for some pairs of qubits, we had to dynamically bias the coupler during readout to avoid any swapping transitions between the qubits during readout. This readout coupler bias is found by sweeping the coupler bias and maximizing the two-qubit readout fidelity.

Second, the pattern of the bare resonator frequencies on the chip as shown in Fig. S20 led to an unexpected problem. Pairs of readout resonators which were coupled to neighboring qubits and were also within a few MHz in frequency space were found to have non-negligible coupling. This coupling was strong enough to mediate swapping of photons from one resonator to the other. The pairs of qubits with similar resonator frequencies were all located in a diagonal chain bisecting the qubit grid, as shown by the red outline in Fig. S20. To mitigate this problem, we arrange the qubit frequencies for these qubits so that the resonator eigenfrequencies are as

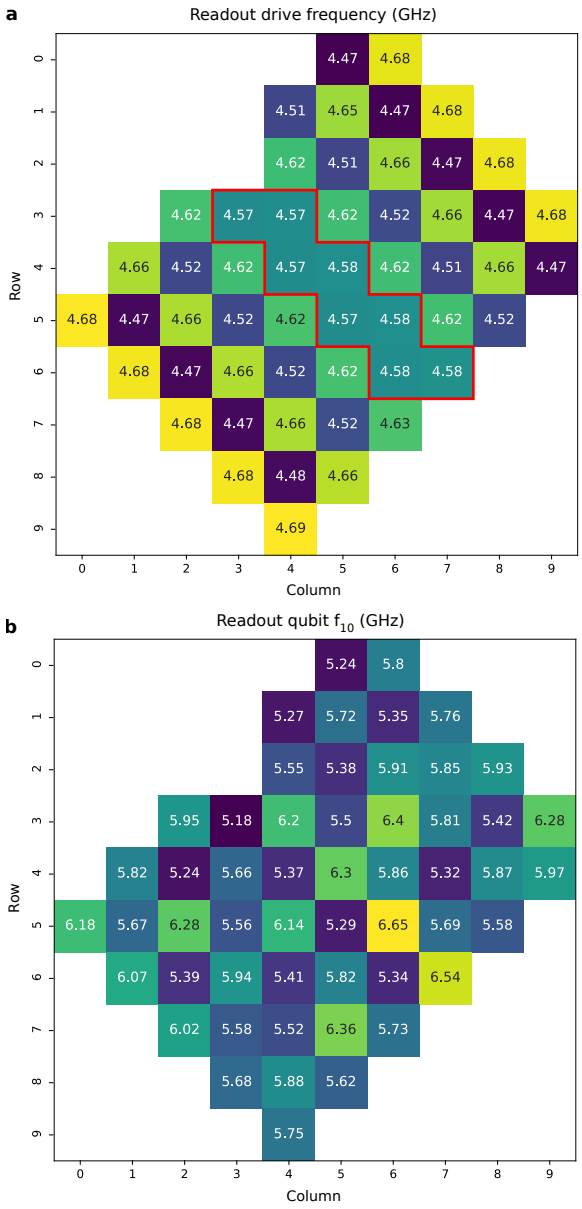


Figure S20: **a,** Drive frequencies for the readout resonators for each qubit. The red outline shows the area where we had to perform correlated discrimination because of unwanted cross-couplings between the resonators. **b,** Qubit frequencies during readout, found using a frequency optimization procedure.

far apart as possible. The resulting spectral separation is not quite enough to eliminate all deleterious effects, so in addition, we use correlated discrimination on the eight of the qubits in this chain. In other words, we use the results of all eight detector values to determine which one of $2^8 = 256$ states the eight qubits were in. All other qubits in the grid are discriminated as isolated qubits.

Single qubit calibration

After placing the qubit frequencies for readout, we calibrate and fine tune the readout parameters for each qubit. For each qubit, we use a 1 μs drive pulse and a 1 μs demodulation window. We summarize the procedure for choosing the remaining parameters as follows:

- Choose the resonator drive frequency to maximize the separation between measurements performed with the qubit in either $|0\rangle$ and $|1\rangle$ [16].
- Choose the resonator drive power to hit a target separation between $|0\rangle$ and $|1\rangle$, so that the error due to this separation is below a 0.3% threshold. We do not choose the readout power to maximize the separation as doing so would saturate our amplifiers, and cause unwanted transitions of the qubit state [53, 22, 54, 17].
- Find the optimal demodulation weight function by measuring the average detector voltage as a function of time during the course of the readout pulse [16, 21].
- Finally, choose the discrimination line between the measurement results for $|0\rangle$ and $|1\rangle$, except as noted in the previous section where we need to apply correlated discrimination.

After completing these calibrations, we check each qubit's readout fidelity by preparing either $|0\rangle$ or $|1\rangle$ and reading the qubit out. We define the identification error to be the probability that the qubit was not measured in the state we intended to prepare. We achieve 0.97% median identification error for the $|0\rangle$ state, and 4.5% for $|1\rangle$, when each qubit is measured in isolation. The full distribution is shown in dashed lines in Fig. S21a. We conjecture that the error in $|0\rangle$ is due to thermal excitation during preparation or measurement, and that the error in $|1\rangle$ is due to energy relaxation during readout.

Characterizing multi-qubit readout

To assess the fidelity of multi-qubit readout, we prepare and measure 150 random classical bitstring states with 53 qubits, with 3000 trials per state. We find that 13.6% of all trials successfully identified the prepared state. We can decompose this overall fidelity in two ways. First, we plot in solid lines in Fig. S21 the errors for each qubit during simultaneous readout, averaged over the 150 random bitstrings. We find that the median errors increase from 0.97% for $|0\rangle$ and 4.5% for $|1\rangle$ in isolation, to 1.8% and 5.1% for simultaneous readout. We do not yet understand the root causes of this increase in error. In addition, we show in Fig. S21 the distribution of errors among the multiqubit results. We see that the most likely error is one lost excitation in the measured state.

11.6.5 Summary of system parameters

Table 12 reports aggregate values for qubit and pair parameters in our processor. A complete table of single-qubit parameter values by qubit is available in supporting online materials, Ref. [55], and illustrated in Figs. S22 through S24. Single-qubit metrics represent a sample size of 53. Two-qubit metrics represent 86 pairs.

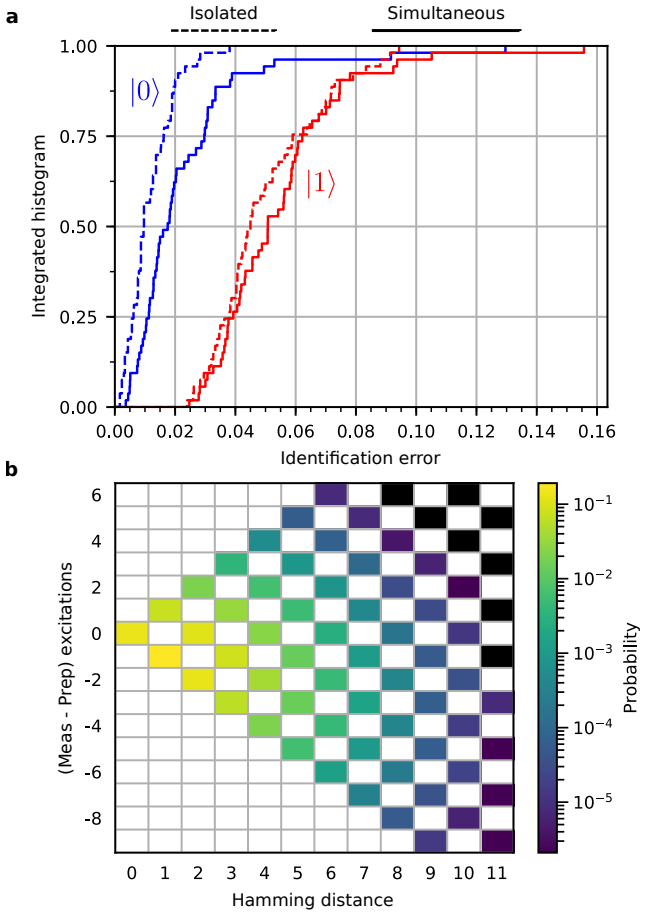


Figure S21: **Readout errors. a,** Histogram of readout errors for each qubit when prepared in $|0\rangle$ or $|1\rangle$, and readout in isolation or simultaneously. **b,** Distribution of errors in multi-qubit readout. The x-axis Hamming distance is the number of bits that are different between measured and prepared states, while the y-axis is the difference in the number of 1's in the states. For example, if we prepare $|011\rangle$ and measure $|101\rangle$, the Hamming distance is 2 and the difference in the number of excitations is 0.

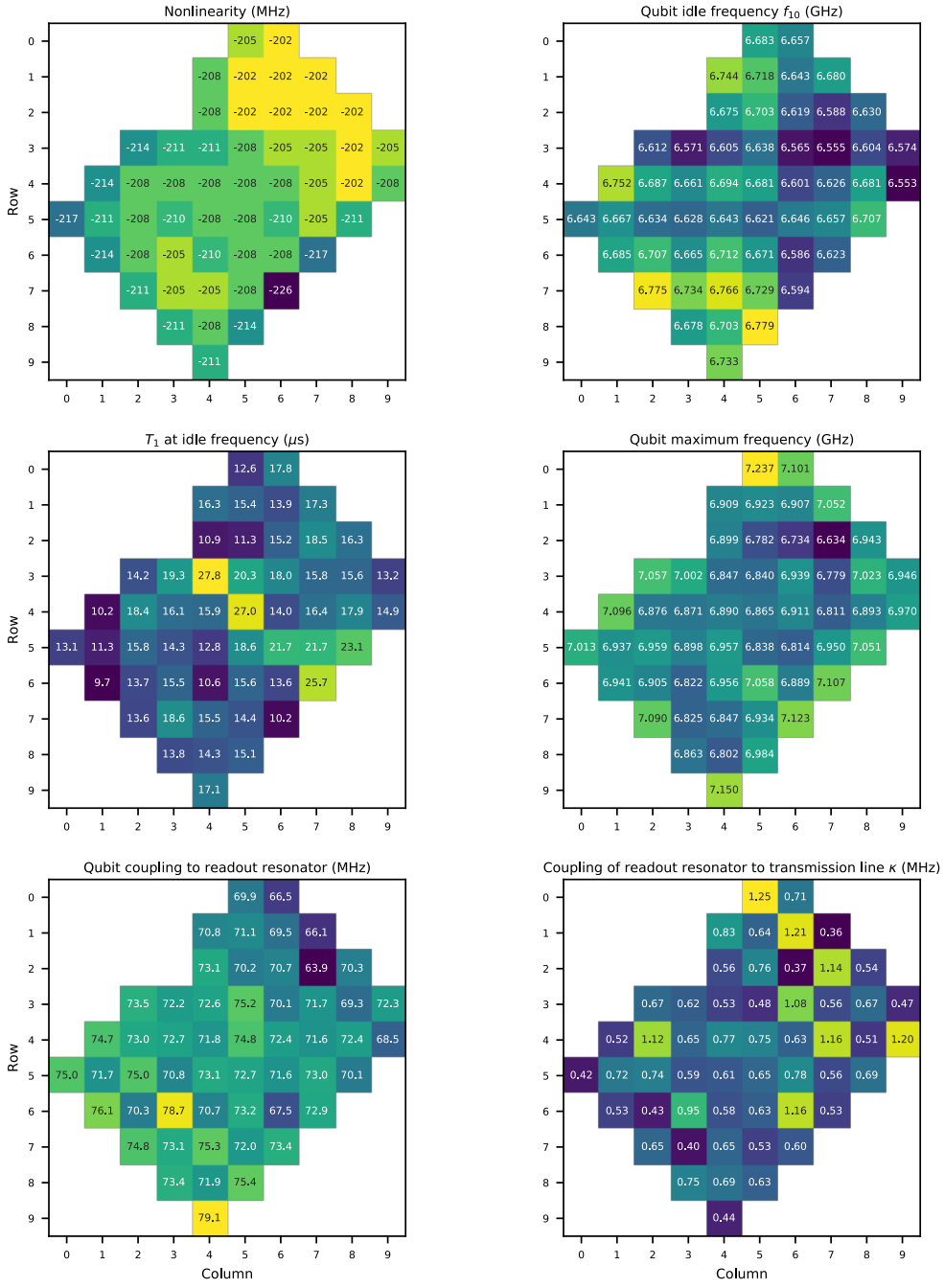


Figure S22: Typical distribution of single-qubit parameters over the Sycamore processor.

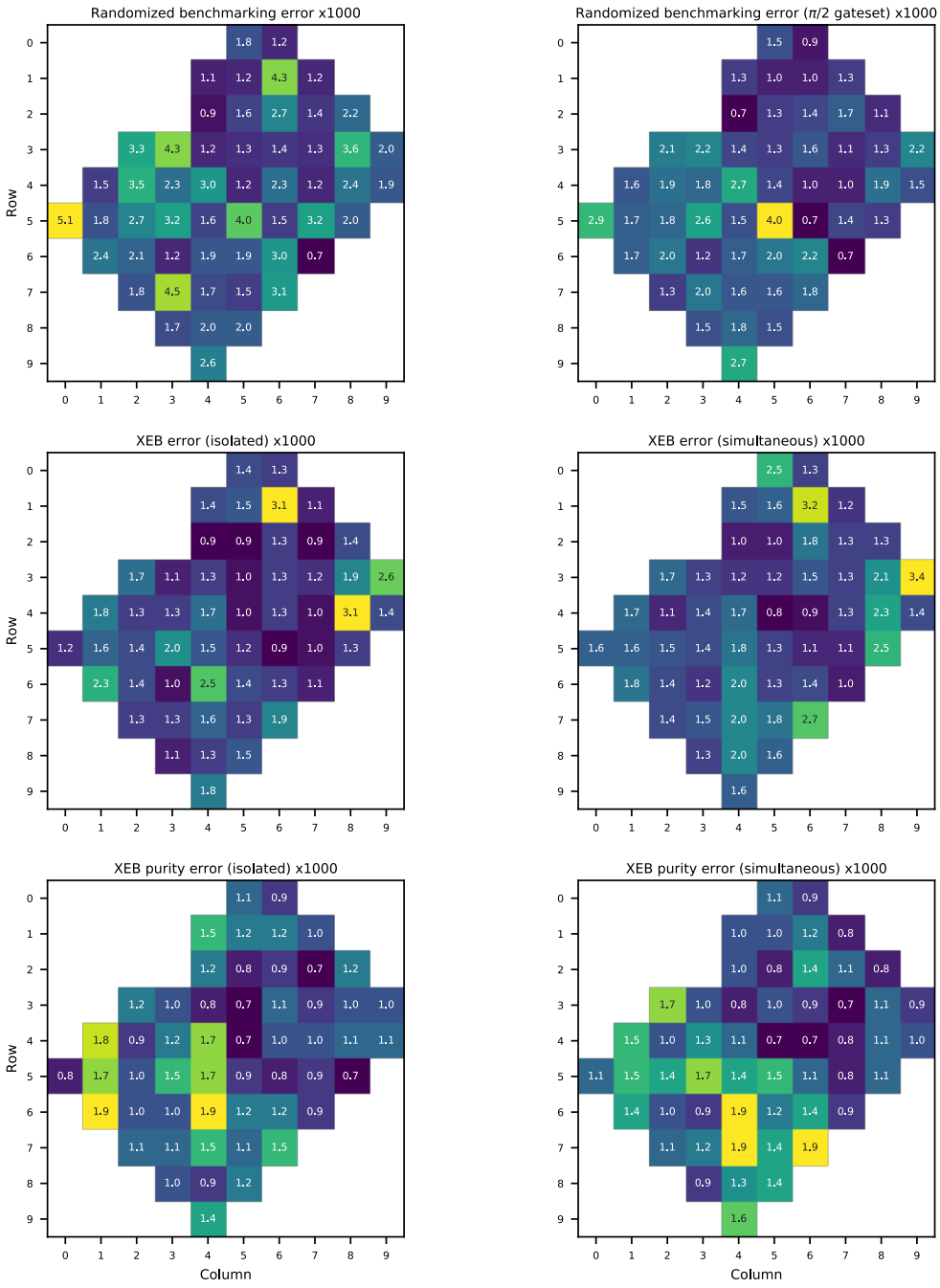


Figure S23: Typical distribution of single-qubit gate benchmarking errors over the Sycamore processor, for both isolated and simultaneous operation.

Table 12: Aggregate system parameters

Parameter	Median	Mean	Stdev.	Units	Figu
Qubit maximum frequency	6.924	6.933	0.114	GHz	S
Qubit idle frequency	6.661	6.660	0.057	GHz	S
Qubit frequency at readout	5.750	5.766	0.360	GHz	S
Readout drive frequency	4.618	4.588	0.076	GHz	S
Qubit anharmonicity	-208.0	-208.0	4.7	MHz	S
Resonator linewidth $\kappa/2\pi$	0.64	0.69	0.23	MHz	S
Qubit-resonator coupling $g/2\pi$	72.3	72.1	2.8	MHz	S
T_1 at Idle Frequency	15.54	16.04	4.00	μs	S
Readout error $\|0\rangle$ isolated / simultaneous	0.97 / 1.8	1.2 / 2.3	0.8 / 2.1	%	S
Readout error $\|1\rangle$ isolated / simultaneous	4.5 / 5.1	5.0 / 5.5	1.8 / 2.2	%	S
1Q RB[1] e_1	0.19	0.22	0.10	%	S
1Q RB[1] e_1 ($\pi/2$ gateset)	0.15	0.16	0.06	%	S
1Q RB[1] tomographic e_1 purity	0.14	0.15	0.04	%	S
1Q XEB e_1 isolated / simultaneous	0.13 / 0.14	0.15 / 0.16	0.05 / 0.05	%	3a (main) S
1Q XEB e_1 purity isolated / simultaneous	0.11 / 0.11	0.11 / 0.12	0.03 / 0.03	%	S
2Q XEB e_2 isolated / simultaneous	0.30 / 0.60	0.36 / 0.62	0.17 / 0.24	%	3a (mai
2Q XEB e_{2c} isolated / simultaneous	0.64 / 0.89	0.65 / 0.93	0.20 / 0.26	%	3a (mai
2Q XEB e_{2c} purity isolated / simultaneous	0.59 / 0.86	0.62 / 0.89	0.20 / 0.24	%	S
Measurement e_m isolated / simultaneous	2.83 / 3.50	3.05 / 3.77	1.09 / 1.61	%	3a (mai

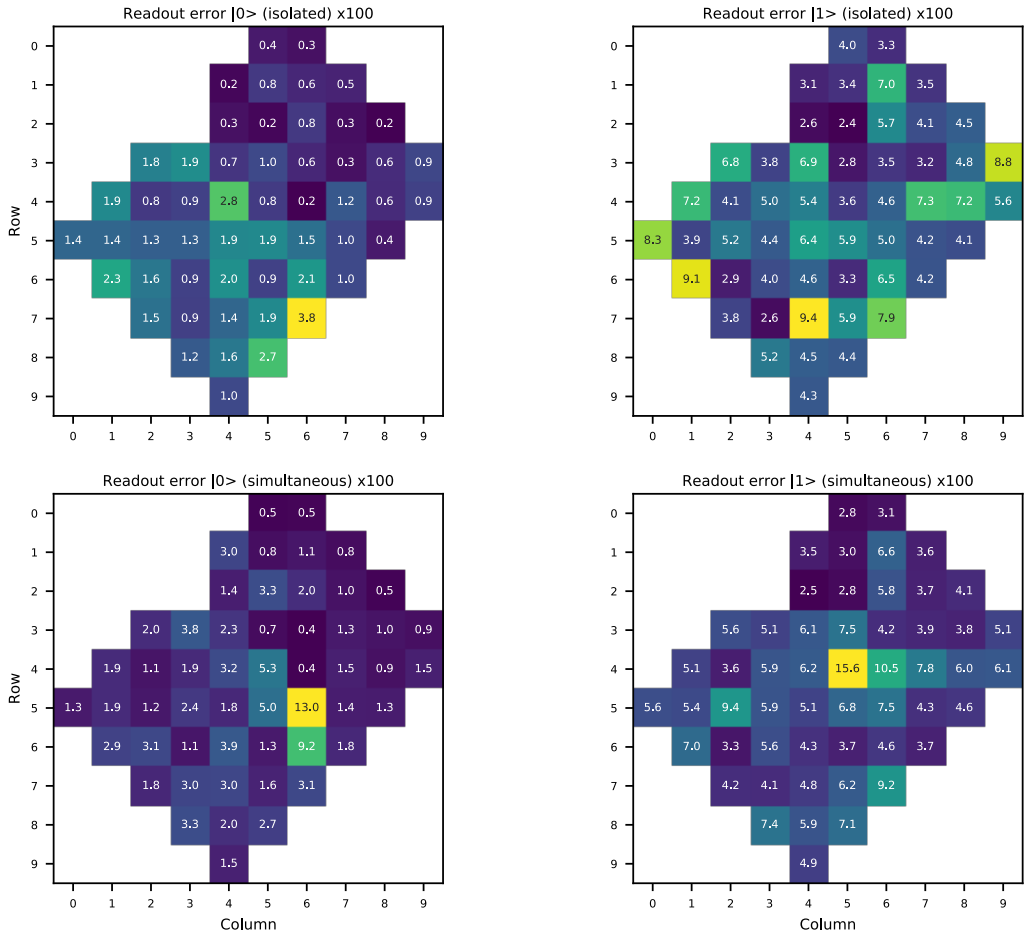


Figure S24: Typical distribution of readout errors over the Sycamore processor, for both isolated and simultaneous operation.

11.7 Quantum circuits

11.7.1 Background

We sample the output of random quantum circuits (RQCs) with two use cases in mind: performing a computational task beyond the reach of state-of-the-art supercomputers (quantum supremacy); and estimating the experimental fidelity (performance evaluation).

In order for the RQCs to cover both use cases, we define a circuit family with a varying number of qubits n and cycles m. Our quantum supremacy demonstration uses RQCs with a large number of qubits $n = 53$ and high depth $m = 20$. Large number of qubits hinders wave function (Schrödinger) simulation and high depth impedes tensor network (Feynman) simulation (see Sec. 11.10.2). We find that the most competitive classical simulator for our hardest RQCs is the Schrödinger-Feynman algorithm (SFA, see Sec. 11.10.1) which copes well with high depth circuits on many qubits.

SFA takes as input an n-qubit quantum circuit and a *cut* which divides $n = n_1 + n_2$ qubits into two contiguous partitions with n_1 and n_2 qubits. The algorithm computes the output state as the sum over simulation paths formed as the product of the terms of the Schmidt decomposition of all cross-partition gates. By the distributive law there are r^g such simulation paths for a circuit with g cross-partition gates of Schmidt rank r. Consequently, the algorithm achieves runtime proportional to $(2^{n_1} + 2^{n_2})r^g$. Circuit cuts with n_1, n_2 and g that make the simulation task tractable are called *promising cuts*. The most promising cut for our largest RQCs runs parallel to the shorter axis of the device starting in the vicinity of the broken qubit. The sum over the simulation paths can be interpreted as tensor contraction. In this view, the r^g factor can be thought of as the *bond dimension* associated with the circuit partitioning, i.e. the cardinality of the index set ranged over in the contraction corresponding to all cross-partition gates. SFA is described in more detail in [38] and section 11.10.

11.7.2 Overview and technical requirements

The two use cases for our RQCs give rise to a tension in technical requirements at the heart of quantum supremacy. On the one hand, supremacy RQC sampling should by definition be prohibitively hard to simulate classically. On the other hand, performance evaluation entails classical simulation of the RQCs. To resolve the conflict, we note that the fidelity of a RQC experiment depends primarily on the number and quality of the gates. By contrast, the simulation cost is highly sensitive to minor perturbations in the circuit. Consequently, experiment fidelity for RQCs that cannot be simulated directly may be approximated from the experiment fidelity of similar RQCs obtained as the result of transformations that reduce simulation cost without significantly affecting experiment fidelity (see Section 11.7.7).

Performance evaluation using XEB provides another design consideration. The procedure requires knowledge of the cross-entropy of the theoretical output distribution of the circuit. An analytical expression for this quantity has been derived in [27] for circuits whose measurement probabilities approach the Porter-Thomas distribution. We find that our RQCs satisfy this assumption when the circuit depth is larger than 12, see Fig. **??**a. Note that high circuit depth also increases the cost of classical simulation.

11.7.3 Circuit structure

A RQC with n qubits generally utilizes qubits 1 through n in the qubit order shown in Fig. S27 with small deviations from this default qubit ordering in some circuits. The qubit order has been chosen to ensure that for most RQCs with fewer than 51 qubits, there is a partitioning of the qubits into two similarly sized blocks connected by only five couplers. The

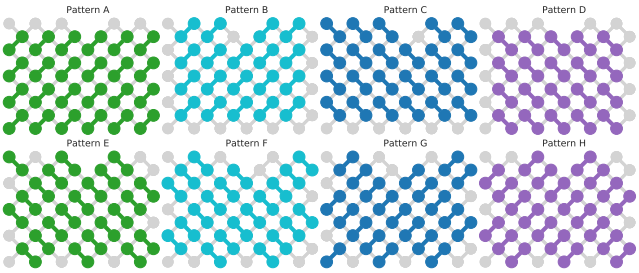


Figure S25: **Coupler activation patterns.** Coupler activation pattern determines which qubits are allowed to interact simultaneously in a cycle. Quantum supremacy RQCs utilize the staggered patterns shown in the top row in the sequence ABCDCDAB, repeated in subsequent cycles. Performance evaluation RQCs employ the patterns shown in the bottom row in the sequence EFGH, likewise repeated in subsequent cycles. The former sequence makes SFA simulation harder by facilitating prompt transfer of entanglement created at promising circuit cuts into the bulk of each circuit partition.

next larger RQC, with 51 qubits, has seven couplers along the most promising circuit cut. Since the cost of SFA grows exponentially in the number of gates across the partitions our circuit geometry leads to a steep increase in the simulation cost of 51-qubit RQCs relative to the circuits with fewer qubits. This creates a sizeable gap in the computational hardness between most of our evaluation circuits and the quantum supremacy circuits ($n = 53$).

In the time dimension, each RQC is a series of m full cycles and one half cycle followed by measurement of all qubits. Every full cycle consists of two steps. In the first step, a single-qubit gate is applied to every qubit. In the second step, two-qubit gates are applied to pairs of qubits. Different qubit pairs are allowed to interact in different cycles. Specifically, in the supremacy RQCs we loop through the direct neighbors of every qubit over the eight-cycle sequence ABCDCDAB and in the evaluation RQCs we use the four-cycle sequence EFGH where A, B, ..., H are coupler activation patterns shown in Fig. S25. The sequence is repeated in subsequent cycles. The cost of SFA simulation is highly sensitive to the specific sequence employed in a circuit, see 11.7.7. Border qubits have fewer than four neighbors and no gate is applied to them in some cycles. The half cycle preceding the measurement consists of the single-qubit gates only. The overall structure of our RQCs is shown in Fig. 3 of the main paper [1].

11.7.4 Randomness

Single-qubit gates in every cycle are chosen randomly using a pseudo-random number generator (PRNG). The generator is initialized with a seed s which is the third parameter for our family of RQCs. The single-qubit gate applied to a particular qubit in a given cycle depends only on s. Consequently, two RQCs with the same s apply the same single-qubit gate to a given qubit in a given cycle as long as the qubit and the cycle belong in both RQCs as determined by their size n and depth m parameters.

Conversely, the choice of single-qubit gates is the sole property of our RQCs that depends on s. In particular, the same two-qubit gate is applied to a given qubit pair in a given cycle by all RQCs that contain the pair and the cycle.

11.7.5 Quantum gates

In our experiment, we configure three single-qubit gates. Each one is a $\pi/2$-rotation around an axis lying on the equator of the Bloch sphere. Up to global phase, the gates are

$$X^{1/2} \equiv R_X(\pi/2) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & -i \\ -i & 1 \end{bmatrix}, \tag{11.50}$$

$$Y^{1/2} \equiv R_Y(\pi/2) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}, \tag{11.51}$$

$$W^{1/2} \equiv R_{X+Y}(\pi/2) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & -\sqrt{i} \\ \sqrt{-i} & 1 \end{bmatrix} \tag{11.52}$$

where $W = (X + Y)/\sqrt{2}$ and $\sqrt{\pm i}$ denotes the principal value of the square root. The first two belong to the single-qubit Clifford group, while $W^{1/2}$ is a non-Clifford gate. Single-qubit gates in the first cycle are chosen independently and uniformly at random from the set of the three gates above. In subsequent cycles, each single-qubit gate is chosen independently and uniformly at random from among the gates above except the gate applied to the qubit in the preceding cycle. This prevents simplifications of some simulation paths in SFA. Consequently, there are $3^n 2^{nm}$ possible random choices for a RQC with n qubits and m cycles.

Two-qubit gates in our RQCs are not randomized, but are determined by qubit pair and cycle number. The gates preserve the number of ground and excited states of the qubits which gives their matrices block diagonal structure with 1×1, 2×2 and 1×1 blocks. Therefore, up to global phase they belong to $U(1) \oplus U(2) \oplus U(1)/U(1)$ and thus can be described by five real parameters (see Fig. S16, and Eq. 11.43). Each gate in this family can be decomposed into four Z-rotations described by three free parameters and the two-parameter fermionic simulation gate

$$\mathrm{fSim}(\theta, \phi) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos(\theta) & -i\sin(\theta) & 0 \\ 0 & -i\sin(\theta) & \cos(\theta) & 0 \\ 0 & 0 & 0 & e^{-i\phi} \end{bmatrix} \tag{11.53}$$

which is the product of a fractional iSWAP and controlled phase gate (see Fig. S14b).

In our experiment, we tune up the two-qubit gates close to $\theta \approx \pi/2$ and $\phi \approx \pi/6$ radians and then infer more accurate values of all five parameters for each qubit pair using XEB. Consequently, all five parameters of the two-qubit gate depend on the qubit pair. While inferred unitaries are suitable for RQC sampling, future applications of the Sycamore processor, for example, in quantum chemistry, will require precise targeting of the entangling parameters [49, 56]. The three parameters which control the Z-rotations implicit in the two-qubit gates can be canceled out with active Z-rotations turning an arbitrary five-parameter gate into pure $\mathrm{fSim}(\theta, \phi)$. In our RQCs, we have decided not to apply such correction gates. This choice affords us greater number of interactions within the available circuit depth budget and introduces additional implicit non-Clifford single-qubit gates into the RQCs.

The Z-rotations have two origins. First, they capture the phase shifts due to qubit frequency excursions during the two-qubit gate. Second, they account for phase changes due to different idle frequencies of the interacting qubits. The latter introduces dependency of the three parameters defining the Z-rotations on the time at which the gate is applied. By contrast, for a given qubit pair θ and ϕ do not depend on the cycle.

The $\mathrm{fSim}(\pi/2, \pi/6)$ gate is the product of a non-Clifford controlled phase gate and an iSWAP which is a two-qubit Clifford gate.

11.7.6 Programmability and universality

Programmability of Sycamore rests on our ability to tune up a variety of gate sets including sets that are universal for quantum computation. For example, the set of gates employed in our quantum supremacy demonstration is universal, as we show in this section.

The proof consists of two parts. First, we show that the CZ gate can be obtained as a composition of two fSim gates and single-qubit rotations. Second, we outline how the well-known proof that the H and T gates are universal for SU(2) [57] can be adapted for $X^{1/2}$ and $W^{1/2}$. The conclusion follows from the fact that the gate set consisting of the CZ gate and SU(2) is universal [58].

Decomposition of CZ into fSim gates

Here, we show how to decompose a controlled-phase gate into two fSim gates and several single-qubit gates. The fSim gate is native to our hardware and can be decomposed into

$$\mathrm{fSim}(\theta,\phi) = e^{-i\theta(X\otimes X+Y\otimes Y)/2}\, e^{-i\phi(I-Z)\otimes(I-Z)/4}\,, \tag{11.54}$$

where the iSWAP angle $\theta \simeq \pi/2$ and the controlled-phase angle $\phi \simeq \pi/6$. The controlled-phase part can be further decomposed into

$$\begin{aligned} &e^{-i\phi(I-Z)\otimes(I-Z)/4} \\ &\quad = e^{-i\phi/4}\, e^{i\phi(Z\otimes I+I\otimes Z)/4}\, e^{-i\phi Z\otimes Z/4}\,. \end{aligned} \tag{11.55}$$

To simplify notations, we introduce the two-qubit gate

$$\begin{aligned} \Upsilon(\theta,\phi) &= e^{-i\theta(X\otimes X+Y\otimes Y)/2}\, e^{-i\phi Z\otimes Z/4} \\ &= e^{i\phi/4}\, e^{-i\phi(Z\otimes I+I\otimes Z)/4}\, \mathrm{fSim}(\theta,\phi)\,, \end{aligned} \tag{11.56}$$

which is equivalent to the fSim gate up to single-qubit Z rotations. The sign of θ in $\Upsilon(\theta,\phi)$ can be changed by the single-qubit transformation,

$$Z_1\, \Upsilon(\theta,\phi)\, Z_1 = \Upsilon(-\theta,\phi)\,, \tag{11.57}$$

where $Z_1 = Z\otimes I$ ($Z_2 = I\otimes Z$ works equally well).

Multiplying two Υ gates with opposite values of θ on both sides the operator $X_1 = X\otimes I$, we have

$$\begin{aligned} \Upsilon(-\theta,\phi)\, X_1\, \Upsilon(\theta,\phi) &= e^{i\theta Y\otimes Y/2}\, X_1\, e^{-i\theta Y\otimes Y/2} \\ &= \cos\theta\, X_1 + \sin\theta\, Z\otimes Y\,. \end{aligned} \tag{11.58}$$

With the identity (11.58), we have

$$\begin{aligned} \Upsilon(-\theta,\phi)\, e^{i\alpha X_1}\, \Upsilon(\theta,\phi) &= \cos\alpha\left(\cos\frac{\phi}{2}\, I\otimes I - i\sin\frac{\phi}{2}\, Z\otimes Z\right) + i\sin\alpha\left(\cos\theta\, X\otimes I + \sin\theta\, Z\otimes Y\right) \\ &= \left(\cos\alpha\cos\frac{\phi}{2}\, I + i\sin\alpha\cos\theta\, X\right)\otimes I - iZ\otimes\left(\cos\alpha\sin\frac{\phi}{2}\, Z - \sin\alpha\sin\theta\, Y\right), \end{aligned} \tag{11.59}$$

where $0 \le \alpha \le \pi/2$ is to be determined. We introduce the Schmidt operators

$$\Gamma_1(\alpha) = \cos\alpha\cos(\phi/2)\, I + i\sin\alpha\cos\theta\, X\,, \tag{11.60}$$

$$\Gamma_2(\alpha) = \cos\alpha\sin(\phi/2)\, Z - \sin\alpha\sin\theta\, Y\,, \tag{11.61}$$

and the unitary (11.59) takes the simple form

$$\Upsilon(-\theta,\phi)\, e^{i\alpha X_1}\, \Upsilon(\theta,\phi) = \Gamma_1\otimes I - iZ\otimes\Gamma_2\,. \tag{11.62}$$

The Schmidt rank of this unitary is two. Therefore, it is equivalent to a controlled-phase gate (also with Schmidt rank two) up to some single-qubit unitaries. The two non-zero Schmidt coefficients of the unitary (11.59) are equal to the operator norms of $\Gamma_{1,2}$.

The target controlled-phase gate that we want to decompose into the fSim gate is

$$\mathrm{diag}\big(1,\, 1,\, 1,\, e^{-i\delta}\big) = e^{-i\delta(I-Z)\otimes(I-Z)/4}\,, \tag{11.63}$$

where $0 \le \delta \le 2\pi$. It has two non-zero Schmidt coefficients $\cos(\delta/4)$ and $\sin(\delta/4)$. For example, we set the operator norm of Γ_2 to be equal to the second Schmidt coefficient of the target unitary

$$\begin{aligned} \big|\Gamma_2(\alpha)\big| &= \sqrt{\big(\cos\alpha\sin(\phi/2)\big)^2 + \big(\sin\alpha\sin\theta\big)^2} \\ &= \sin(\delta/4)\,, \end{aligned} \tag{11.64}$$

and the parameter α can be determined

$$\sin\alpha = \sqrt{\frac{\sin(\delta/4)^2 - \sin(\phi/2)^2}{\sin(\theta)^2 - \sin(\phi/2)^2}}\,. \tag{11.65}$$

This equation has a solution if and only if one of the following two conditions is satisfied

$$|\sin\theta| \le \sin(\delta/4) \le |\sin(\phi/2)|\,, \tag{11.66}$$

$$|\sin(\phi/2)| \le \sin(\delta/4) \le |\sin\theta|\,. \tag{11.67}$$

A large set of controlled-phase gates can be implemented with the typical values of θ and ϕ of the fSim gate, except for those that are very close to the identity.

To fix the local basis of the first qubit in Eq. (11.59), we introduce two X rotations of the same angle

$$e^{-i\xi X/2}\,\Gamma_1(\alpha)\,e^{-i\xi X/2} = \cos(\delta/4)\,I\,, \tag{11.68}$$

$$e^{-i\xi X/2}\,Z\,e^{-i\xi X/2} = Z\,, \tag{11.69}$$

where the angle ξ is

$$\xi = \arctan\left(\frac{\tan\alpha\cos\theta}{\cos(\phi/2)}\right) + \frac{\pi}{2}\Big(1 - \mathrm{sgn}\big(\cos(\phi/2)\big)\Big)\,. \tag{11.70}$$

To fix the local basis of the second qubit in Eq. (11.59), we introduce two X rotations of opposite angles

$$e^{i\eta X/2}\,\Gamma_2(\alpha)\,e^{-i\eta X/2} = \sin(\delta/4)\,Z\,, \tag{11.71}$$

where the angle η is

$$\eta = \arctan\left(\frac{\tan\alpha\sin\theta}{\sin(\phi/2)}\right) + \frac{\pi}{2}\Big(1 - \mathrm{sgn}\big(\sin(\phi/2)\big)\Big)\,. \tag{11.72}$$

Applying these local X rotations before and after the gate sequence in Eq. (11.59), we have

$$\begin{aligned} &e^{-i(\xi X_1 - \eta X_2)/2}\,\Upsilon(-\theta,\phi)\,e^{i\alpha X_1}\,\Upsilon(\theta,\phi)\,e^{-i(\xi X_1+\eta X_2)/2} \\ &\quad = \cos(\delta/4)\,I\otimes I - i\sin(\delta/4)\,Z\otimes Z\,, \end{aligned} \tag{11.73}$$

which is the desired controlled-phase gate up to some single-qubit Z rotations.

The target controlled-phase gate equals to the CZ gate for $\delta = \pi$. We numerically checked that the decomposition (11.73) yields the CZ gate for all 86 fSim gates (with different values of θ and ϕ) in our device.

Universality for SU(2)

Here, we show how the argument for the well-known result that the H and T gates are universal for SU(2) [57] can be adapted for the $X^{1/2}$ and $W^{1/2}$ gates. At the core of the argument lies the observation that $T \equiv R_Z(\pi/4)$ followed by $HTH \equiv R_X(\pi/4)$ is a single-qubit rotation by angle α which is an irrational multiple of π. Specifically, α is such that

$$\cos\frac{\alpha}{2} = \cos^2\frac{\pi}{8} = \frac{1}{2}\left(1 + \frac{1}{\sqrt{2}}\right). \tag{11.74}$$

By Theorem B.1 in Appendix B of [57], α/π is irrational because the monic minimal polynomial with rational coefficients of $e^{i\alpha}$

$$x^4 + x^3 + \frac{1}{4}x^2 + x + 1 \tag{11.75}$$

is not cyclotomic (since not all its coefficients are integers).

Similarly, $W^{1/2} \equiv R_{X+Y}(\pi/2)$ followed by $X^{1/2} \equiv R_X(\pi/2)$ is a single-qubit rotation by angle β such that

$$\cos\frac{\beta}{2} = \cos^2\frac{\pi}{4} - \frac{1}{\sqrt{2}}\sin^2\frac{\pi}{4} = \frac{1}{2}\left(1 - \frac{1}{\sqrt{2}}\right). \tag{11.76}$$

The monic minimal polynomial with rational coefficients of $e^{i\beta}$ is (11.75), the same as that of $e^{i\alpha}$. Therefore, β is also an irrational multiple of π. The rest of the universality argument for H and T also applies in the case of $X^{1/2}$ and $W^{1/2}$.

11.7.7 Circuit variants

Since XEB entails classical simulation, it is hard or impossible to use it to estimate experimental fidelity of circuits which are hard or impossible to simulate classically. As described above, we designed our RQCs to ensure that an effective partitioning for SFA exists for circuits with fewer than 51 qubits. This gives rise to a significant gap in the cost of classical simulation between quantum supremacy circuits and most of our performance evaluation circuits. This gap facilitates performance evaluation of the Sycamore processor near the quantum supremacy frontier. In practice, however, we would like greater control over the simulation hardness, for two reasons. First, performance evaluation is still very costly for large n approaching the supremacy frontier. Second, we would like to be able to estimate the fidelity of supremacy RQCs more directly, even though classical simulation of this case is unfeasible by definition.

In order to achieve more fine-grained control over the cost of classical simulation of our RQCs, we exploit the fact that the experimental fidelity depends primarily on the number and quality of the gates while the simulation cost is highly sensitive to the structure of the quantum circuit. Therefore, we approximate the experimental fidelity of RQCs which are hard or impossible to simulate from the fidelity of similar RQCs obtained as the result of transformations that reduce simulation cost without significantly affecting experimental fidelity.

We employ two such transformations. Each decreases simulation cost by reducing the bond dimension of promising circuit cuts. The first one removes some or all cross-partition gates. We say that the removed gates have been *elided* and term the transformation *gate elision*. The second transformation changes the sequence of coupler activation patterns shown in Fig. S25 to enable the formation of *wedges* which reduce the bond dimension by slowing the spread of entanglement generated at the circuit cut.

The two transformations complete the description of RQCs used in our experiment. Consequently, each RQC is uniquely determined by five parameters: number of qubits n, number of cycles m, PRNG seed s, number of elided gates and the sequence of coupler activation patterns.

Circuit variant	Gates elided	Sequence of patterns
non-simplifiable full	none	ABCDCDAB
non-simplifiable elided	some	ABCDCDAB
non-simplifiable patch	all	ABCDCDAB
simplifiable full	none	EFGH
simplifiable elided	some	EFGH
simplifiable patch	all	EFGH

Table 13: **Circuit variants.** Six variants of RQCs employed in quantum supremacy demonstration (non-simplifiable full) and performance evaluation (remaining five variants) classified by transformations applied in order to control the cost of classical simulation. The eight coupler activation patterns A, B, ..., H are shown in Fig. S25.

Circuit variant	n	m	Single-qubit gates	All two-qubit gates	Cross-partition two
non-simplifiable full	53	20	1113	430	35
non-simplifiable elided	53	20	1113	408	13
non-simplifiable patch	53	20	1113	395	0
simplifiable full	38	14	570	210	18
simplifiable elided	38	14	570	204	12
simplifiable patch	38	14	570	192	0

Table 14: **Gate counts.** Number of gates in selected random quantum circuits employed for quantum supremacy demonstration and performance evaluation of the Sycamore processor.

Gate elision

The most straightforward way to reduce the cost of classical simulation of a RQC is to remove a number of cross-partition gates across the most promising circuit cut. In order to enable independent propagation by the SFA of the wave function of each circuit partition for the first few cycles, the gates are elided beginning with the initial cycle. Each elided gate reduces the bond dimension of the partitioning by a factor of two or four, see Section 11.10.

We refer to RQCs with a small number of elided gates as *elided circuits*. A particularly dramatic speedup is possible when all two-qubit gates across the partitions are elided leading to two disconnected circuits running in parallel. We refer to such disconnected RQCs as *patch circuits*. Base RQCs in which no gates have been elided are referred to as *full circuits*.

If the error probability of the elided two-qubit gate is similar to the error probability of the two-qubit identity gate which it is replaced with, the circuit resulting from gate elision exhibits fidelity that is similar to the fidelity of the original circuit. This assumption holds when the two-qubit gate errors are dominated by the same decoherence processes that govern the single-qubit gate errors such as finite T_1 and T_2. Indeed, for circuit sizes where XEB on full circuits is possible, we have observed good agreement between fidelity estimates produced for patch, elided and full circuits. For harder circuits, we have observed good agreement between fidelity estimates for patch and elided circuits. See Section 11.8 for detailed discussion of these results.

Wedge formation

The most competitive algorithm for our hardest circuits, SFA (see Sec. 11.10.1) scales proportionally to the bond dimension of the circuit partitioning which is equal to the product of Schmidt rank of all cross-partition gates (see Sec. 11.10.4). The Schmidt decomposition of most two-qubit gates in our RQCs consists of four terms (a few gates can be replaced with

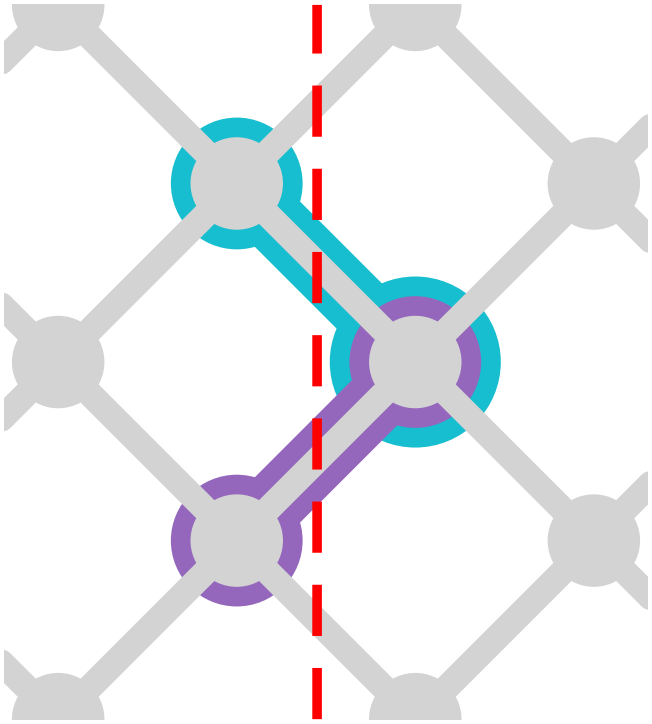


Figure S26: **Cross-partition wedge.** Two consecutive cross-partition gates which share a qubit form a *wedge*, as illustrated here with gates highlighted in turquoise and magenta. Schmidt rank of a single two-qubit gate is at most four. Schmidt rank of a wedge is also at most four. Therefore, generally wedges are not efficient at increasing entanglement across partitions and can be simulated efficiently by the SFA.

simpler gates with Schmidt rank of two, see Section 11.10). Therefore most cross-partition gates contribute a factor of four to the bond dimension of the partitioning. However, when two consecutive cross-partition gates share a qubit forming a *wedge* as shown in Fig. S26, the Schmidt decomposition of the resulting three-qubit unitary also has only four terms. In other words, the second cross-partition gate does not generally produce substantial new entanglement (as quantified by the Schmidt rank) among the partitions in excess of the entanglement produced by the first gate. Consequently, every wedge reduces the bond dimension of the partitioning by a factor of four.

The eight-cycle sequence ABCDCDAB and the four constituent coupler activation patterns A, B, C and D shown in Fig. S25 have been designed to prevent formation of wedges across promising circuit cuts. In other words, the sequence ensures that entanglement created in a given cycle by cross-partition gates is transferred into the bulk of each partition in the following cycle.

On the other hand, the four-cycle sequence EFGH enables formation of wedges and thus efficient simulation of RQCs using SFA. We employ the latter sequence in most evaluation circuits and use the former eight-cycle sequence for the quantum supremacy circuits and largest evaluation circuits, see Table 13.

11.8 Large scale XEB results

In Section 11.6, we have detailed the device calibration processes used for individual components such as qubits, couplers, and coupled pairs of qubits. We have also introduced cross-entropy benchmarking (XEB) as a method that allows us to evaluate the performance of a quantum system. In this section, we describe how we use a few circuit variations to benchmark

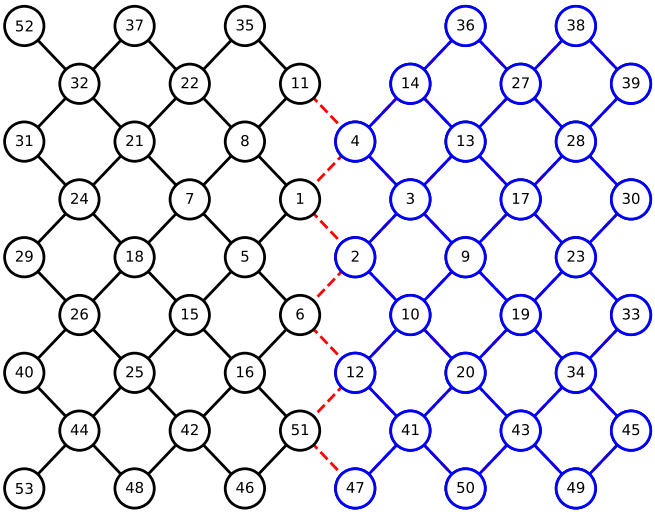


Figure S27: **Qubit ordering for large-scale XEB experiments.** Illustration of the order in which qubits are added for large-scale experiments. The partition between left (black) and right (blue) qubits along the boundary (dashed red lines) is used in patch and elided circuits, as explained below.

our Sycamore processor at a larger scale. In particular, we present a modular version of XEB with "patch circuits" that does not require exponential classical computation resources for estimating XEB fidelities $\mathcal{F}_{\text{XEB}}$ of larger systems. We also describe the effect of choice of unitary model on large-scale $\mathcal{F}_{\text{XEB}}$, as well as how we use patch circuits to monitor the stability of the full system.

11.8.1 Limitations of full circuits

We first discuss what we refer to as "full circuits", where for a given set of qubits, all possible two-qubit gates participate in the circuit. With full circuits, we benchmarked the system as a function of size, where as discussed below the classical resources and techniques used to compute the $\mathcal{F}_{\text{XEB}}$ is a function of the number of qubits. The order in which each qubit was added is labeled in Fig. S27. The rationale behind this ordering is explained in Section 11.7. At each system size, we executed 10 randomly generated circuit instances on the processor and sampled output bitstrings 500k times for each circuit (unless otherwise specified). To minimize potential instance-to-instance fluctuations, we chose the gate sequences in a persistent, "stable" manner: using a known seed for a random number generator, for each circuit, each time a new qubit is added, we maintain the same gateset for all the "existing" qubits and new gates are only introduced to qubits and pairs associated with the added qubit (see Section 11.7 for details).

Once a sufficient number of bitstrings are collected, $\mathcal{F}_{\text{XEB}}$ can be calculated for each system size, following the method described in Section 11.4. As the system size increases, the computational complexity of XEB analysis grows exponentially, which can be qualitatively divided into three regimes. For system size from 12 to 37 qubits, XEB analysis was carried out by evolving the full quantum state (Schrödinger method) on a high-performance server (88 hyper-threads, 1.5TB memory in our case) using the "qsim" program. At 38 qubits we used a n1-ultramem-160 VM in Google's cloud (160 hyperthreads, 3.8TB memory). Above 38 qubits, Google's large-scale cluster computing became necessary, and in addition a hybrid Schrödinger-Feynman approach, the "qsimh" program, was used to improve the efficiency: in this case, we break the system up into two patches, where each patch can be efficiently computed via the Schrödinger method and then connected by a Feynman path-integral approach (see Section

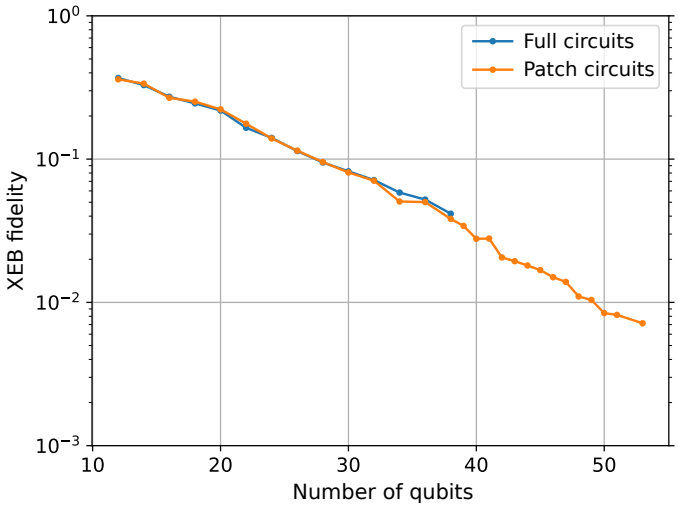


Figure S28: **Comparison between XEB with patch circuits and full circuits.** Full vs. patch circuit benchmarking up to 38 qubits with 14 cycles, showing close agreement to within the intrinsic fluctuations of the system. We plot the results for patch circuits out to 53 qubits.

11.10 for more details). Finally we used a Schrödinger algorithm in the Jülich supercomputer for some circuits up to 43 qubits.

In order to reduce the computational cost, we introduce two modified circuit types in the following sections. By using slightly simplified gate sequences, these two methods can provide good approximate predictions of system performance all the way out to the "quantum supremacy" regime.

11.8.2 Patch circuits: a quick performance indicator for large systems

The simplest approach to large-scale performance estimation is referred to as "patch circuits," which predicts the performance of the full system by multiplying together the fidelities of non-interacting subsystems, or "patches". In this work, we use two such subsystems, where each patch is roughly half the size of the full system. The two subsystems are run simultaneously, so that effects such as gate and measurement crosstalk between patches are included, but the two patches are analyzed separately when computing the fidelity. The two patches are defined by the gates removed along their boundary, as illustrated in Fig. S27. For sufficiently large systems, these removed two-qubit gates represent a small portion of the whole circuit. As a consequence, $\mathcal{F}_{\text{XEB}}$ of the full system can be estimated as the product of the fidelities of the two subsystems; compared with full circuits, the main missing factor is the absence of entanglement between the two patches.

We evaluate the efficacy of using patch circuits by comparing it against full circuits with the same set of qubits. The experimental results can be seen in Fig. 4a (main text), where we show fidelities measured by these two methods for systems from 12 qubits to 53 qubits, in an interleaved fashion. We re-plot this data here in Fig. S28 as well. As expected, the fidelities obtained via patch XEB show a consistent exponential decay (up to fluctuations arising from qubit-dependent gate fidelities and a small amount of system fluctuations) as a function of system size. For every system size investigated, we found that patch and full XEB provide fidelities that are in good agreement with each other, with a typical deviation of $\sim$5% of the fidelity itself (we attribute the worst-case disagreement of 10% at 34 qubits due to a temporary system fluctuation in between the two datasets, which was also seen in interleaved measurement

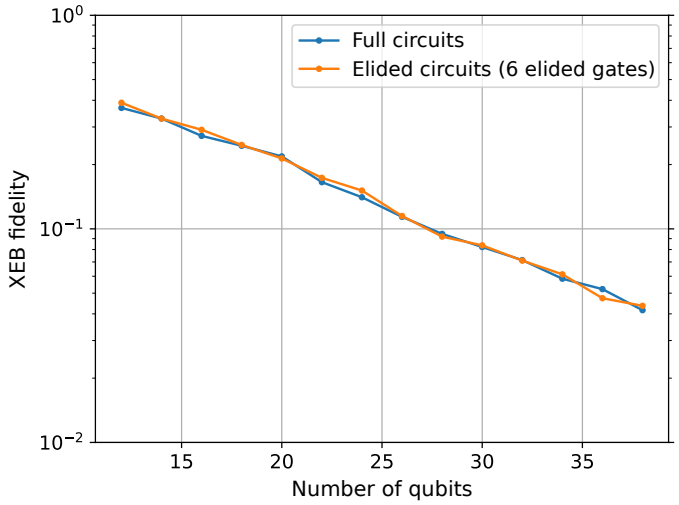


Figure S29: **Comparison between XEB with elided circuits and full circuits.** Full vs. elided circuit benchmarking up to 38 qubits at 14 cycles, showing close agreement to within the intrinsic fluctuations of the system.

fidelity data). Theoretically, one would expect patch circuits to result in $\sim 10\%$ higher fidelity than full circuits due to the slightly reduced gate count. We find that patch circuits perform slightly worse than expected, which we believe is due to the fact that the two-qubit gate unitaries are optimized for full operation and not patch operation. In any case, agreement between patch and full circuits shows that patch circuits can be a good estimator for full circuits, which is quite remarkable given the drastic difference in entanglement generated by the two methods. These results give us a good preview of the system performance in all three regimes discussed earlier.

The advantage of using patch circuits lies in its exponentially reduced computational cost, as it only requires calculating $\mathcal{F}_{\text{XEB}}$ of subsystems at half the full size (or less if a larger number of smaller patches is used). This allows for quick estimates of large-scale system performance on a day-to-day basis, including for system and circuit sizes in the "quantum supremacy" regime. As a consequence, we typically use patch circuits as a quick system performance indicator, which we use for rapid turnarounds between system calibration and performance evaluation, as well as for monitoring full system stability (see Section 11.8.8). We also note that patch circuits can be used well beyond 50 qubits, and in fact can be extended to arbitrary numbers of qubits while keeping the analysis time at most linear in the number of qubits (or even constant if the patches can be analyzed in parallel), assuming that the patch size stays roughly constant and more non-interacting patches are added as the number of qubits grows.

11.8.3 Elided circuits: a more rigorous performance estimator for large systems

For a more rigorous prediction of full $\mathcal{F}_{\text{XEB}}$, we introduce a more sophisticated approach referred to as "elided circuits". Similar to patch circuits, we partition a given set of qubits into two subsets separated by a boundary, but elide (remove) only a fraction of the two-qubit gates along this boundary during a few early cycles of the sequence (more specifically, we elide the earliest gates in time, meaning early layers will have none of their gates along the boundary while later layers will have all of their usual gates across the boundary). Accordingly, the two subsets of qubits are no longer isolated from each other and we cannot simply compute their fidelities separately and multiply. Rather, we must still compute the evolution of the full system. Given that a sufficient number of gates are elided, we can take advantage of the "weak link"

between patches with a hybrid analysis technique: we compute each patch via the Schrödinger method and then connect them with a Feynman path-integral approach (see Section 11.10 for more details on this “qsimh" program).

Compared with patch circuits, elided circuits more closely approach a description of the full system performance under a full circuit: in addition to capturing issues such as control and readout crosstalk, elided circuits allow entanglement to form between the two weakly connected subsystems. It covers essentially all the possible processes that occur in the full circuit, and therefore can be used to predict system performance at a dramatically reduced computational cost, albeit significantly costlier than patch circuits.

In order to validate the use of elided circuits as a system performance estimator, we evaluated its accuracy via a direct comparison with full circuits. In Fig. S29 we show two sets of fidelities from interleaved full and elided circuit experiments. For every system size investigated, using elided circuits yields a fidelity value that is in good agreement with the one obtained with the corresponding full circuits. The average ratio of elided circuit fidelity to full circuit fidelity over all verification circuits was found to be 1.01, with a standard deviation of 5%, dominated by system fluctuations. It is this agreement that certifies elided circuits as a precise predictor for full circuits (within a systematic relative uncertainty of 5%), which we rely on to extrapolate the system performance in the regimes where full circuit analysis is too expensive to perform (i.e., Fig. 4b of the main text).

Compared with full circuits, elided circuits can result in a reduced amount of quantum entanglement in the system. The amount of reduced entanglement can be bounded from above by counting the number of iSWAP gates across the boundary: one iSWAP gate generates at most two units of bipartite entanglements (ebits). This upper bound translates directly into the exponential cost of a Schrödinger-Feynman simulation. For elided circuits with 50 qubits and 14 cycles, the full circuit has approximately 25 ebits of entanglement, while with 6 elisions the elided circuit has at most 12 ebits entanglement between the two patches. For the 53-qubit elided circuits used in the main paper [1], there were enough iSWAPs across the boundary that the amount of entanglement between patches for full vs. elided circuits should be close, giving us even more confidence in using elided circuits to predict the fidelity of the circuit used to claim quantum supremacy.

11.8.4 Choice of unitary model for two-qubit entangling gates

In Section 11.6, we discussed how the two-qubit gate unitaries can be measured by two different approaches: isolated two-qubit XEB and per-layer simultaneous two-qubit XEB. These two methods resulted in two different unitary models when deducing the best-fit unitary. Since we must specify the two-qubit gate unitary matrices in order to compute $\mathcal{F}_{\mathrm{XEB}}$ of the larger system, a natural question is which unitary model should be used. To address this question, we point out that full XEB on the large system occurs in repeated cycles, where during each two-qubit gate layer, all the two-qubit gates in the same orientation take place at the same time (see Fig. 3 in the main text). As a consequence, the two-qubit gate layers during simultaneous pair XEB in Fig. S19 emulate the corresponding layer when running full XEB on a large system. Accordingly, learning the unitaries in parallel operation captures any small coherent modifications induced by the simultaneous application of the other two-qubit gates, such as flux control crosstalk and dispersive shifts from stray interactions. This is evident from the fact that by re-learning the two-qubit unitary parameters, the errors extracted from simultaneous pair XEB become purity-limited (see Fig. S19). This correspondence assures us that unitary parameters extracted from simultaneous pair XEB provides a more accurate description of the full system when full XEB is performed.

In Fig. S30, we show patch circuit fidelities at different system sizes, where the fidelity is

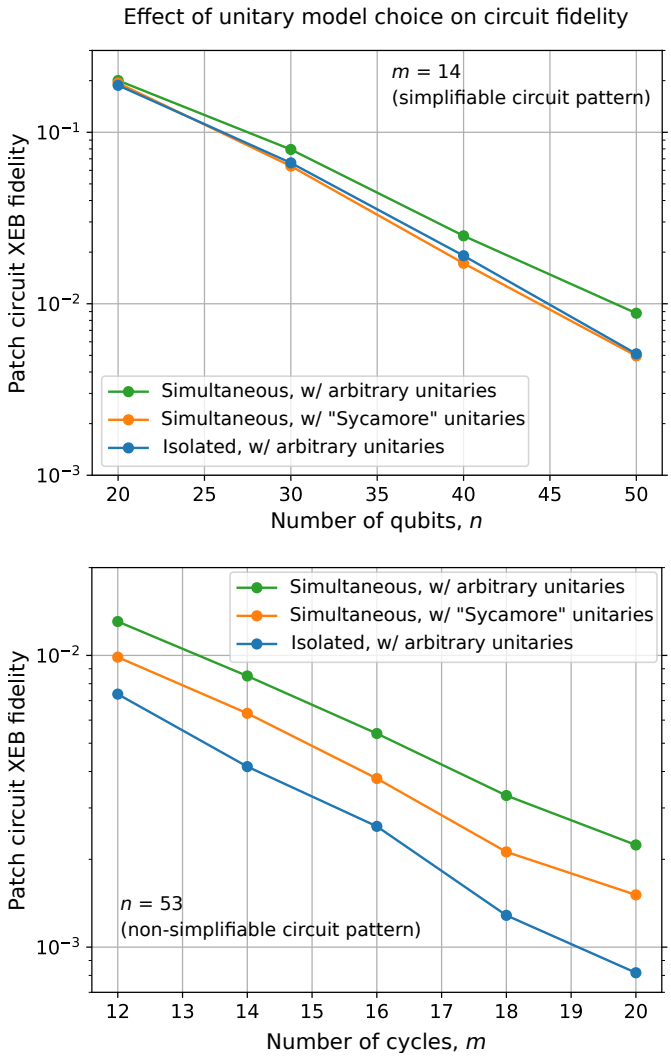


Figure S30: **Effect of unitary model on full system fidelity. a,** Patch circuit fidelity versus number of qubits and choice of unitary model. **b,** Same but versus number of cycles and for the non-simplifiable supremacy circuits. Blue: patch XEB fidelities using the unitaries deduced from the best-fit fSim unitary from isolated pair XEB. Green: patch XEB fidelities using the unitaries deduced from the best-fit fSim unitary from per-layer simultaneous pair XEB. Orange: patch XEB fidelities using the unitaries deduced from the best-fit "Sycamore unitary" ($\theta = \pi/2$, $\phi = \pi/6$) from per-layer simultaneous pair XEB. As expected, the best fidelities arise from fitting to the most general unitary in parallel operation, although the fidelities are high enough to achieve quantum supremacy with the Sycamore unitary model as well.

evaluated using three different unitary models: the best-fit unitaries from isolated pair XEB, the best-fit unitaries from simultaneous pair XEB, and the best-fit "Sycamore" unitaries from simultaneous pair XEB. The Sycamore unitaries are the unitaries obtained when keeping the swap angle fixed at $\theta = \pi/2$ and conditional phase fixed at $\phi = \pi/6$ for all qubits, and then fitting only for two single-qubit phase terms. For the purpose of benchmarking the system fidelity for the operations we performed, we have focused on using unitaries learned from simultaneous pair XEB, which provide the most accurate description of the system. The validity of this approach is experimentally verified—for the same gate sequences, using the simultaneous pair XEB unitaries leads to the best full-system fidelity values at every system size. This is direct evidence that the unitaries learned from simultaneous pair XEB form a more accurate description of the system than those from isolated pair XEB.

On the other hand, in order to be useful for generic quantum algorithms, it will be desirable to use calibrated gatesets that are independent of the specific gate sequences used. For this purpose, it is important to check the circuit fidelity under the other two unitary models, where the two-qubit gate unitaries were calibrated in more generic settings. One can see that fidelities calculated from these two unitary models still demonstrate nearly as good performance despite the addition of small coherent control errors. They differ from the fidelities using the simultaneous pair XEB unitaries by less than a factor of 2 at 50 qubits (fidelity goes from 9×10^{-3} to 5×10^{-3} at 50 qubits). This is remarkable since it suggests going from a 2-qubit setting to 50-qubit setting, our full system calibration precision degrades only by a factor of < 2 despite the system size increasing by a factor of 25. This high precision in gate calibration gives us confidence to use our processors in NISQ algorithms.

11.8.5 Understanding system performance: error model prediction

In this section, we perform additional analysis to compare the measured fidelities to that predicted from the constituent gate and measurement errors.

The most commonly used error model in quantum computing theory is the digital error model. Analogous to the independent noise model in classical information theory, the digital error model is based on the assumption that there are no space and time correlations between errors of quantum gates [59, 60, 27]. If this assumption is valid, it should be possible to construct the fidelity of a large quantum system from the fidelities of its constituent parts: single- and two-qubit gates, and measurement. It is important to point out that the gate fidelity metric that should be used here is the entanglement fidelity, $1 - e_P$ (see Section 11.5 for more details). This is the correct quantity to describe the fidelity of quantum operations since, in contrast to other metrics such as the commonly used average fidelity, it is independent of the dimension of the Hilbert space.

In Fig. S31, we show fidelities as a function of both system size and number of cycles (circuit depth), measured with patch circuits. In each plot, we compare the measured fidelities to the predicted fidelities, which are calculated from a simple multiplication of individual gate entanglement fidelities as measured during simultaneous operation, along with the measurement fidelities obtained during simultaneous measurement. We note that the measured readout fidelities actually also automatically include the effect of state preparation errors as well. More explicitly, if a circuit contains the set of single-qubit gates G_1, the set of two-qubit gates G_2, and the set of qubits Q, then we approximate the fidelity F as

$$F = \prod_{g \in G_1} (1 - e_g) \prod_{g \in G_2} (1 - e_g) \prod_{q \in Q} (1 - e_q), \tag{11.77}$$

where e_g are the individual gate Pauli errors and e_q are the state preparation and measurement errors of individual qubits. It is evident that there is a good agreement between the measured

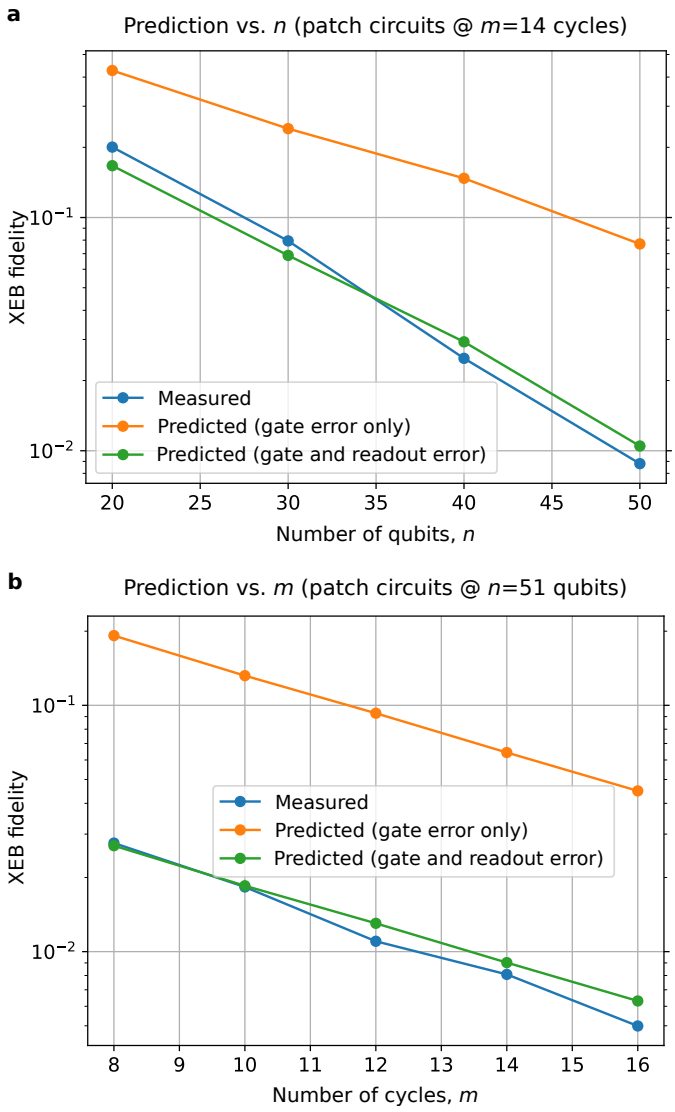


Figure S31: **Predicted vs. measured large-scale XEB fidelity. a,** Data and two predictions for 14-cycle patch circuits vs. number of qubits. Predictions are based on the product of single- and two-qubit gate entanglement fidelities under simultaneous operation. Blue curve contains measured fidelities. Orange is the prediction based only on gate errors during parallel operation, but without taking measurement error into account. Green is the same but multiplied by the measured readout fidelities. **b,** Same as the first panel, but vs. number of cycles at a fixed number of qubits $n = 51$. Again, the prediction from simultaneous gate fidelities and measurement fidelity is a good prediction of the actual system performance.

and predicted fidelities, with deviations of up to only 10-20%. Given that the sequence here involves tens of qubits and $\sim$ 1000 quantum gates, this level of agreement provides strong evidence to the validity of the digital error model.

This conclusion can be further strengthened by the close agreement between the fidelities of full circuits, patch circuits, and elided circuits. Even though these three methods differ only slightly in the gate sequence, they can result in systems with drastically different levels of computational complexity and entanglement between subsystems. The agreement between the fidelities measured by these different methods, as well as the agreement with the predicted fidelity from individual gates, gives compelling evidence confirming the assumptions made by the digital error model. Moreover, these assumptions remain valid even in the presence of quantum entanglement.

The validation of the digital error model has crucial consequences, in particular for quantum error correction. The absence of space or time correlations in quantum noise has been a commonly assumed property in quantum error correction since the very first paper on the topic [59]. Our data is evidence that such a property is achievable with existing quantum processors.

11.8.6 Distribution of bitstring probabilities

In Section 11.4, we motivate two different estimates for fidelity F, one based on the cross entropy, Eq. (11.28), and the other based on linear cross entropy, Eq. (11.27). In this section, we examine the probabilities of sampled bitstrings and compare them against theoretical distributions. We use bitstring samples from non-supremacy region to demonstrate the analysis methodology, then apply it to the sample in the supremacy region.

The theoretical PDF for the bitstring probability p with linear XEB is

$$P_l(x|F) = (Fx + (1-F))e^{-x}$$

where $x \equiv Dp$ is the probability p scaled by the Hilbert space dimension D, and F is the linear cross entropy fidelity. The PDF for $\log p$ is

$$P_c(x|F) = (1 + F(e^x - 1))e^{x-e^x}$$

where $x \equiv \log(Dp)$ and F is the cross entropy fidelity.

From a set of bitstrings $\{q_i\}$, the fidelity is estimated from the ideal probabilities $\{p_i = p_s(q_i)\}$ as

$$\hat{F}_l = \langle Dp \rangle - 1, \tag{11.78}$$
$$\hat{F}_c = \langle \log(Dp) \rangle + \gamma, \tag{11.79}$$

where γ is the Euler-Mascheroni constant, see Sec. 11.4.2.

Figure **??** shows the distribution of $\{p_i\}$ from 0.5 million bitstrings obtained in an experiment with a 20-qubit 14-cycle random quantum circuit. For comparison, we produce 0.5 million bitstrings sampled uniformly at random and 0.5 million bitstrings sampled from the output distribution of the ideal circuit and show them in the same figure. The theoretical distribution curves are also shown, where the fidelity estimated from data is fed into the curve $P_l(x|\hat{F})$ and $P_c(x|\hat{F})$.

We see good agreements between experiment and theory. To quantify the agreements, we use the Kolmogorov-Smirnov test [61] to characterize the goodness of fit of data $\{p_i\}$ to theoretical PDFs. First we compute the Kolmogorov-Smirnov statistics D_{KS}, that is, the distance between data and theory as the supremum of point-wise distances between the empirical cumulative distribution function of data ECDF(p) and the theoretical cumulative distribution function CDF(p):

$$D_{KS} = \sup_i |\text{ECDF}(p_i) - \text{CDF}(p_i)|.$$

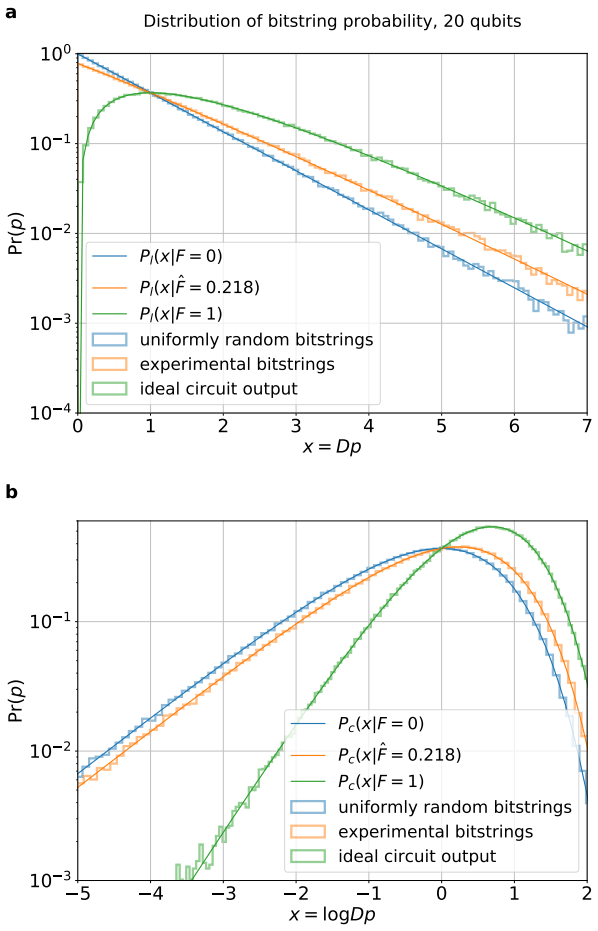


Figure S32: **Histograms of ideal probabilities.** The ideal probability p is calculated from the final state amplitudes of a (20-qubit 14-cycle) random circuit. The blue, orange, and green histogram is the ideal probabilities of bitstrings sampled uniformly at random, from the experiment, and ideal output, respectively. **a,** The distribution of Dp and theoretical curves $P_l(x|F_l)$ normalized to histogram counts for $F_l = 0, \hat{F}_l, 1$, respectively. **b,** The distribution of $\log(Dp)$ and theoretical curves $P_c(x|F_c)$ for $F_c = 0, \hat{F}_c, 1$, respectively.

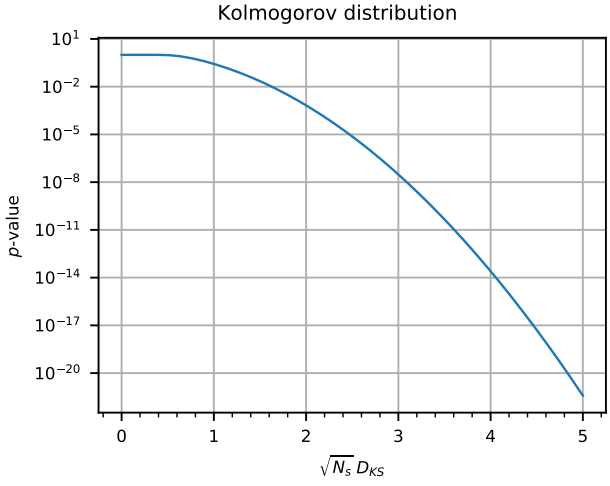


Figure S33: **The Kolmogorov distribution function.** This function is used to compute p-value from a given D_{KS} and number of samples N_s.

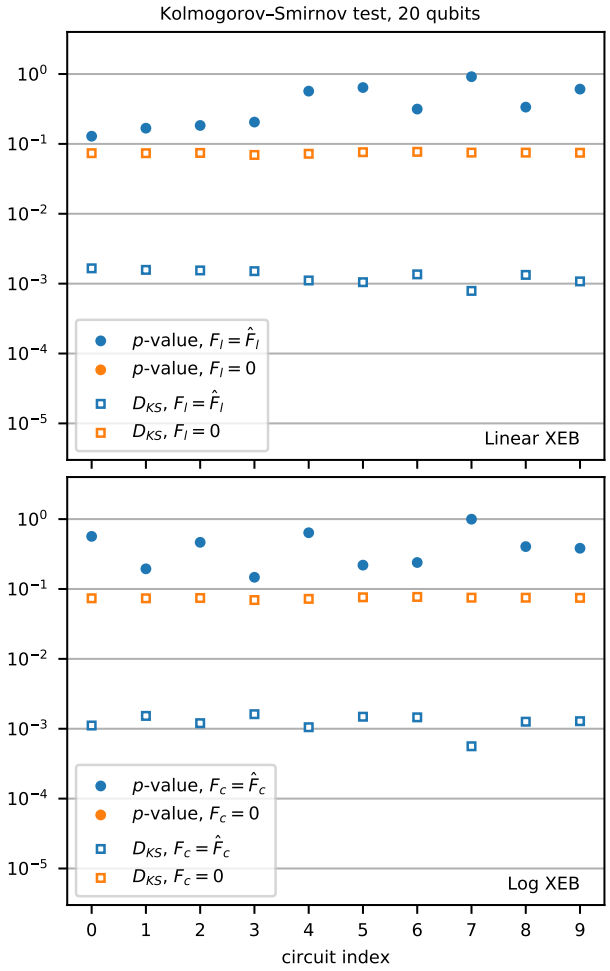


Figure S34: **The Kolmogorov-Smirnov test results for each of 10 circuits for a (20-qubit 14-cycle) random circuit.** See text for the definition of D_{KS} and p-value. The upper plot is for linear XEB, and the lower one is for log XEB.

	D_{KS}		p-value	
	$F = \hat{F}$	$F = 0$	$F = \hat{F}$	$F = 0$
Linear XEB	1.3×10^{-4}	9.6×10^{-4}	0.66	$< 2.2 \times 10^{-16}$
Log XEB	9.5×10^{-5}	9.6×10^{-4}	0.95	$< 2.2 \times 10^{-16}$

Table 15: **The Kolmogorov-Smirnov test results on combined samples**.

We then convert the distance D_{KS} to a p-value using the Kolmogorov distribution shown in Fig. ??. The p-value is used for rejecting the null hypothesis that the data $\{p_i\}$ is consistent with the theoretical distribution. The whole Kolmogorov-Smirnov test is done using the scipy package [62] and checked against R package ks.test [63]. Both packages produce consistent results.

We test the ideal probabilities of bitstrings observed in the experiment $\{p_i\}$ against 2 theoretical distributions, one with estimated fidelity $F = \hat{F}$ and one with fidelity $F = 0$. The Kolmogorov-Smirnov statistics D_{KS} and the p-value of every circuit are shown in figure ??. Note that the p-values for $F = 0$ are not shown because they are $\ll 10^{-20}$ due to the large $D_{KS} \approx 0.07$ with $N_s = 5 \times 10^5$ points in the sample. That is evident from reading off Fig. ??.

We reject the null hypothesis that the experimental bitstrings are consistent with the uniform random distribution with very high confidence for this (20-qubit 14-cycle) random circuit.

Now we turn our attention to the supremacy circuits.

We use random circuits with gate elisions for checking the distributions because it is exponentially expensive to calculate the ideal theoretical probability of a bitstring without gate elisions. The effect on fidelity from gate elisions is well understood, see Sec. 11.8.3. The gate elisions are chosen to minimize the effect while making the classical estimation feasible, see Sec. 11.7.7. We sample $N_s = 3 \times 10^6$ bitstrings $\{q_i | i = 1...N_s\}$ from each of 10 (53-qubit 20-cycle) random circuits, and compute the theoretical ideal probabilities of each bitstring $\{p_i | i = 1...N_s\}$.

The distributions of Dp and $\log(Dp)$ from one such circuit along with the corresponding theoretical curves are shown in Fig. ??.

We again use the Kolmogorov-Smirnov test to characterize the goodness of fit of data $\{p_i\}$ to theoretical PDFs with estimated fidelity $F = \hat{F}$ and zero fidelity $F = 0$. The Kolmogorov-Smirnov statistics D_{KS} and the p-value of every circuit are shown in figure ??.

The p-value for the null hypothesis of zero fidelity is generally small for every circuit, with a maximum of 0.045 for circuit number 1. We say that the null hypothesis of zero fidelity is rejected better than a 95% confidence level for each circuit. On the other hand, the p-value of null hypothesis of estimated fidelity $\hat{F}$ is generally large. The p-value is between 0.18 and 0.98 for linear XEB, and between 0.33 and 0.98 for log XEB. That indicates that the empirical cumulative distribution functions $\mathrm{ECDF}(p_i)$ from data is quite consistent with the theoretical $\mathrm{CDF}(p_i|\hat{F})$.

As will be seen in Fig. S38 in section 11.8.7 below, the fidelity of individual circuits are consistent with each other within the statistical uncertainties. Therefore it makes sense to do a Kolmogorov-Smirnov test on all samples combined, containing 30 million bitstrings. The estimated fidelities from the combined sample are $\hat{F}_l = 2.24 \times 10^{-3}$ and $\hat{F}_c = 2.34 \times 10^{-3}$, respectively. The D_{KS} and p-values are listed in table ??. The p-value for the null hypothesis of $F = 0$ is very small: p-value $= 3 \times 10^{-24}$ from scipy, and p-value $< 2.2 \times 10^{-16}$ from R. We note the more conservative value in the table. The null hypothesis of $F = 0$ is rejected with much higher confidence levels than individual circuits.

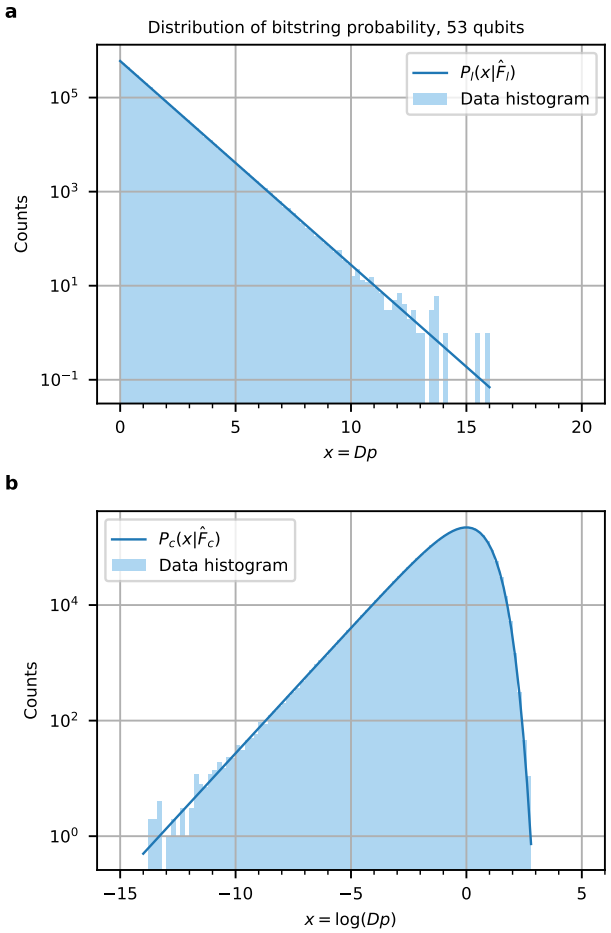


Figure S35: **Distribution of bitstring probabilities from a 53-qubit 20-cycle circuit.** We calculate the theoretical probabilities of experimentally-observed bitstrings. **a,** The distribution of Dp and the theoretical curve $P_l(x|\hat{F}_l)$ normalized to histogram counts. **b,** The distribution of $\log(Dp)$ with theoretical curve $P_c(x|\hat{F}_c)$.

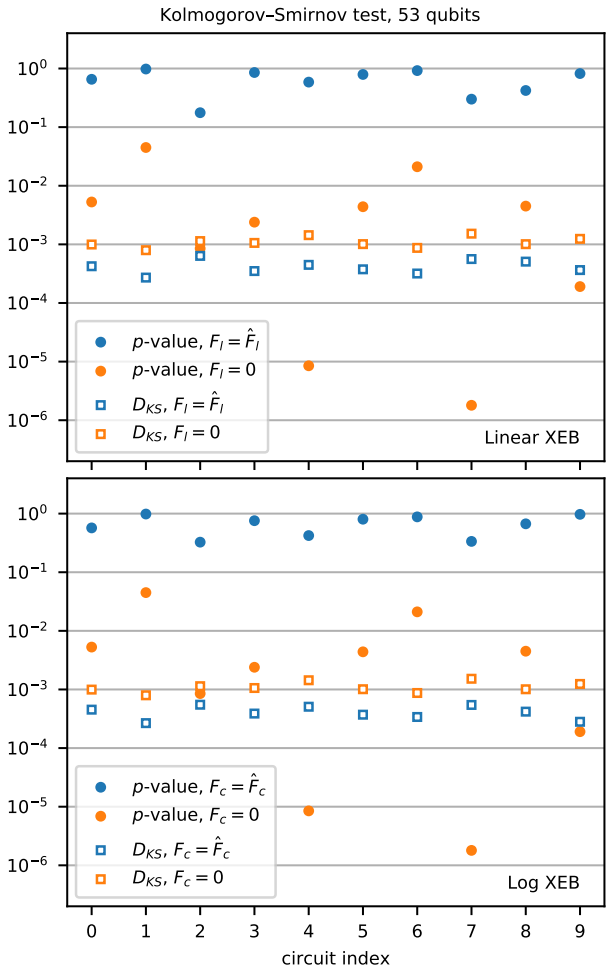


Figure S36: **The Kolmogorov-Smirnov test results for random circuits with 53 qubits.** The upper plot is for linear XEB, and the lower one is for log XEB.

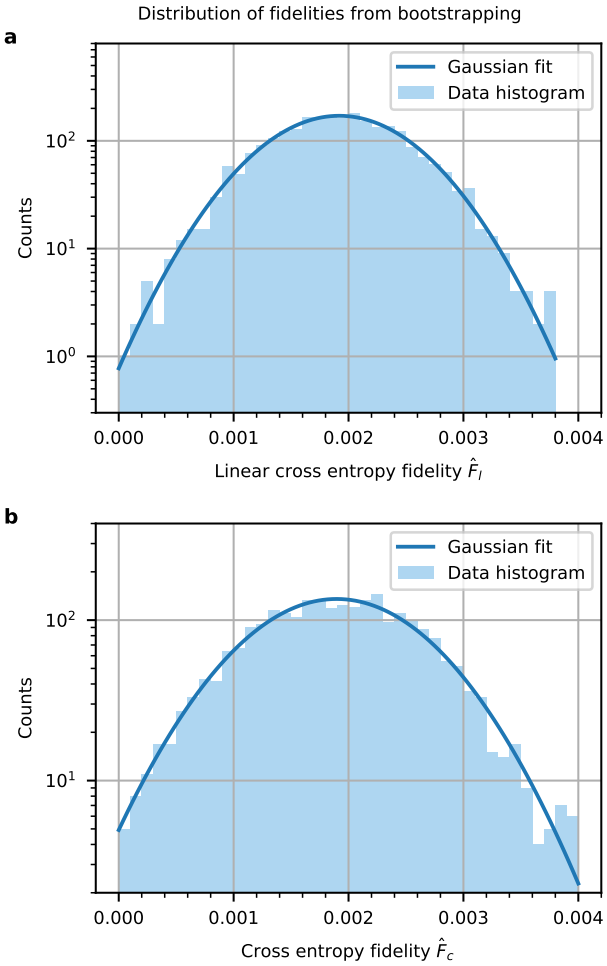


Figure S37: Distribution of fidelity from 4000 bootstrap samples. **a,** The distribution of bootstrap $\hat{F}_l$. The theoretical curve is a Gaussian fit normalized to histogram counts. **b,** The distribution of bootstrap $\hat{F}_c$, with Gaussian fit.

11.8.7 Statistical uncertainties of XEB measurements

In this section we check the statistical uncertainties of our fidelity estimates against theoretical predictions.

The statistical uncertainties of $\hat{F}_l$ and $\hat{F}_c$ are estimated from data using the standard error-on-mean formula as

$$\begin{aligned} \hat{\sigma}_{F_l} &= D\sqrt{\mathrm{Var}(p)/N_s}, \\ \hat{\sigma}_{F_c} &= \sqrt{\mathrm{Var}(\log p)/N_s}, \end{aligned}$$

where $\mathrm{Var}(x)$ is the variance estimator of sample $\{x_i\}$. Because the distribution of p and $\log p$ have finite variances both experimentally and theoretically, we can use the bootstrap procedure [64] to verify the estimate of statistical uncertainties.

The fidelity distribution from 4000 bootstrap samples are shown in Fig. ??. The distribution of $\hat{F}_l$ and $\hat{F}_c$ are each fit to a Gaussian distribution function using maximum likelihood.

The Kolmogorov-Smirnov test on the Gaussian fit produces p-values of 0.99 and 0.41 for $\hat{F}_l$ and $\hat{F}_c$ bootstrap distributions, respectively. It indicates that the central limit theorem is at work and the distributions are consistent with Gaussian distributions.

The estimated statistical uncertainty, the standard deviation of the bootstrap distribution, and the σ parameter of the Gaussian fit are compared against each other to verify that the

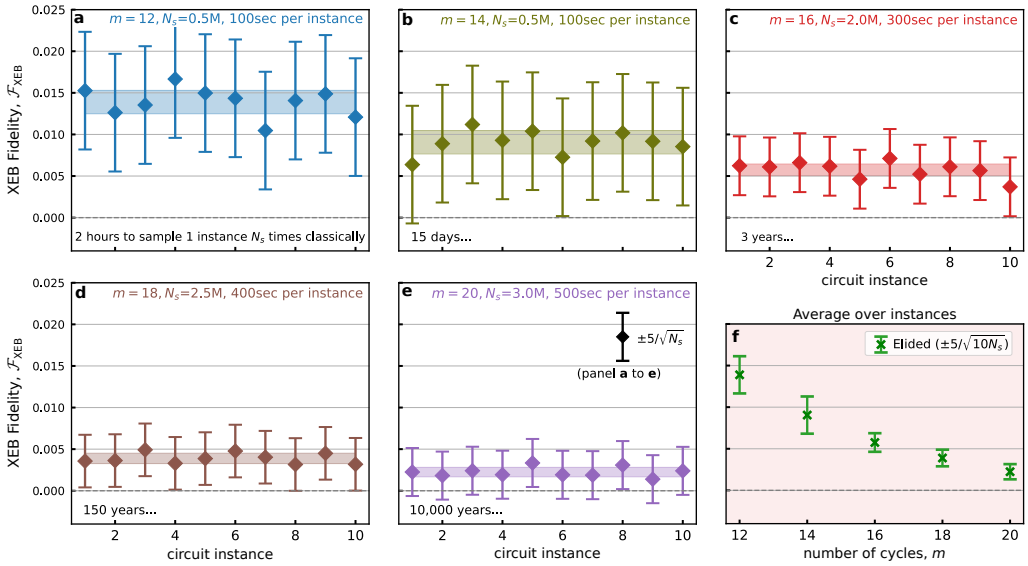


Figure S38: Per-instance elided circuit fidelities and statistical uncertainties. XEB fidelities of all 10 elided circuit instances for each circuit depth from Fig. 4b of the main text. **a** to **e**, Here, each panel corresponds to a single circuit depth m. In these panels, $\pm 5\sigma$ statistical error bars, where $\sigma = 1/\sqrt{N_s}$, are shown for each of the individual circuit instance fidelities. Also shown is a band corresponding to $\pm\sigma$ for a single instance, but about the mean fidelity of the 10 instances, showing that the variations between circuits can be explained by statistical fluctuations from the finite number of samples. **f**, Fidelity averaged over all 10 circuits along with $\pm 5\sigma$ error bars are shown (the same quantity is plotted in Fig. 4b of the main text but on a log scale), where in this case $\sigma = 1/\sqrt{10N_s}$. Here, for all circuit depths, the mean fidelity is more than 5σ above 0.001.

statistical uncertainty estimate is minimally biased. For the example circuit used in the figures, the three parameters are 5.78, 5.78, 5.78 ($\times 10^{-3}$) for $\hat{\sigma}_{F_l}$, respectively. The same parameters for $\hat{\sigma}_{F_c}$ are 7.40, 7.46, 7.46 ($\times 10^{-3}$). The relative differences are less than 1%, consistent with the expected agreement of parameters for 4000 bootstrap samples.

We repeat the bootstrap procedure on all ten 53-qubit 20-cycle circuits with 2500 bootstrap resamples. The statistical uncertainty estimates are all within 3.1% of the bootstrap standard deviation.

The combined linear cross entropy fidelity and statistical uncertainty of 10 random circuits is calculated using inverse-variance weighting to be $\hat{F}_l = (2.24 \pm 0.18) \times 10^{-3}$. The theoretical prediction of the statistical uncertainty, $\sqrt{(1 + 2F - F^2)/N_s}$, is 1.8×10^{-4}, which agrees with the experimental estimate. As a comparison, the combined cross entropy fidelity is $\hat{F}_c = (2.34 \pm 0.23) \times 10^{-3}$. The theoretical prediction of statistical uncertainty, $\sqrt{(\pi^2/6 - F^2)/N_s}$, is 2.3×10^{-4}, which agrees with the experimental estimate as well. Thus, the cross entropy fidelity and linear cross entropy fidelity estimators produce consistent results. Furthermore, the statistical uncertainty of the linear cross entropy estimator is smaller, as expected from its theoretical formula.

In Fig. S38, we also show the linear XEB fidelities and 5σ statistical uncertainties of all 10 elided circuit instances for each circuit depth from Fig. 4b of the main text. Variations between the fidelities of different circuit instances are consistent with the expected statistical noise due to the finite number of samples. In the last panel, we also show the smaller statistical uncertainties of the fidelity averaged over the 10 circuit instances for each depth.

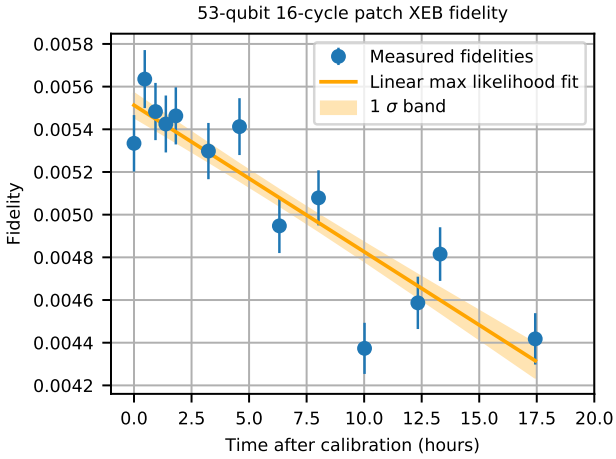


Figure S39: Stability of repeated 53-qubit 16-cycle patch circuit benchmarking over 17.4 hours, without any system recalibration. Statistical error bars from the finite bitstring sample number are included. The intrinsic system fluctuations are likely dominated by a small number of TLSs moderately coupled to a few qubits at their idling and/or readout biases.

11.8.8 System stability and systematic uncertainties

In addition to statistical errors, XEB fidelity is also subject to systematic drift as the system performance may fluctuate and/or degrade over time. To quantify these mechanisms, we performed a patch circuits time stability measurement on 53 qubits using a circuit of 16 cycles and 1 million bitstrings for 17.4 hours after calibration. In between these measurements, we measured the fidelity of other 53-qubit circuits with 16 to 20 cycles. The analyzed results are shown in Fig. S39. The statistical uncertainties of the fidelities are estimated to be 1.29×10^{-4}, as indicated by the error bars.

We repeated the stability measurements twice, with different circuits and on different days. Fig. S39 shows the one that exhibits greater degradation as a conservative estimate of the effect. The measurement indicates a degradation of fidelity within the range of time. A linear fit with $F = p_0 + p_1 t$ results in estimated parameters $\hat{p}_0 = (5.51 \pm 0.055) \times 10^{-3}$, $\hat{p}_1 = (-6.87 \pm 0.64) \times 10^{-5}$, and a correlation coefficient of $\hat{p}_0$ and $\hat{p}_1$, ρ, to be -0.76. The χ^2 per degree of freedom is 26.3/11.

The p-value for the χ^2 for 11 degrees of freedom is 0.0058, indicating that it is not a very good fit. Because the correctness of the estimates of statistical uncertainties has been verified in Section 11.8.7, this is attributed to systematic fluctuation in addition to degradation. It is supported by the larger variance of fidelity than the 1σ band in Fig. S39.

The 1σ band depends on the statistical uncertainties of fidelities and the variance of time on the x-axis, but is independent of the variance of fidelity. To take the variance of fidelity into account, we use the variance of the residuals of the linear fit as an estimator of the variance of fidelity. The standard deviation of residuals is estimated to be 1.84×10^{-4}, which is added to σ_{p_0} in quadrature to be the total σ_{p_0}. The estimate is total $\sigma_{p_0} = 1.92 \times 10^{-4}$, 3.5 times larger than the statistical-only σ_{p_0} of 5.5×10^{-5}.

The uncertainty on a fidelity measured at time t can be estimated by the standard error propagation, assuming that t is uncorrelated with either p_0 or p_1.

$$\sigma_F = \left[\sigma_{p_0}^2 + 2t\sigma_{p_0}\sigma_{p_1}\rho + \sigma_{p_1}^2 t^2\right]^{1/2} \tag{11.80}$$

The value of σ_F as well as the ratio σ_F/F in the range of measured fidelities monotonically decreases. We take $\max(\sigma_F/F)$ as the estimate of relative systematic uncertainty for fidelities measured in the same run. The value is found to be 4.4% and is used in subsequent analysis.

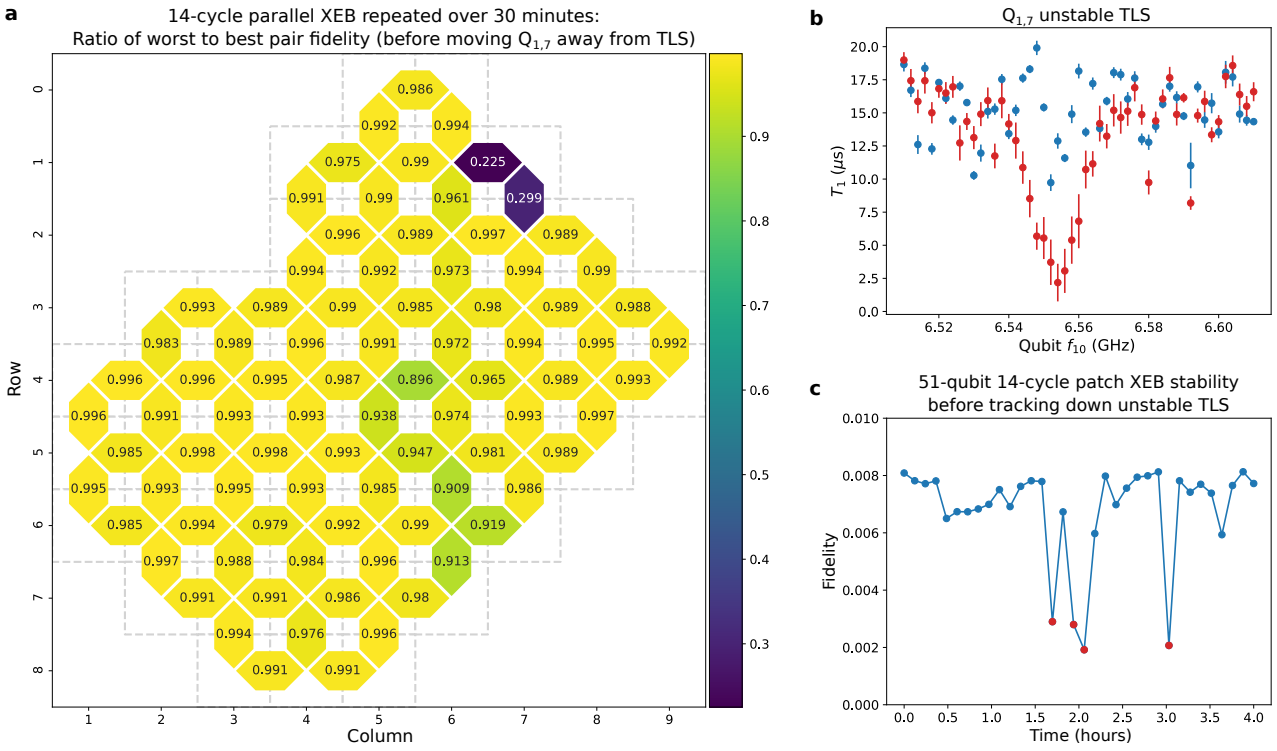


Figure S40: **Identifying sources of fluctuations with repetitive per-layer simultaneous pair XEB. a,** Per-pair ratio of worst fidelity to best fidelity measured via per-layer simultaneous pair XEB at a depth of 14 cycles over the course of 30 minutes. During this time, fluctuations were dominated by a single TLS. **b,** Measured qubit T_1 vs. f_{10} for $Q_{1,7}$ at two different times a few minutes apart (red vs. blue points), showing an unstable TLS that was dominating the fluctuations in full system fidelity seen in **c,**. Moving $Q_{1,7}$ far from this TLS led to the stability seen in Fig. S39.

The physical origin of the observed system fluctuations can be attributed to many possible channels: $1/f$ flux noise, qubit T_1 fluctuations, control signal drift, etc. We speculate that the dominant mechanism is the moderate interaction between a small number of TLS's and a few qubits at their idling and/or readout biases. In Fig. S40a, we show the result of measuring per-layer simultaneous pair XEB at a fixed depth of 14 cycles repeatedly over time. The quantity plotted is the ratio of the worst pair fidelity to best fidelity observed over the course of 30 minutes. This type of repetitive measurement allows us to pinpoint which pairs dominate the fluctuations in full system fidelity. Note that because we used fidelity at a fixed cycle depth rather than the one extracted from the exponential decay, these numbers contain the effect of fluctuating measurement fidelity as well.

As shown in Fig. S40a, the depth-14 fidelity of most pairs fluctuates downward by only $\sim$1% at depth 14, which translates to either a $\sim$1% fluctuation in measurement fidelity for a pair, or a $\sim$0.08% fluctuation in the two-qubit gate fidelity for a pair. Before finding the unstable TLS defect in Fig. S40b, a single qubit dominated the fluctuations in full system fidelity seen in Fig. S40c. After we moved this problematic qubit far from the fluctuating TLS, the fluctuations in fidelity during the actual quantum supremacy experiment (Fig. S39) were dominated by a handful of pairs containing qubits in the "degenerate" readout region (described in section 11.6). For these qubits, due to constraints from readout crosstalk we had little freedom in what readout detunings we could choose, and so the best we could do was to put some qubits near defects or transmon-resonator transition modes during readout. We speculate that this is where the remaining dominant fluctuations originate.

11.8.9 The fidelity result and the null hypothesis on quantum supremacy

We use the mean fidelity of ten 53-qubit 20-cycle circuits as the final benchmark of the system. In section 11.8.7 we estimated the fidelity and statistical uncertainty to be $(2.24 \pm 0.18) \times 10^{-3}$ using the linear cross entropy. In section 11.8.8 we estimated the relative systematic uncertainty due to drift to be 4.4%. Combining these 2 estimations we arrive at the final fidelity as $(2.24 \pm 0.10(\text{syst.}) \pm 0.18(\text{stat.})) \times 10^{-3}$. Fidelity estimates with statistical and systematic uncertainty for other quantum circuits are shown in Figure S41.

As we show in section 11.10, a noisy sampling of a random quantum circuit at fidelity $F = 10^{-3}$ requires 5000 years with a classical computer with CPU power equivalent to 1 million cores, and it scales linearly with fidelity F. It takes a quantum computer less than an hour to complete the same noisy sampling. Therefore we form the null hypothesis that the fidelity of the quantum computer is $F \leq 10^{-3}$, and the alternative hypothesis that $F > 10^{-3}$. If the alternative hypothesis is true, we can say that a classical computer can not perform the same noisy sampling task as the quantum computer.

The total uncertainty on fidelity is estimated with addition in quadrature of systematic uncertainty and statistical uncertainty. The mean fidelity of 10 random circuits with 53 qubits and 20 cycles is $(2.24 \pm 0.21) \times 10^{-3}$. The null hypothesis is therefore rejected with a significance of 6σ.

While our analysis of the uncertainty in $\mathcal{F}_{\text{XEB}}$ was computed from both statistical and systematic errors, some care should be taken in the consideration of systematic errors as they pertain to the claim of quantum supremacy. Systematic errors should be included if we wish to use the XEB fidelity value, for example comparing fidelities of patch, elided and full circuits. However for quantum supremacy, a false claim would arise if $\mathcal{F}_{\text{XEB}}$ was zero, but we obtained a non-zero value because of a fluctuation. Systematic fluctuations produce a change in magnitude of XEB, as seen in the data in this section, which is thus a multiplicative-type error that does not change the XEB fidelity value when it is zero. A false positive is only produced by a additive-

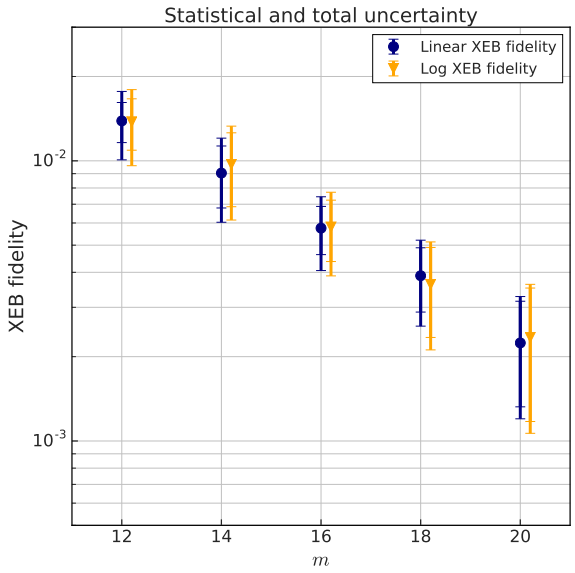


Figure S41: Statistical and total uncertainty of fidelity estimates produced by the linear XEB and logarithmic XEB from ten random quantum circuits with 53 qubits and m cycles. The inner error bars represent the statistical uncertainty discussed in section 11.8.7. The outer error bars represent the total uncertainty discussed in section 11.8.8.

type statistical fluctuations and thus it is the only mechanism that should be considered when computing the uncertainty. Therefore, the 6σ significance of our claim should be considered as conservative.

Some skeptics have warned that a quantum computer may not be possible [65, 66], for example due to the fragility of quantum information at large qubit number and exponentially large Hilbert space. The demonstration here of quantum behavior at 10^{16} Hilbert space is strong confirmation that nothing unusual or unexpected happens to our current understanding of quantum mechanics at this scale.

11.9 Sensitivity of XEB to errors

An important requirement for a procedure used to evaluate quantum processors, such as XEB, is sensitivity to errors. Qubit amplitudes are complex variables and therefore quantum errors are inherently continuous. Nevertheless, they can be given a discrete description, for example in the form of a finite set of Pauli operators. The digital error model is used for instance in quantum error correction where errors are discretized by syndrome extraction. In this section we examine the impact of both discrete and continuous errors on the fidelity estimate obtained from the XEB algorithm.

The XEB procedure uses a set of random quantum circuits $\mathcal{U} = \{U_1, \ldots, U_S\}$ with n qubits and m cycles. Every circuit is executed N_s times on the quantum processor under test. Each execution of the circuit U_j applies the quantum operation Λ_j, which is an imperfect realization of U_j, to the input state $|0\rangle\langle 0|$. The result of the experiment is a set $\mathcal{B}$ of SN_s bitstrings $q_{i,j}$ sampled from the distributions $p_e(q_{i,j}) = \langle q_{i,j}| \rho_j |q_{i,j}\rangle$ where $\rho_j = \Lambda_j(|0\rangle\langle 0|)$ is the output state in the experiments with circuit U_j. For each bitstring $q_{i,j}$, a simulator computes the ideal probability $p_s(q_{i,j}) = |\langle q_{i,j}|\psi_j\rangle|^2$ where $|\psi_j\rangle = U_j|0\rangle$ is the ideal output state of the circuit U_j. Finally, XEB uses Eq. (11.27) or (11.28) to compute an estimate $\mathcal{F}_{\text{XEB}}(\mathcal{B},\mathcal{U})$ of fidelity $F(|\psi_j\rangle\langle\psi_j|, \rho_j) = \langle\psi_j|\rho_j|\psi_j\rangle$ averaged over circuits $\mathcal{U}$. The result quantifies how well the

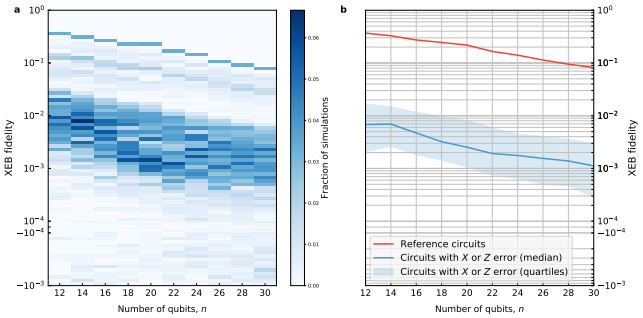


Figure S42: **Impact of one single-qubit Pauli error on fidelity estimate from XEB. a,** Distributions of fidelity estimates from XEB using measured bitstrings and quantum circuits with one bit-flip or one phase-flip error. For each n, shades of blue represent the normalized histogram of the estimates obtained for the error gate placed at different circuit locations. The highest fidelity estimates correspond to phase-flip errors immediately preceding measurement and are equal to the fidelity estimates from XEB using error-free circuits. **b,** Quartiles of the distributions shown in **a** (blue) compared to the fidelity estimates from XEB using measured bitstrings and unmodified quantum circuits (red). Both plots use linear scale between 10^{-4} and -10^{-4} and logarithmic scale everywhere else.

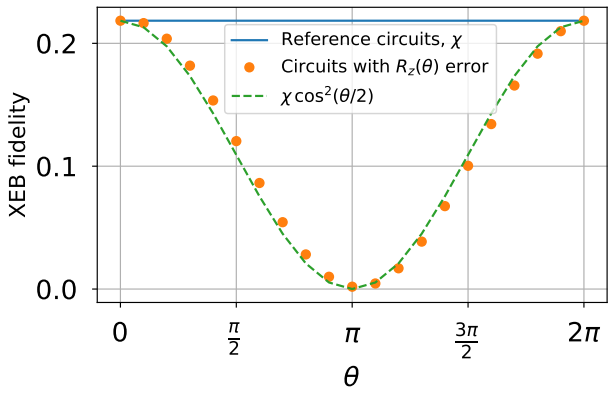


Figure S43: **Impact of the $R_z(\theta)$ error on XEB.** Fidelity estimates computed by XEB from measured bitstrings and circuits with $n = 20$ qubits and $m = 14$ cycles modified to include $R_z(\theta)$ error applied in 10th cycle to one of the qubits as a function of θ (orange dots). Also shown is XEB fidelity computed using the same bitstrings and unmodified circuits (blue solid line) and a simple model which predicts the effect of the error (green dashed line).

quantum processor is able to realize quantum circuits of size n and depth m. See section 11.4 for more details on XEB.

The estimate $\mathcal{F}_{\rm XEB}(\mathcal{B},\mathcal{U})$ is a function of bistrings $\mathcal{B}$ obtained in experiment and of the set of quantum circuits $\mathcal{U}$ used to compute ideal probabilities. This enables a test of the sensitivity of the method to errors by replacing the error-free reference circuits $\mathcal{U} = \{U_1, \ldots, U_S\}$ with circuits $\mathcal{U}_E = \{U_{1,E}, \ldots, U_{S,E}\}$ where $U_{j,E}$ is the quantum circuit obtained from U_j by the insertion at a particular location in the circuit of a gate E representing the error. We identify errors inserted at different circuit locations that lead to the same output distribution since XEB cannot differentiate between them.

We first consider the impact of a discrete single-qubit Pauli error E placed in a random location in the circuit. In Fig. S42 we plot $\mathcal{F}_{\rm XEB}(\mathcal{B},\mathcal{U}_E)$ where $\mathcal{B}$ are bitstrings observed in our experiment and $\mathcal{U}_E$ are quantum circuits modified by the insertion of an additional X or Z gate following an existing single-qubit gate. Each fidelity estimate corresponds to a different circuit location where the error gate has been inserted. For every n, the highest fidelity values correspond to the insertion of the Z gate in the final cycle of the circuit. They have no impact on measurements and thus are equivalent to absence of error. The corresponding fidelity estimates match the estimates for the unmodified circuits.

The probability of only seeing the error E is approximately $q = ep$ where e is the probability of E arising at the particular circuit location and p is the probability that no other error occurs. The fraction q of executions realize circuit $U_{j,E} \in \mathcal{U}_E$ yielding bitstrings $\mathcal{B}_E$ while the remaining fraction $1-q$ yield bitstrings $\mathcal{B}_*$. XEB averages over circuit executions, so

$$\mathcal{F}_{\rm XEB}(\mathcal{B},\mathcal{U}_E) = q\,\mathcal{F}_{\rm XEB}(\mathcal{B}_E,\mathcal{U}_E) + (1-q)\,\mathcal{F}_{\rm XEB}(\mathcal{B}_*,\mathcal{U}_E). \quad (11.81)$$

Since bitstrings $\mathcal{B}_E$ originated in a perfect realization of $\mathcal{U}_E$ we have $\mathcal{F}_{\rm XEB}(\mathcal{B}_E,\mathcal{U}_E) \simeq 1$ with high probability. Also, assuming the circuits randomize the output quantum state sufficiently, we have $\mathcal{F}_{\rm XEB}(\mathcal{B}_*,\mathcal{U}_E) \simeq 1/\sqrt{D}$, where $D = 2^n$, see Eq. (11.25) and Fig. S7. Therefore, for large n

$$\mathcal{F}_{\rm XEB}(\mathcal{B},\mathcal{U}_E) \simeq q + \frac{1-q}{\sqrt{D}} \simeq q \quad (11.82)$$

with high probability.

Now, the probability p that no error other than E occurs is approximately equal to the experimental fidelity F which is approximated by $\mathcal{F}_{\rm XEB}(\mathcal{B},\mathcal{U})$, so

$$\mathcal{F}_{\rm XEB}(\mathcal{B},\mathcal{U}_E) \simeq e\,\mathcal{F}_{\rm XEB}(\mathcal{B},\mathcal{U}) \quad (11.83)$$

which means that XEB result obtained using circuits modified to include E is approximately proportional to the XEB result obtained using the error-free reference circuits. Moreover, the ratio of the two XEB results is approximately equal to the probability of E.

The data in Fig. S42 agrees with the approximate proportionality in Eq. (11.83) and allows us to estimate the median probability of a Pauli error. Based on the drop in XEB fidelity estimate by a factor of almost 100 due to the insertion of one single-qubit Pauli error into the circuit, the probability is on the order of 1%. While more work on the gate failure model needs to be done to correctly relate Sycamore gate error rates to the probability of specific Pauli errors, we already see that e has the same order of magnitude as our per cycle and per qubit error given by $e_{2c}/2 \simeq 0.5\%$, see Table 12. A possible resolution of the factor of two discrepancy may lie in the fact that more than one gate failure can manifest itself as a particular Pauli error E in a particular circuit location.

Lastly, we consider the impact of continuous errors on XEB result. Fig. S43 shows the fidelity estimate obtained from XEB using bitstrings observed in our experiment and quantum circuits modified to include a single rotation $R_Z(\theta)$. The middle point of the plot is equal to the fidelity estimate obtained for one of the discrete errors in Fig. S42 whereas the leftmost and rightmost points correspond to the fidelity estimate obtained from XEB using the error-free reference circuit.

The analysis above illustrates how questions about the behavior and performance of quantum processors can be formulated in terms of modifications to the reference quantum circuits and how XEB can help investigate these questions. While XEB has proven itself a powerful tool for calibration and performance evaluation (see sections 11.6 and 11.8), more work is required to assess its efficacy as a diagnostic tool for quantum processors.

11.10 Classical simulations

11.10.1 Local Schrödinger and Schrödinger-Feynman simulators

We have developed two quantum circuit simulators: qsim and qsimh. The first simulator, qsim, is a Schrödinger full state vector simulator. It computes all 2^n amplitudes, where n is the number of qubits. Essentially, the simulator performs matrix-vector multiplications repeatedly. One matrix-vector multiplication corresponds to applying one gate. For a 2-qubit gate acting on qubits `q1` and `q2` (`q1` < `q2`), it can be depicted schematically by the following pseudocode.

```
#iterate over all values of qubits q > q2
for (int i = 0; i < 2^n; i += 2 * 2^q2) {
  #iterate values for q1 < q < q2
  for (int j = 0; j < 2^q2; j += 2 * 2^q1) {
    #iterate values for q < q1
    for (int k = 0; k < 2^q1; k += 1) {
      #apply gate for fixed values
      #for all q not in [q1,q2]
      int l = i + j + k;

      float v0[4]; #gate input
      float v1[4]; #gate output

      #copy input
      v0[0] = v[l];
      v0[1] = v[l + 2^q1];
      v0[2] = v[l + 2^q2];
      v0[3] = v[l + 2^q1 + 2^q2];

      #apply gate
      for (r = 0; r < 4; r += 1) {
        v1[r] = 0;
        for (s = 0; s < 4; s += 1) {
          v1[r] += U[r][s] * v0[s];
        }
      }

      #copy output
      v[l] = v1[0];
```

qubits, n	run time in seconds
32	111
34	473
36	1954
38	8213

Table 16: Circuit simulation run times using qsim on a single Google cloud node (n1-ultramem-160).

```
      v[l + 2^q1] = v1[1];
      v[l + 2^q2] = v1[2];
      v[l + 2^q1 + 2^q2] = v1[3];
    }
  }
}
```

Here `U` is a 4x4 gate matrix and `v` is the full state vector. To make the simulator faster, we use gate fusion [67], single precision arithmetic, AVX/FMA instructions for vectorization, and OpenMP for multi-threading. We are able to simulate 38-qubit circuits on a single Google cloud node that has 3844 GB memory and four CPUs with 20 cores each (n1-ultramem-160). The run times for different circuit sizes at depth 14 are listed in Table **??**.

The second simulator, qsimh, is a hybrid Schrödinger-Feynman algorithm (SFA) simulator [38]. We cut the lattice into two parts and use the Schmidt decomposition for the 2-qubit gates on the cut. If the Schmidt rank of each gate is r and the number of gates on the cut is g then there are r^g paths, corresponding to all the possible choices of Schmidt terms for each 2-qubit gate across the cut. To obtain fidelity equal to unity, we need to simulate all the r^g paths and sum the results. The total run time is proportional to $(2^{n_1} + 2^{n_2})r^g$, where n_1 and n_2 are the qubit numbers in the first and second parts. Each part is simulated by qsim using the Schrödinger algorithm. Path simulations are independent of each other and can be trivially parallelized to run on supercomputers or in data centers. Note that one can run simulations with fidelity $F < 1$ just by summing over a fraction F of all the paths (see Ref. [38] and Sec. 11.10.4). In order to speed up the computation, we save a copy of the state after the first p 2-qubit gates across the cut, so the remaining r^{g-p} paths can be computed without re-starting the simulation from the beginning. We call the specific choice of Schmidt terms for the first p gates in the cut a *prefix*.

11.10.2 Feynman simulator

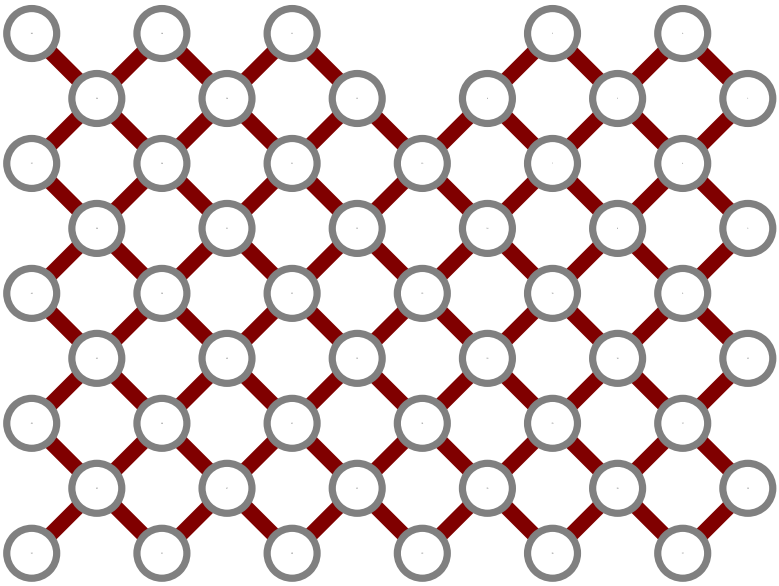
qFlex was introduced in Ref. [50] and later adapted to GPU architectures in Ref. [68] to allow efficient computation on Summit, currently the world's Top-1 supercomputer. qFlex is open source and available at https://github.com/ngnrsaa/qflex. Given a random quantum circuit, qFlex computes output bitstring amplitudes by adding all the Feynman path contributions via tensor network (TN) contractions [69, 70], and so it follows what we call a Feynman approach (FA) to circuit sampling. TN simulators are known to outperform all other methods for circuits with low depth or a large number of qubits (*e.g.*, Ref. [68] successfully simulates 121 qubits at low depth using this technique), as well as for small sample sizes (N_s), since simulation cost scales linearly with N_s.

TN simulators compute one amplitude (or a few amplitudes; see below) per contraction of the entire network. In order to sample bitstrings for a given circuit, a set of random output bitstrings is chosen before the computation starts. Then, the amplitudes for these bitstrings are

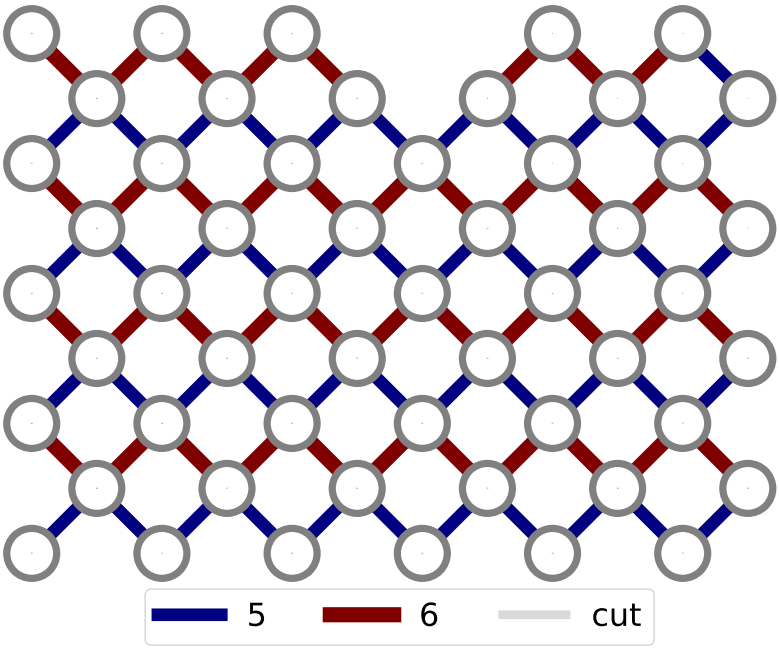
						PFlop/s*		efficiency (%)		
qubits	**cycles**	$\mathcal{F}_{\mathbf{XEB}}$ (%)	N_s	**nodes**	**runtime**	**peak**	**sust.**	**peak**	**sust.**	**power**
53	12	0.5	1M	4550	1.29 hours	235.2	111.7	57.4	27.3	5
		1.4	0.5M		1.81 hours**					
		1.4	3M		10.8 hours**					
	14	2.22×10^{-6}	1M		0.72 hours	347.5	252.3	84.8	61.6	7
		0.5	1M		67.7 days**					
		1.0	0.5M		67.7 days**					
		1.0	3M		1.11 years**					

Table 17: **Runtimes, efficiency and energy consumption for the simulation of random circuit sampling of N_s bitstrings from Sycamore with fidelity $\mathcal{F}$ using qFlex on Summit**. Simulations used 4550 nodes out of 4608, which represents about 99% of Summit. Single batches of 64 amplitudes were computed on each MPI task using a socket with three GPUs (two sockets per node); given that one of the 9100 MPI tasks acts as master, 9099 batches of amplitudes were computed. For the circuit with 12 cycles, 144/256 paths for these batches were computed in 1.29 hours, which leads to the sampling of about 1M bitstrings with fidelity $\mathcal{F} \approx 0.5\%$ (see Ref. [50] for details on the sampling procedure); runtimes and energy consumption for other sample sizes and fidelities are extrapolated linearly in N_s and $\mathcal{F}$ from this run. At 14 cycles, 128/524288 paths were computed in 0.72 hours, which leads to the sampling of about 1M bitstrings with fidelity 2.22×10^{-6}. In this case, one would need to consider 288101 paths on all 9099 batches in order to sample about 1M (0.5M) bitstrings with fidelity $\mathcal{F} \approx 0.5\%$ (1.0%). By extrapolation, we estimate that such computations would take 1625 hours (68 days). For N_s =3M bitstrings and $\mathcal{F} \approx 1.0\%$, extrapolation gives us an estimated runtime of 1.1 years. Performance is higher for the simulation with 14 cycles, due to higher arithmetic intensity tensor contractions. Power consumption is also larger in this case. Job, MPI, and TAL-SH library initialization and shutdown times, as well as initial and final IO times are not considered in the runtime, but they are in the total energy consumption. *Single precision. **Extrapolated from the simulation with a fractional fidelity.

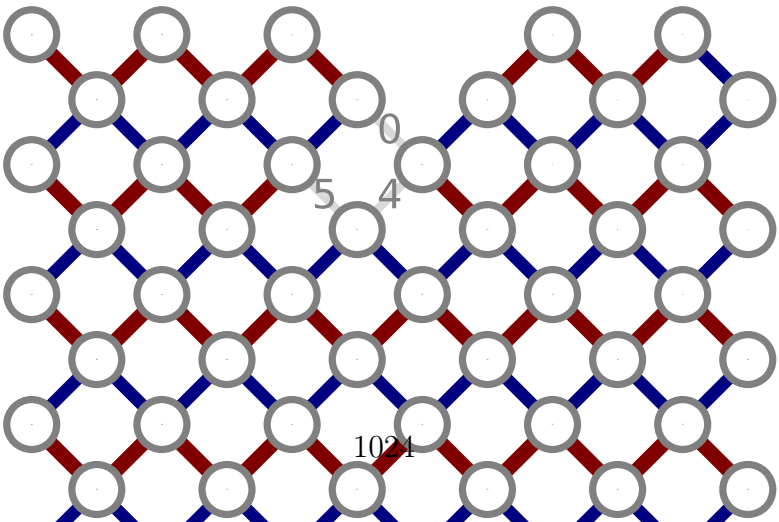
Raw circuit

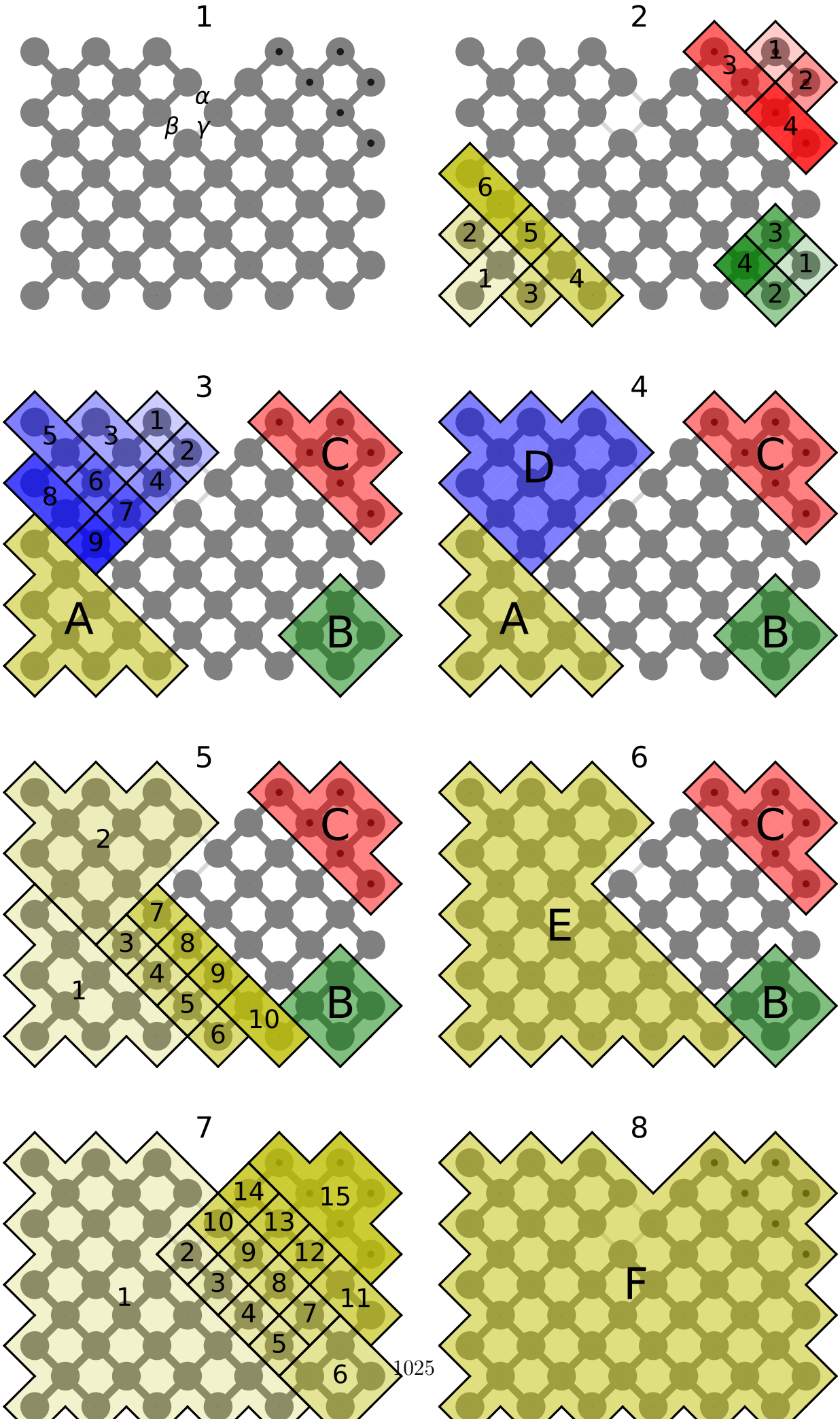


SWAP-cphase transformation



SWAP-cphase transformation & cuts




1
α
β γ
2
3
1
2
4
6
2
5
1
3
4
3
4
1
2
3
5
3
1
2
6
4
8
7
9
C
A
B
4
D
C
A
B
5
2
C
7
3
8
4
9
1
5
10
6
B
6
C
E
B
7
14
15
10
13
2
9
12
3
8
11
1
4
7
5
6
8
F

computed and either accepted or rejected using *frugal rejection sampling* [38]. This ensures that the selected subset of bitstrings is indistinguishable from bitstrings sampled from a quantum computer. The cost of the TN simulation is therefore linear in the number of output bitstrings. This makes TN methods more competitive for small sets of output bitstrings.

The optimization of qFlex considers a large number of factors to achieve the best time-to-solution on current supercomputers, an approach that often diverges from purely theoretical considerations on the complexity of TN contractions. More precisely, qFlex implements several features such as:

- **Avoidance of distributed tensor contractions:** by "cutting" the TN (slicing some indexes), the contraction of the TN is decomposed into many *paths* that can be contracted locally and independently, therefore avoiding internode communication, which is the main cause for the slowdown of distributed tensor contractions.
- **Contraction orderings for high arithmetic intensity:** TN contraction orderings are chosen so that the expensive part of the computation consists of a small number of tensor contractions with high arithmetic intensity. This lowers the time-to-solution.
- **Highly efficient tensor contractions on GPU:** the back-end TAL-SH library [71] provides fully asynchronous execution of tensor operations on GPU and fast tensor transposition, allowing out-of-core tensor contractions for instances that exceed GPU memory. This achieves very high efficiency (see Table 17) on high arithmetic intensity contractions.

In addition, qFlex implements two techniques in order to lower the cost of the simulation:

- **Noisy simulation:** the cost of a simulation of fidelity $\mathcal{F} < 1$ ($\mathcal{F} \approx 5 \times 10^{-3}$ in practice) is lowered by a factor $1/\mathcal{F}$, *i.e.*, is linear in $\mathcal{F}$ [38, 50].
- **Fast sampling technique:** the overhead in applying the frugal rejection sampling mentioned above is removed by this technique, giving an order of magnitude speedup [50]. This involves the computation of the amplitudes of a few correlated bitstrings (*batch*) per circuit TN contraction.

As shown in Table 17, qFlex is successful in simulating Sycamore with 12 cycles on Summit, sampling 1M bitstrings with fidelity close to 0.5% in 1.29 hours. At 14 cycles, we perform a partial simulation and extrapolate the simulation time for the sampling of 1M bitstrings with fidelity close to 0.5% using Summit, giving an estimated 68 days to complete the task. Sampling 3M bitstrings at 14 cycles with fidelity close to 1.0% (average experimentally realized fidelity) would take an estimated 1.1 years to complete. Other estimates for different sample sizes and fidelities can be found in Table 17. At 16 cycles and beyond, however, the enormous amount of Feynman paths required so that the computation does not exceed the 512 GB of RAM of each Summit node makes the computation impractical.

The contraction of the TNs involved in the computation of amplitudes from Sycamore using qFlex is preceded by a simplification of the circuits, which allows us to decrease the bond (index) dimension of some of the indexes of the TN. This comes from the realization that $\mathrm{fSim}(\theta = \pi/2, \phi) = -i \cdot [\mathrm{R_z}(-\pi/2) \otimes \mathrm{R_z}(-\pi/2)] \cdot \mathrm{cphase}(\pi + \phi) \cdot \mathrm{SWAP}$ (see Sections 11.6 and 11.7.5); note that the SWAP gate can be applied either at the beginning or at the end of the sequence. We apply this transformation to all fSim gates at the beginning (end) of the circuit that affect qubits that are not affected by any other two-qubit gate before (after) in the circuit. The SWAP is then applied to the input (output) qubits and their respective one-qubit gates trivially, and the bond dimension remaining from this gate is 2, corresponding

to the cphase gate, as opposed to the bond dimension 4 of the original fSim gate. Note that in practice this identity is only approximate, since $\theta \approx \pi/2$; we find that transforming all gates described above causes a drop in fidelity to about 95%.

After the above simplification is applied, we proceed to cut (slice) some of the indexes of the TN (see Ref. [50] for details). The size of the slice of the index involved in each cut (the effective bond dimension of the index) is variable, and is chosen differently for different number of cycles on the circuit. Cutting indexes decomposes the contraction of the TN into several simpler contractions, whose results are summed after computing them independently on different nodes of the supercomputer.

Fig. S44 shows the bond dimensions of the TN corresponding to the circuits with 12 and 14 cycles simulated. We can see the decrease in bond dimension after the fSim simplification is applied, as well as the remaining bond dimension on the indexes cut for each case.

Finally, we contract the tensor network corresponding to the computation of a set of amplitudes (for fast sampling) for a particular batch of output bitstrings. The contraction ordering, which is chosen (together with the size and position of the cuts) in order to minimize the time-to-solution of the computation (which involves a careful consideration of the memory resources used and the efficiency achieved on the GPUs) is shown in Fig. S45. The computation can be summarized in the following pseudo-code, where α, β, and γ are variables that denote the different instances of the cuts:

```
# Qubits on C are used for fast sampling.
# size_of_batch amps. per circuit contraction.
size_of_batch = 2^num_qubits(C)

# Placeholder for all amplitudes in the batch.
batch_of_amplitudes = zeros(size_of_batch)

# Start contracting...
contract(A)  # Panel 2
contract(B)  # Panel 2
contract(C)  # Panel 2

# alpha labels instances of 1st cut
for each alpha {

    # beta labels instances of 2nd cut
    for each beta {
        contract(D)  # Panels 3 & 4
        contract(E)  # Panels 5 & 6

        # gamma labels instances of 3rd cut
        for each gamma {
            contract(F)  # Panels 7 & 8

            # Add contribution from this
            # path (alpha, beta, gamma).
            batch_of_amplitudes += F
        }
    }
}
```

Dotted qubits on Fig. S45 denote the region used for fast sampling, where output indexes are

left open. The circuit TN contraction leads to the computation of 64 amplitudes of correlated bitstrings (tensor F). Note that computing only a fraction $\mathcal{F}$ of the paths results in amplitudes with a fidelity roughly equal to $\mathcal{F}$. Computing a set of perfect fidelity batches of amplitudes, where the number of batches is smaller than the number of bitstrings to sample also provides a similar fidelity $\mathcal{F}$ in the sampling task, where $\mathcal{F}$ is equal to the ratio of the number of batches to the number of bitstrings in the sample. A hybrid approach (fraction of batches, each only with a fraction of paths), which we use in practice, also provides a similar sampling fidelity. See Refs. [38, 50] and Section 11.10.1 for more details.

A new feature of qFlex, implemented for this work, is the possibility to perform out-of-core tensor contractions (of tensors that exceed GPU memory) over more than one GPU on the same node. Although the arithmetic intensity requirements to achieve high efficiency are now higher (about an arithmetic intensity of 3000 for an efficiency close to 90% over three GPUs, as opposed to 1000 for a similar efficiency using a single GPU), the fact that a large part of a node is performing a single TN contraction lets us work with larger tensors, which implies reducing the number of cuts, as well as increasing the bond dimension of each cut; this, in turn, achieves better overall time-to-solution for sampling than simulations based on TNs with smaller tensors and with a lower memory footprint during their contraction (which could perhaps show a higher GPU efficiency due to the simultaneous use of each GPU for independent TNs). It is worth noting that the TN contraction ordering presented in Fig. S45 provides us with the best time-to-solution after considering several possibilities for the simulation of sampling from Sycamore using qFlex for both 12 and 14 cycles. This is generally not the case, since different numbers of cycles generate different TNs, which generally have different contraction schemes for best simulation time-to-solution.

Sampling of random circuits on Sycamore is difficult to simulate with TN simulators at 16 cycles and beyond. Indeed, FA simulators suffer from an exponential scaling of runtime with circuit depth. For qFlex, this is manifested in the large size of the tensors involved in the circuit TN contraction (this size grows exponentially with the number of cycles of the circuit), which require a large number of cuts in order not to exceed the RAM of a computation node, and which in turn generates an impractical number of Feynman paths. For other simulators, such as the one presented in Ref. [72], the number of projected variables is expected to be so large that the computation time (which increases exponentially with the number of projected variables) on a state-of-the-art supercomputer makes the computation impractical; see Section 11.10.5 for a detailed analysis. For TN-based simulators that attempt the circuit contraction distributed over several nodes (without cuts) [73], we expect the size of the largest tensor encountered during the TN contraction (which grows exponentially with depth) to exceed the RAM available on any current supercomputer. Not having enough memory for a simulation is the problem that led to developing FA simulators in the first place, for circuits of close to 50 qubits and beyond, for which the Schrödinger simulator (see Section 11.10.3) requires more memory to store the wave function than available. FA simulators give best performance as compared to other methods in situations with a large number of qubits and low depth. For circuits where both the number of qubits and the number of cycles are considered large enough to make the computation expensive, and contribute equally in doing so (formally, each linear dimension of the qubit grid is comparable to the time dimension), like the supremacy circuits considered in this work, we expect SFA of Section 11.10.1 to be the leading approach for sampling from a random circuit, given a large enough sample size ($\sim$ 1M in this work); note the linear dependence of the runtime of FA with sample size, which is absent for SFA.

11.10.3 Supercomputer Schrödinger simulator

We also performed supercomputer Schrödinger simulations in the Jülich Supercomputing Centre. For a comprehensive description of the universal quantum computer simulators JUQCS-E and JUQCS-A, see Refs. [74] and [75].

For a given quantum circuit U designed to generate a random state, JUQCS-E [75] executes U and computes (in double precision floating point) the probability distribution $p_U(j)$ for each output or bitstring $j \in \{0, \ldots, D-1\}$, where $D = 2^n$, n denoting the number of qubits. JUQCS-E can also compute (in double precision floating point) the corresponding distribution function $P_U(k) = \sum_{j=0}^{k} p_U(j)$ and sample bitstrings from it. We denote by $\mathcal{U}$ the set of m states generated by executing the circuit U. A new feature of JUQCS-E, not documented in Ref. [75], allows the user to specify a set $\mathcal{Q}$ of M bitstrings for which JUQCS-E calculates $p_U(j)$ for all $j \in \mathcal{Q}$ and saves them in a file.

Similarly, for the same circuit U, JUQCS-A [75] computes (with adaptive two-byte encoding) the probability distribution $p_A(j)$ for each bitstring $j \in \{0, \ldots, D-1\}$. Although numerical experiments with Shor's algorithm for up to 48 qubits indicate that the results produced by JUQCS-A are sufficiently accurate, there is, in general, no guarantee that $p_A(j) \approx p_U(j)$. In this sense, JUQCS-A can be viewed as an approximate simulator of a quantum computing device.

In principle, sampling states with probabilities $p_A(j)$ requires the knowledge of the distribution function $P_A(k) = \sum_{j=0}^{k} p_A(j)$. If D is large, and $p_A(j) \approx O(1/D)$, as in the case of random states, computing $P_A(k)$ requires the sum over j to be performed with sufficiently high precision. For instance, if $D = 2^{39}$, $p_A(j) \approx O(10^{-12})$ and even with double precision arithmetic (≈ 16 digits), adding $D = 2^{39}$ small numbers requires some care. Note that in practice, each MPI process only calculates a partial sum, which helps to reduce the loss of significant digits. JUQCS-A can compute $P_A(k)$ in double precision and sample bitstrings from it. We denote by $\mathcal{A}$ the set of M bitstrings generated by JUQCS-A after executing the circuit U. Activating this feature requires additional memory, effectively reducing the maximum number of qubits that can be simulated by three. This reduction of the maximum number of qubits might be avoided as follows. In the case at hand, we know that all $p_A(j) \approx O(1/D)$. Then, since $p_A(j)$ is known, one might as well sample the states from a uniform distribution, list the weight $w_A(j) = Np_A(j)$ for each generated state j and use these weights to compute averages. We do not pursue this possibility here because for the present purpose, it is essential to be able to compute $p_U(j)$ and therefore, the maximum number of qubits that can be studied is limited by the amount of memory that JUQCS-E, not JUQCS-A, needs to perform the simulation.

For an XEB comparison, the quantities of interest are

$$\alpha_{U,U} \equiv \log D + \gamma + \sum_{j=0}^{D-1} p_U(j) \log p_U(j), \tag{11.84}$$

$$\alpha_{A,U} \equiv \log D + \gamma + \sum_{j=0}^{D-1} p_A(j) \log p_U(j), \tag{11.85}$$

$$\alpha_{A,A} \equiv \log D + \gamma + \sum_{j=0}^{D-1} p_A(j) \log p_A(j), \tag{11.86}$$

$$\alpha_{\mathcal{X},U} \equiv \log D + \gamma + \frac{1}{M} \sum_{j \in \mathcal{X}} \log p_U(j), \tag{11.87}$$

where $\mathcal{X}$ is one of the four sets $\mathcal{U}$, $\mathcal{A}$, $\mathcal{M}$ (a collection of bitstrings generated by the experiment), or $\mathcal{C}$ (obtained by generating bistrings distributed uniformly). If M is sufficiently large ($M = 500000$ in the case at hand), we may expect that $\alpha_{\mathcal{U},U} \approx \alpha_{U,U}$ and $\alpha_{\mathcal{A},U} \approx \alpha_{A,U}$.

In addition to the cross entropies Eqs. (11.84)–(11.87), we also compute the linear cross entropies

$$\widehat{\alpha}_{U,U} \equiv \sum_{j=0}^{D-1} p_U(j)(Dp_U(j)-1), \tag{11.88}$$

$$\widehat{\alpha}_{A,U} \equiv \sum_{j=0}^{D-1} p_A(j)(Dp_U(j)-1), \tag{11.89}$$

$$\widehat{\alpha}_{A,A} \equiv \sum_{j=0}^{D-1} p_A(j)(Dp_A(j)-1), \tag{11.90}$$

$$\widehat{\alpha}_{\mathcal{X},U} \equiv \frac{1}{M}\sum_{j\in\mathcal{X}}(Dp_U(j)-1). \tag{11.91}$$

Table 18 presents simulation results for the α's defined by Eqs. (11.84)–(11.87) and for the $\widehat{\alpha}$'s defined by Eqs. (11.88)–(11.91), obtained by running JUQCS-E and JUQCS-A on the supercomputers at the Jülich Supercomputer Centre. For testing quantum supremacy using these machines, the maximum number of qubits that a universal quantum computer simulator can handle is 43 (45 on the Sunway TaihuLight at Wuxi China [75]).

The fact that in all cases, $\alpha_{U,U} \approx \alpha_{A,A} \approx 1$ supports the hypothesis that the circuit U, executed by either JUQCS-E or JUQCS-A, produces a Porter-Thomas distribution. The fact that in all cases, $\alpha_{\mathcal{U},U} \approx 1$ supports the theoretical result that replacing the sum over all states by the sum over $M = 500000$ states yields an accurate estimate of the former (see Section 11.4). Although $\alpha_{A,A} \approx 1$ in all cases, using the sample $\mathcal{A}$ generated by JUQCS-A to compute $\alpha_{\mathcal{A},U}$ shows an increasing deviation from one, the deviation becoming larger as the number of qubits increases. In combination with the observation that $\alpha_{A,A} \approx 1$, this suggests that JUQCS-A produces a random state, albeit not the same state as JUQCS-E. Taking into account that JUQCS-A stores the coefficients of each of the basis states as two single-byte numbers and not as two double precision floating point numbers (as JUQCS-E does), this is hardly a surprise.

From Table 18 it is clear that the simulation results for $\alpha_{\mathcal{X},U}$ and $\widehat{\alpha}_{\mathcal{X},U}$ where $\mathcal{X} = \mathcal{A}, \mathcal{M}, \mathcal{C}$ are consistent. The full XEB fidelity estimates $\alpha_{\mathcal{M},U}$ and $\widehat{\alpha}_{\mathcal{M},U}$, that is the values computed with the bitstrings produced by the experiment, are close to the fidelity estimates of the probabilistic model, patch XEB, and elided XEB, as seen in Fig. 4(a) of the main text.

For reference, in Tables 19 and 20 we present some technical information about the supercomputer systems used to perform the simulations reported in this appendix and give some indication of the computer resources used.

11.10.4 Simulation of random circuit sampling with a target fidelity

A classical simulator can leverage the fact that experimental sampling from random circuits occurs at low fidelity $\mathcal{F}_{\text{XEB}}$ by considering only a small fraction of the Feynman paths (see Secs. 11.10.1 and 11.10.2) involved in the simulation [38], which provides speedups of at least a factor of $1/\mathcal{F}_{\text{XEB}}$. This is done by Schmidt decomposing a few two-qubit gates in the circuit and counting only a fraction of their contributing terms (*paths*). A key assumption here is that the different paths result in orthogonal output states, as was studied in Ref. [38] and later in Ref. [50]. In what follows, we argue that, provided the generation of paths through decomposing gates, the Schmidt decomposition is indeed the optimal approach to achieving the largest speedup, *i.e.*, that the fidelity kept by considering only a fraction of paths is largest when keeping the paths with the largest Schmidt coefficient. This is different from proving the optimality of the Schmidt decomposition of a single gate, since here we refer to the fidelity

Table 18: Simulation results for various α's as defined by Eqs. (11.84)–(11.87), obtained by JUQCS-E and JUQCS-A. The results for the $\widehat{\alpha}$'s defined by Eqs. (11.88)–(11.91) are given in parenthesis. The set of bitstrings $\mathcal{M}$ has been obtained from experiments. In the first column, the number in parenthesis is the circuit identification number. Horizontal lines indicate that data is not available (and would require additional simulation runs to obtain it).

qubits	$\alpha_{U,U}$	$\alpha_{A,A}$	$\alpha_{\mathcal{U},U}$	$\alpha_{\mathcal{A},U}$ $(\widehat{\alpha}_{\mathcal{A},U})$	$\alpha_{\mathcal{M},U}$ $(\widehat{\alpha}_{\mathcal{M},U})$	$\alpha_{\mathcal{C},U}$ $(\widehat{\alpha}_{\mathcal{C},U})$
30	1.0000	1.0000	0.9997	0.8824 (0.8826)	0.0708 (0.0711)	+0.0026 (+0.0017)
39(0)	1.0000	1.0000	0.9992	0.4746 (0.4762)	0.0281 (0.0261)	−0.0003 (−0.0011)
39(1)	1.0000	1.0000	1.0002	—; (—)	0.0350 (0.0362)	—; (—)
39(2)	1.0000	1.0000	0.9996	—; (—)	0.0351 (0.0332)	—; (—)
39(3)	1.0000	1.0000	0.9999	—; (—)	0.0375 (0.0355)	—; (—)
42(0)	1.0000	1.0001	0.9998	0.4264 (0.4268)	0.0287 (0.0258)	−0.0024 (−0.0001)
42(1)	1.0000	1.0000	1.0027	—; (—)	0.0254 (0.0273)	—; (—)
43(0)	1.0000	1.0001	1.0013	0.3807 (0.3784)	0.0182 (0.0177)	−0.0010 (−0.0003)
43(1)	1.0000	1.0000	—	—; (—)	0.0217 (0.0204)	—; (—)

Table 19: Specification of the computer systems at the Jülich Supercomputing Centre used to perform all simulations reported in this appendix. The row "maximum # qubits" gives the maximum number of qubits n that JUQCS-E (JUQCS-A) can simulate on a specific computer.

Supercomputer	JURECA-CLUSTER [76]	JURECA-BOOSTER [76]	JUWEL
CPU	Intel Xeon E5-2680 v3 Haswell	Intel Xeon Phi 7250-F Knights Landing	Dual Inte Platinun
Peak performance	1.8 PFlop/s	5 PFlop/s	10.4 PF
Clock frequency	2.5 GHz	1.4 GHz	2.7 G
Memory/node	128 GB	96 GB + 16 GB (MCDRAM)	96 G
# cores/node	2×12	64	$2 \times$
# threads/core used	1	1	3
maximum # nodes used	256	512	204
maximum # MPI processes used	4096	32768	327
maximum # qubits	40 (43)	41 (44)	43 (

Table 20: Representative elapsed times and number of MPI processes used to perform simulations with JUQCS-E and JUQCS-A on the supercomputer indicated. Note that the elapsed times may fluctuate significantly depending on the load of the machine/network.

		JUQCS-E			JUQCS-A	
qubits	gates	Supercomputer	MPI processes	Elapsed time	Supercomputer	MPI processes
30	614	BOOSTER	128	0:02:28	CLUSTER	128
39	802	CLUSTER	4096	0:42:51	CLUSTER	4096
42	864	JUWELS	16384	0:51:16	JUWELS	8192
43	886	JUWELS	32768	1:01:53	JUWELS	32768

of the entire output state, and decomposed gates are embedded in a much larger circuit. In addition, we show that, for the two-qubit gates used in this work, the speedup is very close to linear in $\mathcal{F}_{\rm XEB}$ (and not much larger), since their Schmidt spectrum is close to flat. We close this section by relating the present discussion to Section 11.7.7, where the formation of simplifiable gate patterns in some two-qubit gate tilings of the circuit is introduced.

In summary, this section provides a method to simulate approximate sampling with a classical computational cost proportional to $\mathcal{F}_{\rm XEB}$. Sec. 11.11 argues, based on complexity theory, that this scaling is optimal. We note that Refs [78, 79, 80] propose an alternative method to approximately sample the output distribution at low fidelity. In essence, this method relies on the observation that, for some noise models, the high weight Fourier components of the noisy output distribution decay exponentially to 0. Then this method proposes to estimate low weight Fourier components with an additive error which is polynomial in the computational cost. Nevertheless, Ref. [81] shows that all Fourier components of the output distribution of random circuits are exponentially small, and therefore they can not be estimated in polynomial time with this method. The conclusion is then that the noisy output distribution can be approximated by sampling bitstrings uniformly at random, the distribution for which all Fourier components are 0. This is consistent with Ref. [27] and Secs. 11.4 and 11.8.5, but it will produce a sample with $\mathcal{F}_{\rm XEB} = 0$, while the output of the experimental samples at 53 qubits and $m = 20$ still has $\mathcal{F}_{\rm XEB} \geq 0.1\%$

Optimality of the Schmidt decomposition for gates embedded in a random circuit

Consider a two-qubit gate V_{ab} acting on qubits a and b. We would like to replace it by a tensor product operator $M_a \otimes N_b$. The final state of the ideal circuit is

$$|\psi\rangle := U_2 V_{ab} U_1 |0^n\rangle \tag{11.92}$$

where $U_1(U_2)$ is a unitary composed by all the gates applied before (after) V_{ab}. The final normalized state of the circuit with the replacement by $M_a \otimes N_b$ is

$$|\phi_{M,N}\rangle := U_2(M_a \otimes N_b)U_1|0^n\rangle / \|U_2(M_a \otimes N_b)U_1|0^n\rangle\|. \tag{11.93}$$

We would like to find M, N which maximize the fidelity of the two states, given by

$$\langle\psi|\phi_{M,N}\rangle = \langle 0^n|U_1^\dagger V_{ab}^\dagger|\beta\rangle / \sqrt{\langle\beta|\beta\rangle}, \tag{11.94}$$

where

$$|\beta\rangle \equiv (M_a \otimes N_b)U_1|0^n\rangle \tag{11.95}$$

As the overlap is invariant if we multiply $(M_a \otimes N_b)$ by a constant, we fix the normalization $\mathrm{tr}[(M_a \otimes N_b)^\dagger (M_a \otimes N_b)] = 1$.

We now make the assumption that the circuit is random (or sufficiently scrambling) and that the V_{ab} is a gate placed sufficiently in the middle of the computation that the reduced density matrix of qubits a and b of $U_1|0^n\rangle$ shows maximal mixing between the two. In more detail, let

$$\varepsilon := \left\| \mathrm{tr}_{\setminus(a,b)}(U_1|0^n\rangle\langle 0^n|U_1^\dagger) - \frac{I}{4} \right\|_2, \tag{11.96}$$

with $\|X\|_2 := \mathrm{tr}(X^\dagger X)^{1/2}$ the Hilbert-Schmidt norm and $\mathrm{tr}_{\setminus(a,b)}$ the partial trace of all qubits except a and b.

Using Eq. (11.96) and Eq. (11.94), we find

$$\begin{aligned} \langle\psi|\phi_{M,N}\rangle &= \mathrm{tr}(\mathrm{tr}_{\setminus(a,b)}(U_1|0^n\rangle\langle 0^n|U_1^\dagger)V_{ab}^\dagger(M_a \otimes N_b)) \\ &= \frac{1}{4}\mathrm{tr}[V_{ab}^\dagger(M_a \otimes N_b)] \pm \|(M_a \otimes N_b)\|_2 \|V_{ab}\|_2 \varepsilon. \end{aligned} \tag{11.97}$$

As $\|(M_a \otimes N_b)\|_2 = 1$ and $\|V_{ab}\|_2 = 2$, we find

$$\langle\psi|\phi_{M,N}\rangle = \frac{1}{4}\mathrm{tr}[V_{ab}^\dagger (M_a \otimes N_b)] \pm 2\varepsilon. \tag{11.98}$$

Refs. [82, 83] proved that for a random circuit U_1 of depth D in one dimension, $\varepsilon \leq (4/5)^D$. In two dimensions we expect ε to go to zero even faster with depth, so we can ignore the second term of Eq. (11.98) for sufficiently large depth.

We now want to find M_a, N_b which are optimal for

$$\max_{M_a, N_b : \|M_a\|_2 = \|N_b\|_2} \mathrm{tr}[V_{ab}^\dagger (M_a \otimes N_b)]. \tag{11.99}$$

At this point, we have reduced the problem to finding the optimal decomposition of the gate as a standalone operator.

Consider the operator Schmidt decomposition of V_{ab}:

$$V_{ab} = \sum_i \lambda_i R_{a,i} \otimes S_{b,i}, \tag{11.100}$$

where $R_{a,i}$ ($S_{b,i}$) are orthonormal set of operators in the Hilbert-Schmidt inner product, i.e. $\mathrm{tr}(R_{a,i}^\dagger R_{a,j}) = \mathrm{tr}(S_{a,i}^\dagger S_{b,j}) = \delta_{ij}$. The Schmidt singular values $\lambda_1 \geq \lambda_2 \geq \ldots$ are in decreasing order. Then it follows that the solution of Eq. (11.99) is λ_1, with optimal solution $M_a = R_{a,1}$ and $N_b = S_{b,1}$. Indeed we can write Eq. (11.99) as

$$\max_{|x\rangle, |y\rangle} \langle x|\overline{V}|y\rangle \tag{11.101}$$

where the maximum is over all unit vectors $|x\rangle, |y\rangle$ in $(\mathbb{C}^2)^{\otimes 2}$ and $\overline{V}$ is the matrix

$$\overline{V} := \sum_i \lambda_i (R_{a,i} \otimes I)|\Phi\rangle\langle\Phi|(S_{b,i}^\dagger \otimes I) \tag{11.102}$$

with $|\Phi\rangle = \sum_i |i\rangle \otimes |i\rangle$. This can be verified using the fact that any unit vector $|x\rangle$ in $(\mathbb{C}^d)^{\otimes 2}$ can be written as $|x\rangle = (L \otimes I)|\Phi\rangle$ for a matrix L acting on $(\mathbb{C}^d)$ s.t. $\|L\|_2 = 1$. The result follows by noting that λ_i are the singular values of $\overline{V}$.

The argument above easily generalizes to the problem of finding the optimal operator of Schmidt rank k for replacing the unitary gate. In that case the optimal choice is $\sum_{i=1}^k \lambda_i R_{a,i} \otimes S_{b,i}$.

Classical speedup for imbalanced gates

We now want to analyze the Schmidt spectrum of the two-qubit gates used in this work. The $\mathrm{fSim}(\theta, \phi)$ gate is introduced in Section 11.7.5. This gate, which is presented in matrix form in Eq. (11.53), has the following Schmidt singular values:

$$\lambda_1 = \sqrt{1 + 2 \cdot |\cos(\phi/2)\cos\theta| + \cos^2\theta} \tag{11.103}$$

$$\lambda_2 = \lambda_3 = \sin\theta \tag{11.104}$$

$$\lambda_4 = \sqrt{1 - 2 \cdot |\cos(\phi/2)\cos\theta| + \cos^2\theta}\,, \tag{11.105}$$

where normalization is chosen so that $\sum_i^4 \lambda_i^2 = 4$. In practice, we have $\theta \approx \pi/2$ and $\phi \approx \pi/6$, and so we obtain $\lambda_i \approx 1$, $\forall i \in \{1, 2, 3, 4\}$, which gives a flat spectrum.

In the case that $\theta = \pi/2 \pm \delta_\theta$, the spectrum becomes imbalanced, as expected. When considering the decomposition of a number g of $\mathrm{fSim}(\pi/2 \pm \delta_\theta, \phi \approx \pi/6)$ gates, the set of

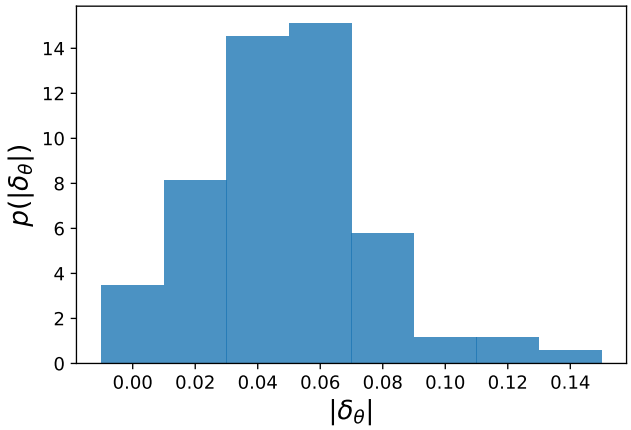


Figure S46: **Probability distribution of the deviations $|\delta_\theta|$ from $\theta \approx \pi/2$ for** fSim **gates.** The magnitude of δ_θ is directly related to the runtime speedup low fidelity classical sampling can take from exploiting the existence of paths with large Schmidt coefficients. In practice, $|\delta_\theta| \approx 0.05$ radians on average, which imposes a bound of less than an order of magnitude on this potential speedup for the circuits, gates, and simulation techniques considered in this work.

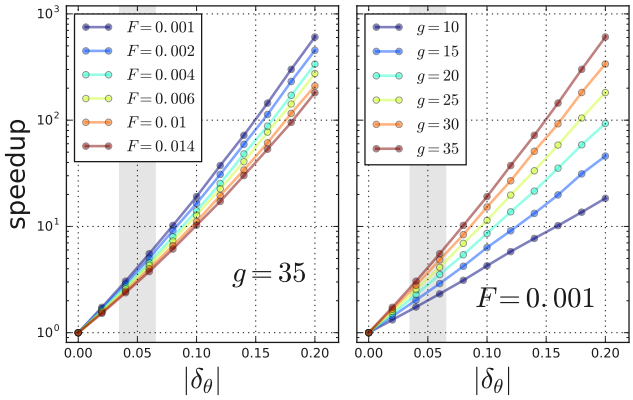


Figure S47: **Classical speedup given by the imbalance in the Schmidt coefficients of the gates decomposed.** The speedup is computed by comparison with the case where $\theta = \pi/2$ exactly. The classical simulation has a target fidelity $\mathcal{F}$, and g fSim gates are decomposed. For simplicity, we assume $\theta = \pi/2 + \delta_\theta$ is the same for all gates, as well as $\phi = \pi/6$. *Left:* speedup at different target fidelities for fixed $g = 35$. Note that the speedup decreases with $\mathcal{F}$; this is due to the fact that at very low fidelity, considering a few paths with very high weight might be enough to achieve the target fidelity, while for larger values of $\mathcal{F}$, paths with a smaller weight have to be considered, and so a larger number of them is needed per fractional fidelity increase. *Right:* speedup for fixed fidelity $\mathcal{F} = 0.001$ for different values of g. As expected, the speedup is greater as g increases, since the weight of the highest contributing paths increases exponentially with g. The largest speedup is achieved at large g and small $\mathcal{F}$. For $g = 35$ and $\mathcal{F} \gtrapprox 0.001$, we find speedups well below an order of magnitude, given that $|\delta_\theta| \approx 0.05$ radians in practice (shaded area); this case is representative of our simulation of Sycamore with $m = 20$ (see Section 11.10.1) targeting the fidelity measured experimentally.

weights of all paths is equal to the outer product of all sets of Schmidt coefficients (one per gate). Achieving a fidelity $\mathcal{F}_{\text{XEB}} > 0$ implies (in the optimal case) including the largest contributing paths, and so the advantage one can get from this is upper bounded by the magnitude of the largest weight, which is equal to $\prod_{\alpha=1}^{g} \lambda_{\alpha,max}^2$, where α labels the gates decomposed and $\lambda_{\alpha,max}$ is the largest Schmidt coefficient for gate α. In practice, $|\delta_\theta|$ has values of around 0.05 radians (see Fig. S46). The geometric mean of λ_{max} is about 1.047, which gives an upper bound of 1.047^{2g} to the speedup discussed here. For the largest value of g considered in this work, *i.e.*, the decomposition of $g = 35$ gates using the SFA simulator (Section 11.10.1) on a circuit of $m = 20$ cycles, we obtain a value of $1.047^{2\times 35} = 25.4$. Note that the speedup obtained in practice (as compared to runtimes over circuits with perfectly flat gate Schmidt decompositions) for fidelities of the order of 0.1% and larger is expected to be far smaller than this value, given that one has to consider a large number of paths, from which only an exponentially small number will have a weight close to 25.4.

We can get a better estimate for the speedup achieved in practice, beyond the upper bound of about a factor of 25 that decomposing $g = 35$ gates with typical parameters would give. For simplicity, let us assume that all g gates have the same values of θ and ϕ. Then the weight of each path arising from this decomposition can be written as $W_i = W_{(a,b,c)} = \lambda_1^{2a}\lambda_2^{2b}\lambda_3^{2c}$, where $a + b + c = g$, and that the number of paths for each choice of (a, b, c) is equal to $\#(a, b, c) = \sum_{k=0}^{b} \text{multinomial}(a, b - k, k, c) = 2^b \times \text{multinomial}(a, b, c)$. After sorting all 4^g weights (and paths) by decreasing value, given a target fidelity, $\mathcal{F}$, one now has to consider the first S paths (*i.e.*, those with the largest weight), up to the point where the sum of their weights $\sum_{i=1}^{S} \frac{W_i}{4^g}$ matches the target fidelity. The normalization factor 4^g guarantees that if one were to consider all paths, the fidelity would be unity, as expected. Compared to the case where we consider a number $\mathcal{F} \times 4^g$ of paths, as for a flat Schmidt spectrum, this provides a speedup equal to $\frac{S}{\mathcal{F}\times 4^g}$. We show the speedup achieved this way in Fig. S47. For the case where we would achieve the largest speedup in the simulations considered in this work, namely the simulation of Sycamore at $m = 20$ cycles and a fidelity $\mathcal{F} \approx 0.2\%$ with $g = 35$ gates decomposed (see Section 11.10.6), we estimate that the speedup obtained this way would be well below an order of magnitude, since $|\delta_\theta|$ typically takes values of about 0.05 radians.

Verifiable and supremacy circuits

So far we have considered the decomposition of gates one by one, *i.e.*, where the total number of paths is equal to the product of the Schmidt rank of all gates decomposed. However, by fusing gates together in a larger unitary, one can provide some speedup to the classical simulation of the sampling task.

The rationale here comes from the realization that a unitary that involves a number of qubits q cannot have a rank larger than $4^{\min(q_l,q_r)}$ when Schmidt decomposed over two subsets of qubits of size q_l and q_r, with $q_l + q_r = q$. Therefore one might reduce exponentially the number of paths by fusing gates such that the resulting unitary reaches on either side (l or r) a number of qubits that is smaller than the product of the ranks of the fused gates to be decomposed. This is at the heart of the formation of *wedges* of Section 11.7.7. These wedges denote particular sequences of consecutive two-qubit gates that only act upon three qubits. Fusing these two-qubit gates together generates 4 paths, as opposed to a naive count of 4^2 paths if one decomposes each gate separately. Each wedge identified across a circuit cut provides a speedup by a factor of 4.

In this work, we define two classes of circuits: *verifiable* and *supremacy* circuits. Verifiable circuits present a large number of wedges across the partition used with the SFA simulator (Section 11.10.1) and are therefore classically simulatable in a reasonable amount of time. These circuits were used to perform full XEB over the entire device up to depth $m = 14$ (see Fig. 4a of the main article and Sections 11.7 and 11.8), which involves perfect fidelity computations. On the other hand, supremacy circuits are designed so that the presence of

wedges and similar sequences is mitigated, therefore avoiding the possibility of exploiting this classical speedup.

It is natural to apply the ideas presented here beyond *wedges*. It is also easy to look for similar structures in the circuits algorithmically. This way, we find that for the supremacy circuits there is a small number of such sequences. On the sequence of cycles DCD (see Fig. S25), three two-qubit gates are applied on qubits 16, 47, and 51 (see Fig. S27 for numbering). These three gates can be fused in one. Then, if the two gates between qubits 47 and 51 are decomposed (as is done with the SFA simulations of Section 11.10.1 used in Fig. 4 of the main article), this technique provides a speedup of a factor of 4. The sequence of layouts DCD appears twice for circuits of $m = 20$, which provides a total speedup of $4^2 = 16$ in the simulation of the supremacy circuits. This particular decomposition is currently not implemented, and the estimated timings of Section 11.10.1 and Fig. 4 of the main article do not take it into account.

Beyond this, one has to go to groups of several cycles of the circuit (more than two) in order to identify regions where the fusion of several gates provides any advantage of this kind. In our circuits, the resulting unitaries act upon a large number of qubits, which makes explicitly building the unitary impractical.

11.10.5 Treewidth upper bounds and variable elimination algorithms

We explained in Section 11.10.2 that the Feynman method to compute individual amplitudes of the output of a quantum circuit can be implemented as a tensor network when quantum gates are interpreted as tensors. All indexes of the tensor network have dimension two because indexes correspond to qubits. Similarly, Ref. [70] showed that a quantum circuit can be mapped directly to an undirected graphical model. In the undirected graphical model, vertices or variables correspond to tensor indexes, and cliques correspond to tensors. Individual amplitudes can be computed using a variable elimination algorithm on the undirected graphical model, which is similar to a tensor contraction on a tensor network. The variable elimination algorithm depends on the ordering in which variables are eliminated or contracted. If we define the *contraction width* of an ordering to be the rank of the largest tensor formed along the contraction, the *treewidth* of the undirected graph is equal to the minimum contraction width over all orderings. Therefore, the complexity of a tensor network contraction grows in the optimal case exponentially with the treewidth, and the treewdith can be used to study the complexity of Feynman methods for simulating quantum circuits [69]. Ref. [70] showed that for diagonal gates the undirected graphical model is simpler, potentially lowering its treewidth, and hence improving the complexity. This simplification is not achievable in the tensor network view without including hyperedges, *i.e.*, edges attached to more than two tensors. Ref. [70] also introduced the use of `QuickBB` to find a heuristic contraction ordering [84]. If allowed to run for long enough, `QuickBB` finds the optimal ordering, together with the treewidth of the graph. However, note that obtaining the treewidth of a graph is an NP-hard problem, and so in practice a suboptimal solution is considered for the simulations described here.

Once the width of a contraction is large enough, the largest tensor it generates is beyond the memory resources available. This constraint was overcome in Ref. [72] by *projecting* a subset of p variables or vertices in the undirected graphical model into each possible bistring of 0 and 1 values. This generates 2^p similar subgraphs, each of which can be contracted with lower complexity and independently from each other, making the computation embarrassingly parallelizable. Choosing the subset of variables that, after projection, optimally decreases the treewidth of the resulting subgraph is also NP-hard. However, Ref. [72] developed a heuristic

approach that works well in practice. The algorithm proceeds as follows:

1. Run `QuickBB` for S seconds on the initial graph. This gives a heuristic contraction ordering, as well as an upper bound for the treewidth.

2. For each variable, estimate the cost of contracting the subgraph after projection. The estimate is done with the ordering inherited from the previous step.

3. Choose to project the variable which results in the minimum contraction cost.

4. Repeat steps 2 and 3 until the cost is within reasonable resources.

5. Once all variables have been chosen and projected, run `QuickBB` for S seconds on the resulting subgraph to try to improve the contraction ordering inherited from step 1 and lower the contraction cost.

In the top panel of Fig. S48 we show the contraction width as a function of the number of variables that are projected for the supremacy circuits used in this paper. In order to decrease the contraction width to 28 or below (a tensor with 28 binary indexes consumes 2 GB of memory using single precision complex numbers), we need to project between 8 and 63 variables, depending on the depth of the circuits. In addition, we report the result of the projection procedure on the Bristlecone circuits considered in Refs. [50, 85] and available at https://github.com/sboixo/GRCS for depths (1+32+1) and (1+40+1), since these cases were benchmarked in Ref. [85]. We obtain a contraction width equal to 28 after 10 projections for Bristlecone at depth (1+32+1), and width 26 after 22 projections for Bristlecone at depth (1+40+1), consistent with the results in Ref. [85]. Even though Ref. [72] uses $S = 60$, we run `QuickBB` for 1800 seconds (30 minutes) every time, in order to decrease the contraction width of the Bristlecone simulations to values that match the memory requirements reported in Ref. [85]. Note that Ref. [85] neither reports the value of S used nor the contraction widths found; however, with $S = 1800$ we are able to match the scaling of time complexity reported, as is explained below.

To estimate the runtime of the computation of a single amplitude using this algorithm on the circuits presented in this work, we use the following scaling formula:

$$T_{\mathrm{VE}} = C_{\mathrm{VE}}^{-1} \cdot 2^{p} \cdot (\text{cost after } p \text{ projections})/n_{\mathrm{cores}}, \tag{11.106}$$

where VE refers to the variable elimination algorithm with projections described in this section, C_{VE} is a constant factor, p is the number of variables projected, and n_{cores} is the number of cores used in the computation. The cost of the full contraction of each subgraph is estimated as the sum of 2^{rank}, where the rank refers to the number of variables involved in each individual contraction along the full contraction of the subgraph. We obtain the value of C_{VE} from the runtimes reported in Ref. [72], which shows that a single amplitude of Bristlecone at depth (1+32+1) takes 0.43 seconds to compute on 127,512 CPU cores with 10 projected variables, and at depth (1+40+1) it takes 580.7 seconds with 22 projected variables using the same number of cores. We use the benchmark at depth (1+32+1) because it provides the largest value for C_{VE} (lowest time estimates), which is equal to 52.7 MHz; the benchmark at depth (1+40+1) gives $C_{\mathrm{VE}} = 51.6$ MHz. In order to sample 1M bitstrings from a random circuit with fidelity 0.5%, we need to compute 5000 amplitudes.

We present our estimates for Sycamore supremacy circuits in the bottom panel of Fig. S48. Note that depth (1+40+1) in Refs. [72, 85] is equivalent to m=20 cycles here because of the denser layout of two-qubit gates. Furthermore, computation times reported previously are for circuit variations less complex than for Sycamore, arising from changes in complexity such as

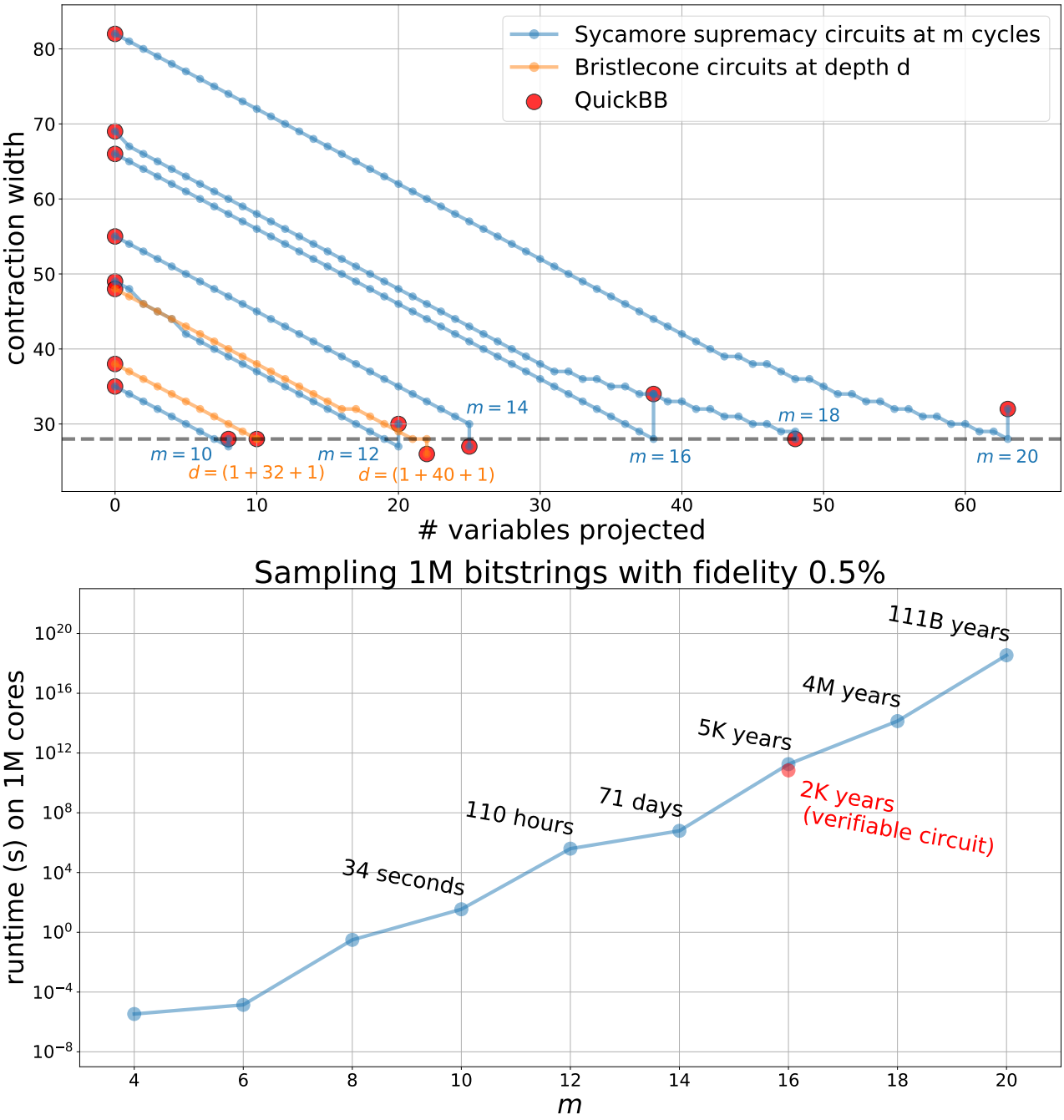


Figure S48: **Contraction widths and estimated runtimes for classical sampling using the variable elimination algorithm with projected variables of Ref. [72] for Sycamore supremacy circuits.** *Top:* contraction width as a function of the number of variables projected using the algorithm of Ref. [72]. We project enough variables in order to decrease the width to 28 or lower. Note that often the second `QuickBB` run does not decrease the treewidth (and might even increase it), in which case the resulting contraction ordering it is ignored. *Bottom:* estimated runtimes for the classical sampling of 1M bitstrings from the supremacy circuits with fidelity 0.5% using the contraction ordering found by `QuickBB` at the end of the projection procedure shown in the top panel. The red data point shows the estimated runtime for a verifiable circuit; note that the heuristic algorithm analyzed here provides some speedup in this case. Our time estimates assume the use of fast sampling, although it is so far unclear whether this technique can be adapted to the algorithm described here. Failure to do so would result in a slowdown of about an order of magnitude.

CZ vs. fSim gates and differing patterns; with this change of gates, depth (1+40+1) in Refs. [72, 85] is actually equivalent to m=10 cycles here. Finally, note that we present optimistic estimates, since we are assuming that the fast sampling technique discussed in Section 11.10.2 is applicable here. To the best of our knowledge, it is not known how to apply this technique for the heuristic variable elimination algorithm discussed here; in the absence of an implementation of this technique, in order to successfully apply rejection sampling we would instead need to compute a few independent amplitudes per sampled bitstring, which would increase the estimated times by about an order of magnitude (see Section 11.10.2 and Refs. [38, 86] for more details). According to our estimates, sampling from supremacy circuits at $m = 16$ and beyond is out of reach for this algorithm. Interestingly, we find some speedup for the simulation of verifiable circuits, as is shown in Fig. S48 for $m = 16$ (red data point).

Finally, note that the undirected graphical model derived from the supremacy circuits can take advantage of the structure of the Sycamore gates (fSim plus single-qubit R_z rotations). Due to the fact that $\text{fSim}(\theta \approx \pi/2, \phi) \approx -i \cdot [R_z(-\pi/2) \otimes R_z(-\pi/2)] \cdot \text{cphase}(\pi + \phi) \cdot \text{SWAP}$, the Sycamore gate corresponds to a subgraph of only two variables, which explicitly represents the diagonal cphase and the logical SWAP. This simplification, used in our estimates, results in an undirected graphical model that is simpler than that one generated by arbitrary two-qubit gates. See Fig. S49 for an example.

11.10.6 Computational cost estimation for the sampling task

We find that the most efficient simulator for our hardest circuits is the SFA simulator (see Sec. 11.10.1). In order to estimate the computational cost associated with simulating a 53 qubit circuit with 20 cycles, where no gates are elided on the cut, we use a Google cloud cluster composed of 1000 machines with 2 vCPUs and 7.5 GB of RAM each (n1-standard-2). We use n1-standard-2 because this is the smallest non-custom machine with sufficient RAM for simulating the two halves of the circuit. In 20 cycles, the circuit contains 35 gates across the cut. All cross gates have a Schmidt rank of 4 except for the last four gates which can be simplified to cphase with a Schmidt rank of 2. To obtain a perfect fidelity simulation we would need to simulate all $4^{31} \times 2^4$ paths. We configure qsimh according to Ref. [38] to have a prefix of 30 cross gates, thus requiring 4^{30} separate qsimh runs. The first 1000 paths of the required 4^{30} were used for timing purposes. In Figure S50 we plot the distribution of simulation times with qsimh consuming two hyperthreads. The average job time is 246 seconds resulting in a calculated 1.6×10^{14} core hours for a simulation of the circuit with 0.002 fidelity [87]. Extrapolated run times for other circuits with 53 qubits are shown in Table **??**. To calculate a total cost for the largest circuit we multiply the Google Cloud preemptible n1-standard-2 price in zone us-central-1 of $0.02 per hour, 246 seconds average run time, 0.002 target fidelity, and 4^{30} qsimh runs. This results in an estimated cost of 3.1 trillion USD. For perfect fidelity simulations (necessary for XEB), an extrapolation to a fidelity value of 100% gives a good estimate of the run time. We believe these estimates are a lower bound on costs and simulation time due to the fact that these calculations are likely to compete with each other if they are run on the same nodes.

As a final remark, note that a hypothetical implementation of the decomposition discussed at the end of Section 11.10.4 could decrease the computation time presented here by a factor of 16.

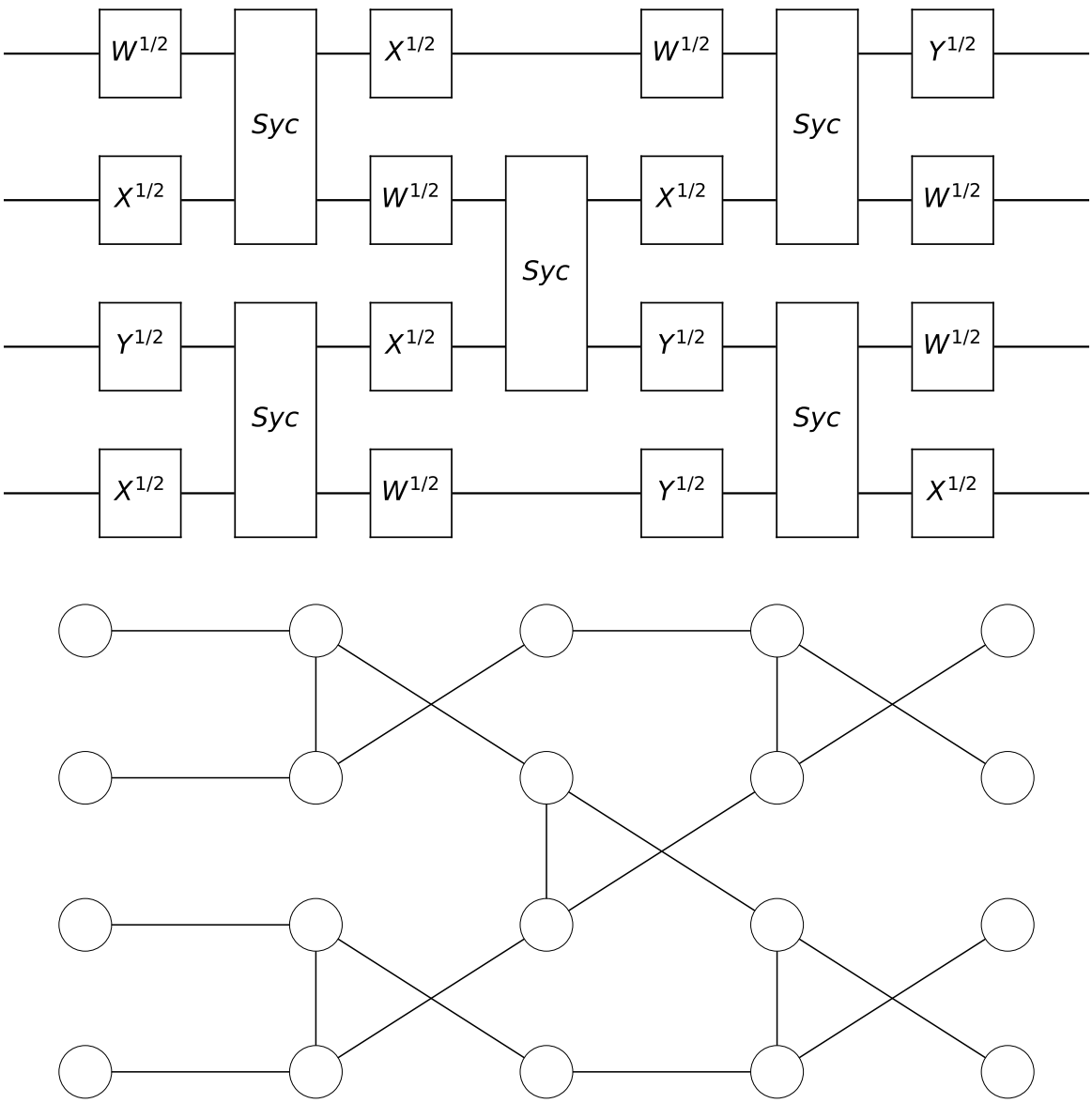


Figure S49: **Circuit with Sycamore gates (top) and its corresponding undirected graphical model (bottom).** Each non-diagonal single-qubit gate introduces a new vertex or variable. Note that, even though two-qubit gates are generally represented by a clique with four vertices or variables, Sycamore gates can be simplified as a cphase followed by a SWAP. The cphase is represented as an edge between two existing variables. The SWAP, however, provides more complexity to the graph as it swaps the corresponding variables.

qubits, n	cycles, m	total #paths	fidelity	run time
53	12	$4^{17}2^4$	1.4%	2 hours
53	14	$4^{21}2^4$	0.9%	2 weeks
53	16	$4^{25}2^3$	0.6%	4 years
53	18	$4^{28}2^3$	0.4%	175 years
53	20	$4^{31}2^4$	0.2%	10000 years

Table 21: Approximate qsimh run times using one million CPU cores extrapolated from the average simulation run time for 1000 simulation paths on one CPU core.

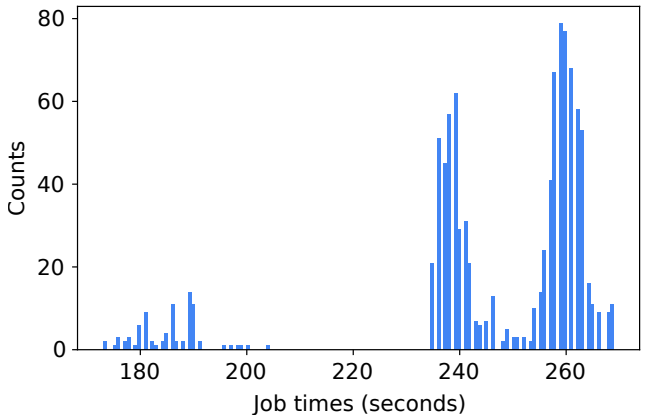


Figure S50: Qsimh execution time for a 53 qubit circuit with 20 cycles for the first 1000 prefix values. The average job time $\langle t_{\text{prefix}} \rangle$ is calculated to be 246 seconds.

11.10.7 Understanding the scaling with width and depth of the computational cost of verification

Runtime scaling formulas

Here we study the scaling of the runtime of the classical computation of exact amplitudes from the output wave function of a circuit with m cycles and n qubits on Sycamore, assuming a supercomputer with 1M cores. This computation is needed in order to perform XEB on the circuits run. We consider two algorithms: a distributed Schrödinger algorithm (SA) [74, 75] (see Section 11.10.3) and a hybrid Schrödinger-Feynman algorithm (SFA) [38] that splits the circuit in two patches and time evolves each of them for all Feynman paths connecting both patches (see Section 11.10.1). The latter is embarrassingly parallelizable. Note that these scaling formulas provide rough estimates presented with the intent of building intuition on the scaling of runtimes with the width and depth of the circuits, and that the finite size effects of the circuits can give discrepancies of an order of magnitude or more for the circuit sizes considered in this work.

For SA, the runtime is directly proportional to the size of the wave function on n qubits. This is equal to 2^n. In addition, the runtime is proportional to the number of gates applied, which scales linearly with n and m. For this reason, we propose the scaling:

$$T_{\text{SA}} = C_{\text{SA}}^{-1} \cdot mn \cdot 2^n, \tag{11.107}$$

where the constant C_{SA} is fit to runtimes observed experimentally when running on a supercomputer, and scaled to 1M cores.

For SFA the runtime is proportional to the number of paths connecting both patches, as well as to the time taken to simulate each pair of patches. When using the *supremacy* two-qubit gate layouts (ABCDCDAB...), each fSim gate bridging between the two patches (cross-gates) generates a factor of 4 in the number of paths. The number of cross-gates scales with $\sqrt{n}$ (we assume a two-dimensional grid) and with m. The time taken to simulate each patch is proportional to $2^{n/2}$, where $n/2$ estimates the number of qubits per patch, and the exponential dependence comes from a linear scaling of the runtime with the size of the wave function over that patch. The runtime therefore scales as:

$$T_{\text{SFA, supremacy}} = C_{\text{SFA}}^{-1} \cdot 2 \cdot 2^{\frac{n}{2}} \cdot 4^{B \cdot m\sqrt{n}}, \tag{11.108}$$

where the extra factor of two accounts for the fact that, for every path, two patches have to be simulated. The constant C_{SFA}, with units of frequency, is the effective frequency with which 1M cores simulate paths and is fit from experimentally observed runtime. The constant B accounts for the average number of cross-gates observed per cycle, which depends on the two-dimensional grid considered and on the two-qubit gate layouts used. For Sycamore, with the supremacy layouts, we find 35 cross-gates for $n = 53$ and $m = 20$, which gives $B = 0.24 \approx 1/4$.

For SFA, using the *verifiable* two-qubit gate layouts (EFGHEFGH...), the main difference with the supremacy circuits case is the fact that most of the cross-gates can be fused in pairs, forming three-qubit gates we refer to as *wedges* (see Sec. 11.7.7 and 11.10.4). Each cross-wedge generates only 4 paths, as opposed to the 4^2 paths the two independent fSim gates would have generated. Since every 4 cycles provide 7 cross-gates, and from those 7 gates, 6 are converted into 3 wedges, we count only 4^4 paths, as opposed to a naive count of 4^7 for those 4 cycles. In turn, the exponent in the last factor of Eq. 11.108 is corrected by the fraction $\frac{4}{7}$. This results in:

$$T_{\text{SFA, verifiable}} = C_{\text{SFA}}^{-1} \cdot 2 \cdot 2^{\frac{n}{2}} \cdot 4^{\frac{4}{7} B \cdot m\sqrt{n}}. \tag{11.109}$$

Assumptions and corrections

There are several assumptions considered in Section 11.10.7 and other details that can either (1) contribute to a somewhat large discrepancy between the runtimes predicted by the scaling formulas and the actual runtimes potentially measured experimentally, or (2) be ignored with no significant impact on the accuracy of the predictions. Here we discuss the ones we consider most relevant.

Concerning SA, the algorithm is benchmarked in practice on up to 100K cores. Since this is a distributed algorithm, the scaling with number of cores is not ideal and therefore the constant C_{SA} can only be estimated roughly. We assume perfect scaling in our estimates for runtime on 1M cores, *i.e.*, the runtime on 1M cores is the one on 100K cores divided by 10; this is of course an optimistic estimate, and runtimes should be expected to be larger.

For memory requirement estimates, we assume a 2 byte encoding of complex numbers. Beyond about 49 qubits there is not enough RAM on any existing supercomputer to store the wave function. In those cases, runtimes are given for the unrealistic, hypothetical case that one *can* store the wave function.

SFA is embarrassingly parallelizable, and so it does not suffer from non-ideal scaling. However, there are other factors to take into account. First, we have written no explicit dependence of the time to simulate patches of the circuit with m; the number of cycles m only plays a role when counting the number of paths to be considered. SFA stores several copies of the state of a patch after its evolution at different depths, iterating over paths over several nested loops. For this reason, most of the time is spent iterating over the inner-most loop, which accounts for the last few gates of the circuit and is similar in cost for all depths. This implies that the amortized time per path is considered approximately equal for all depths and the direct m dependence was correctly ignored.

A factor contributing to the discrepancy between the predicted runtimes of the scaling formulas of Section 11.10.7 and those expected in practice is due to finite size effects. While these scaling formulas consider the average number of cross-gates encountered per cycle, different cycles have layouts that contribute a few more (or less) gates than others. Since the runtime dependency is exponential in the number of gates, this might cause discrepancies of around an order of magnitude. Furthermore, for verifiable circuits, wedges form over groups of two cycles; this coarse graining exacerbates finite size effects. For the sake of simplicity in the scaling

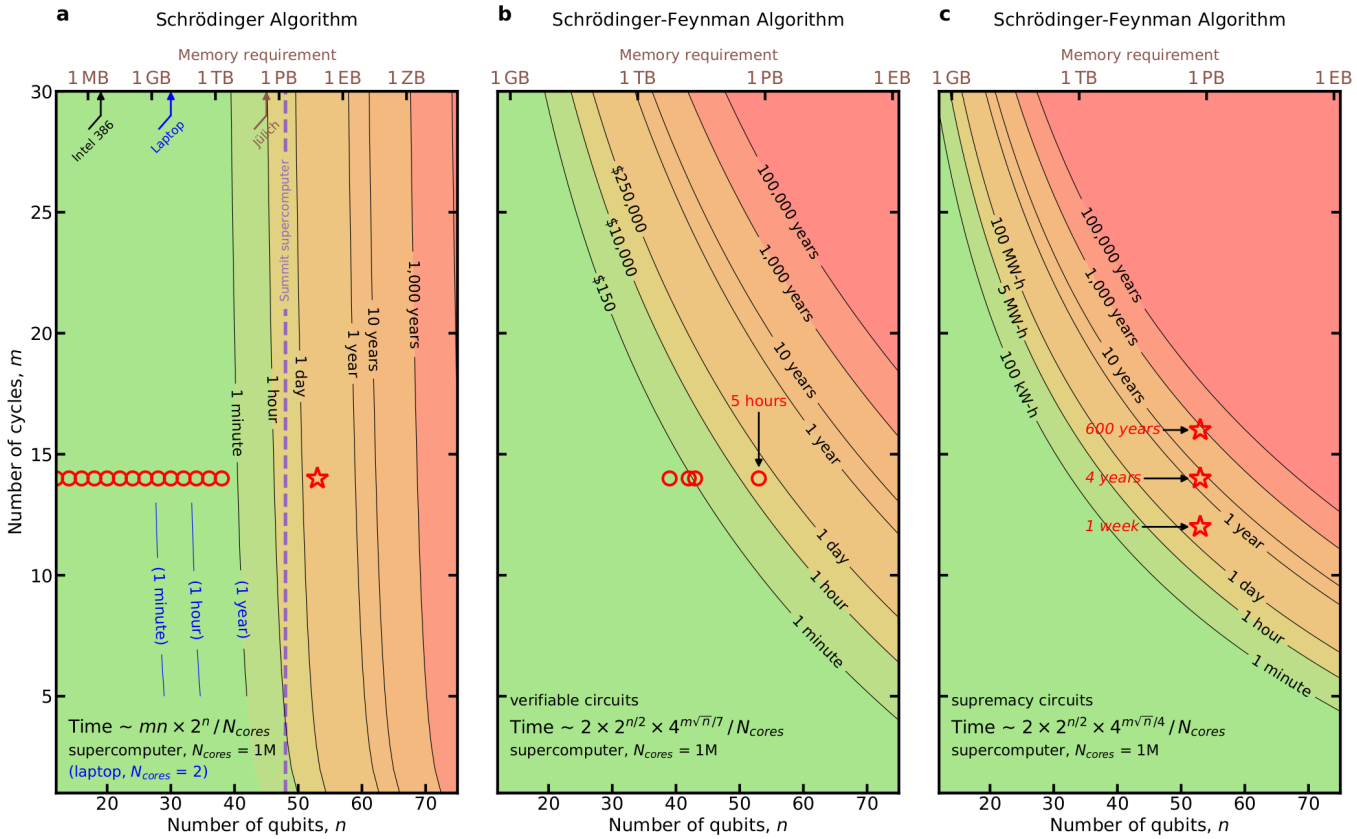


Figure S51: **Scaling of the computational cost of XEB using SA and SFA. a,** For a Schrödinger algorithm, the limitation is RAM size, shown as vertical dashed line for the Summit supercomputer. Circles indicate full circuits with $n = 12$ to 43 qubits that are benchmarked in Fig. 4a of the main paper [1]. 53 qubits would exceed the RAM of any current supercomputer, and is shown as a star. **b,** For the hybrid Schrödinger-Feynman algorithm, which is more memory efficient, the computation time scales exponentially in depth. XEB on full verifiable circuits was done at depth $m = 14$ (circle). **c,** XEB on full supremacy circuits is out of reach within reasonable time resources for $m = 12$, 14, 16 (stars), and beyond. XEB on patch and elided supremacy circuits was done at $m = 14$, 16, 18, and 20.

formulas, we do not perform any corrections to include these factors. However, in order to mitigate the propagation of finite size effect errors, we consider different constants $C_{\text{SFA, supremacy}}$ and $C_{\text{SFA, verifiable}}$, that we fit independently.

Finally, we refer to runtimes of our simulations on a hypothetical supercomputer with 1M cores. While this is a realistic size for a Top-5 supercomputer currently, a core-hour can vary significantly between different CPU types. Again, we only intend to provide rough estimates in order to build intuition on the dependence of runtimes with circuit width and depth.

Fitting constants

In the case of SA, we fit the constant C_{SA} with a runtime of 0.1 hours for the simulation with $n = 43$ and $m = 14$. This runtime is obtained by assuming ideal scaling when extrapolating a runtime of 1 hour on nearly 100K nodes (2^{15} MPI processes, 3 cores per process), as reported in Sec. 11.10.3. This gives a value of

$$C_{\text{SA}} = 0.015 \times 10^6 \text{ GHz}. \tag{11.110}$$

For SFA, we consider $B = 1/4$ for simplicity. In order to fit C_{SFA}, we consider a runtime of 5 hours and 4 years for the case with $n = 53$ and $m = 14$ for verifiable and supremacy circuits, respectively (see Fig. 4 of the main text). This gives:

$$\begin{aligned} C_{\text{SFA, verifiable}} &= 0.0062 \times 10^6 \text{ GHz} \\ C_{\text{SFA, supremacy}} &= 3.3 \times 10^6 \text{ GHz}. \end{aligned} \tag{11.111}$$

As discussed above, these fits provide times estimated for a supercomputer with 1M cores. Contour plots showing the dependency of runtime with n and m are presented in Fig. S51.

Memory usage scaling

Let us conclude with a discussion of the memory footprint of both algorithms. For these estimates, we assume a 2-byte encoding of complex numbers, as opposed to 8 bytes (single precision) or 16 bytes (double precision). This results in a lower bound for the memory usage of these two algorithms. These estimates need an extra factor of 4 (8) when using single (double) precision. SA stores the wave function of the state on all qubits. For this reason, it needs $2^n \times 2 = 2^{n+1}$ bytes. SFA simulates the wave function of both halves of the system ($n/2$ qubits) per path, one at a time. This requires $2^{\frac{n}{2}} \cdot 2$ bytes per path. In practice, the use of checkpoints implies the need to store more than one wave function per path; for simplicity, and in the same optimistic spirit of other assumptions, we ignore this fact. If 1M cores are used and each path is simulated using a single core, the total memory footprint is estimated to be $10^6 \times 2^{\frac{n}{2}+1}$ bytes. State-of-the-art supercomputers have less than 3 PB of memory.

11.10.8 Energy advantage for quantum computing

With the end of Dennard scaling for CMOS circuits, gains in computing energy efficiency have slowed significantly [88]. As a result, today's high performance computing centers are usually constrained by available energy supplies rather than hardware costs. For example, the Summit supercomputer at Oak Ridge National Laboratory has a total power capacity of 14 MW available to achieve a design specification of 200 Pflop/s double-precision performance. We took detailed energy measurements with qFlex running on Summit. The energy consumption grows exponentially with the circuit depth, as illustrated in Table 17.

For a superconducting quantum computer, the two primary sources of energy consumption are:

1. **A dilution refrigerator:** our refrigerator has a direct power consumption of ∼10 kW, dominated by the mechanical compressor driving the 3 K cooling stage. The power required to provide chilled water cooling for the compressor and pumps associated with the refrigerator can be an additional 10 kW or more.

2. **Supporting electronics:** these include microwave electronics, ADCs, DACs, clocks, classical computers, and oscilloscopes that are directly associated with a quantum processor in the refrigerator. The average power consumption of supporting electronics was nearly 3 kW for the experiments in this paper.

We estimate the total average power consumption of our apparatus under worst-case conditions for chilled water production to be 26 kW. This power does not change appreciably between idle and running states of the quantum processor, and it is also independent of the circuit depth. This means that the energy consumed during the 200 s required to acquire 1M samples in our experiment is $\sim 5 \times 10^6$ J ($\sim$ 1 kWh). As compared to the qFlex classical simulation on Summit, we require roughly 7 orders of magnitude less energy to perform the same computation (see Table 17). Furthermore, the data acquisition time is currently dominated by control hardware communications, leading to a quantum processor duty cycle as low as 2%. This means there is significant potential to increase our energy efficiency further.

11.11 Complexity-theoretic foundation of the experiment

The notion of quantum supremacy was originally introduced by John Preskill [89]. He conceived of it as "the day when well controlled quantum systems can perform tasks surpassing what can be done in the classical world". For the purpose of an experimental demonstration we would like to refine the definition.

Demonstrating quantum supremacy requires:

1. A well defined computational task, i.e. a mathematical specification of a computational problem with a well defined solution.

   Comment: This requirement, standard in computer science, excludes tasks such as "simulate a glass of water". However, it would include finding the ground state energy of an H_2O molecule to a given precision governed by a specific Hamiltonian. Note that a mathematical specification of a computational problem calls for highly accurate control resulting in measurable system fidelity.

2. Programmable computational device

   Comment: Many physics experiments estimate the values of observables to a precision which can not be obtained numerically. But those do not involve a freely programmable computational device and the computational task is often not well defined as required above. Ideally, we would even restrict ourselves to devices that are computationally universal. However, this would exclude proposals to demonstrate quantum supremacy with BosonSampling [90] or IQP circuits [91].

3. A scaling runtime difference between the quantum and classical computational processes that can be made large enough as a function of problem size so that it becomes impractical for a supercomputer to solve the task using any known classical algorithm.

Comment: What is impractical for classical computers today may become tractable in ten years. So the quantum supremacy frontier will be moving towards larger and larger problems. But if a task is chosen such that the scaling for the quantum processors is polynomial while for the classical computer it is exponential then this shift will be small. Establishing an exponential separation requires substantial efforts designing and benchmarking classical algorithms [74, 67, 27, 70, 50, 75, 68, 72, 69, 85], and support from complexity theory arguments [27, 30, 92]. Sampling the output of random quantum circuits is likely to exhibit this scaling separation as a function of the number of qubits for large enough depth. In this context, we note that quantum analog simulations that estimate an observable in the thermodynamic limit typically do not define a problem size parameter.

The requirements above are satisfied by proposals of quantum supremacy emerging from computer science, such as BosonSampling [90], IQP circuits [91], and random circuit sampling [27, 6, 30, 92, 93]. They are also implicit in the "Extended Church-Turing Thesis": any "reasonable" model of computation can be efficiently simulated, as a function of problem size, by a Turing machine.

We note that formal complexity proofs are asymptotic, and therefore assume an arbitrarily large number of qubits. This is only possible with a fault tolerant quantum computer and therefore near term practical demonstrations of quantum supremacy must rely on a careful comparison with highly optimized classical algorithms on state-of-the-art supercomputers.

So far we have argued for quantum supremacy by comparing the running time of the quantum experiment with the time required for the same task using the best known classical algorithms, running on the most powerful supercomputers currently available. The fastest known algorithm for exact sampling (or for computing transition probabilities) runs in time exponential in the treewidth of the quantum circuit [69, 70]; for a depth D circuit on a rectangular lattice of sizes l_x and l_y, the treewidth is given by $\min(\min(l_x, l_y)D, l_x l_y)$. For approximate simulation in which one only requires a given global fidelity F, the classical cost is reduced linearly in F [38]. As classical algorithms and compute power can be improved in the future, the classical cost benchmark is a moving target.

A complementary approach to back up supremacy claims consists of giving complexity-theoretic arguments for the classical hardness of the problem solved (in our case sampling from the output distribution of a random circuit of a given number of qubits, depth and output fidelity). Previous work gave hardness results for sampling *exactly* from the output distribution of different classes of circuits [90, 94, 95, 27, 96]. Most relevant to us are Refs. [92, 97, 93], which proved that it is classically intractable (unless the polynomial hierarchy collapses to its third level, which is considered extremely unlikely [98]) to sample from the exact probability distribution of outcomes of measurements in random circuits. We note the distribution of circuits considered in [92, 97, 93] is different from ours.

An important clarification is that such results are asymptotic, i.e. they show that, unless the polynomial hierarchy collapses, there are no polynomial-time classical algorithms for sampling from output measurements of certain quantum circuits. But they cannot be used directly to give concrete lower bounds for quantum computations of a fixed number of qubits and depth. Refs. [99, 100, 101] tackled this question using tools from fine-grained complexity, giving several finite size bounds.

There are also results arguing for the hardness of *approximate* sampling (see e.g. [90, 91, 27, 95]), where the task is only to sample from a distribution which is close to the ideal one. As the quantum experiment will never be perfect, this is an important consideration. However those results are weaker than the ones for exact sampling, as the hardness assumptions required have been much less studied (and in fact were introduced with the exact purpose of arguing for quantum supremacy). Another drawback is that the results only apply to the situation where

the samples come from a distribution very close to the ideal one (i.e. with high fidelity with the ideal one). This is not the regime in which our experiment operates.

With these challenges in mind, we consider an alternative hardness argument in this section, which will allow us to lower bound the classical simulation cost of noisy quantum circuits by the cost of the ideal one. On one hand, our argument will be more restrictive than previous results in that we will assume a particular noise model for the quantum computer (one, however, which models well the experiment). On the other hand, it will be stronger in two ways: (1) it will apply even to the setting in which the output fidelity of the experimental state with the ideal one can be very small, but still the product of total fidelity with exact computational cost is large; and (2) it will be based on more mainstream complexity assumptions in contrast to the tailor-made conjectures required in e.g. [90, 91, 95] to handle the case of small adversarial noise.

11.11.1 Error model

Our error model is the following. We assume that the quantum computer samples from the following output distribution:

$$r_{U,F}(x) := F|\langle x|U|0\rangle|^2 + (1-F)/2^n, \tag{11.112}$$

with U the circuit implemented. In words, we assume global depolarizing noise. Ref. [27] argues that Eq. (11.112) is a good approximation for the output state of random circuits (see Sec. 11.4 and Section III of [27]); this form has also been verified experimentally on a small number of qubits. In the experiment, F is in the range $10^{-2} - 10^{-3}$.

We note that while we assume a global white noise model in this section, we do not assume it in the rest of the paper, neither for validating the cross entropy test nor in the comparison with state-of-the-art classical algorithms (and indeed the algorithm considered in Section 11.10 samples from an approximate distribution different from the one in Eq. (11.112)).

11.11.2 Definition of computational problem

Before stating our result, let us define precisely the computational problem we consider. We start with the ideal version of the problem with no noise:

Circuit Sampling: The input is a description of a n qubit quantum circuit U, described by a sequence of one- and two-qubit gates. The task of the problem is to sample from the probability distribution of outcomes $p_U(x) := |\langle x|U|0\rangle|^2$.

Circuit sampling is an example of a *sampling problem* [102]. A classical algorithm for circuit sampling can be thought of, without loss of generality, as a function A mapping $m \in \text{poly(n)}$ bits $r = (r_1, \ldots r_m)$ to n bits such that

$$\frac{1}{2^m}|\{(r_1, \ldots, r_m) \text{ s.t. } A(r_1, \ldots, r_m) = x\}| = \tilde{p}_U(x), \tag{11.113}$$

with $\tilde{p}(x)$ an approximation of $p_U(x)$ to $l \in \text{poly(n)}$ bits of precision. So when r is chosen uniformly at random, the output of A are samples from p (up to rounding errors which can be made super-exponentially small).

Assuming the polynomial hierarchy does not collapse, it is known that Circuit Sampling cannot be solved classically efficiently in n, meaning any algorithm A satisfying Eq. (11.113) must have superpolynomial circuit complexity, for several classes of circuits (such as short depth circuits [96], IQP [94] and Boson Sampling [90]). We might also be interested in the average case of circuit sampling (for a restricted class of circuits).

Random Circuit Sampling: The input is a set of quantum circuits $\mathcal{U}$ on n qubits. The task is to sample from $p_U(x) := |\langle x|U|0\rangle|^2$ for most circuits $U \in \mathcal{U}$.

Ref. [92] proved that an efficient (in terms of n) classical algorithm for this task for random circuits would also collapse the polynomial hierarchy. As every realistic quantum experiment will be somewhat noisy, it is relevant to consider a variant of this task allowing for small deviations from ideal. One possible formulation is the following:

ε-Approximate Random Circuit Sampling: The input is a set of quantum circuits $\mathcal{U}$ on n qubits. The task is to sample for most circuits $U \in \mathcal{U}$, from any distribution q_U s.t. $d_{\mathrm{VD}}(q_U, p_U) \leq \varepsilon$, where $d_{\mathrm{VD}}(p, q)$ is the variational-distance between the distributions p, q [103] and $p_U(x) := |\langle x|U|0\rangle|^2$.

Refs. [90, 91, 27] put forward new complexity-theoretic assumptions about the #P-hardness of certain problems and proved they imply that several restricted classes of circuits are hard to approximately sample for ε sufficiently close to zero. However, we cannot use these results here as the ε we achieve is far from zero. We will resort to the following different variant of approximate circuit sampling.

Unbiased-Noise F-Approximate Random Circuit Sampling: The input is a set of quantum circuits $\mathcal{U}$ on n qubits. The task is to sample from the distribution $r_{U,F}$ given by Eq. (11.112), for most circuits $U \in \mathcal{U}$.

We note that there are alternatives for defining the computational problem for which supremacy is achieved without having to use sampling problems. These have the advantage that it is possible to verify, for each problem instance, that the task was achieved (whereas while it is in principle possible to verify that one is sampling from the correct distribution by estimating the frequencies of outcomes, this is unfeasible in practice for high entropy distributions with $> 2^{50}$ outcomes as the one we consider here).

One such problem (considered on Refs. [30, 27]) is the following:

b-Heavy Output Generation: Given as input a number $b > 1$ and a random circuit U on n qubits (drawn at random from a set of circuits $\mathcal{U}$), generate output strings $x_1, \ldots, x_k$ s.t.

$$\frac{1}{k}\sum_{j=1}^{k} |\langle x_j|U|0\rangle|^2 \geq \frac{b}{2^n} \tag{11.114}$$

Ref. [30] argues for the hardness of this task for every $b > 1$, although here again one has to resort to rather bold complexity-theoretic conjectures. Cross entropy benchmarking allows us to estimate b for a reasonable value of k (though the classical time needed to compute $|\langle x_j|U|0\rangle|^2$ still grows very fast), see Sec. 11.4. In terms of known algorithms, the complexity of solving Heavy Output Generation is equivalent to the complexity of sampling k samples from a noisy distribution corresponding to the same b value.

The experiment we report in this paper can be interpreted as showing quantum supremacy in solving the b-Heavy Output Generation with $b = 1 + F$ and F the fidelity of the output quantum state.

11.11.3 Computational hardness of unbiased-noise sampling

To state our result, we use the complexity class Arthur-Merlin, which is a variant of the class NP and is denoted by AM[T]. It is defined as the class of problems for which there is an Arthur-Merlin one-round protocol of the following form: given an instance of a problem in $AM[T]$ (which Arthur would like to decide if it is a YES or NO instance), Arthur first sends random bits to Merlin. Merlin (which is computationally unbounded) then sends back a proof

to Arthur. Finally Arthur uses the proof and decides in time T if he accepts. In the YES case, Arthur accepts with probability larger than 2/3. In the NO case, he accepts with probability no larger than 1/3.

Теорема 1. *Assume there is a classical algorithm running in time T and using m bits of randomness that samples from the distribution $r_{U,F}(x)$ given by Eq. (11.112), for a given quantum circuit U on n qubits and $F \geq 0$. Then for every integer L, there is an $AM[LT+2Lm]$ protocol for deciding, given $\lambda > 0$, whether*

$$|\langle 0|U|0\rangle|^2 \geq \lambda\left(1+\frac{2}{L}\right)+\frac{2(1-F)}{FL2^n} \tag{11.115}$$

or

$$|\langle 0|U|0\rangle|^2 \leq \lambda\left(1-\frac{2}{L}\right)-\frac{2(1-F)}{FL2^n} \tag{11.116}$$

Before giving the proof, let us discuss the significance of the result. We are interested in the theorem mostly when $L = c/F$ with c a small constant (say 10). Noting that for a random circuit, with high probability, $|\langle 0|U|0\rangle|^2 \geq 2^{-n}/5$ [97], the theorem states that if we can sample classically in time T from the distribution given in Eq. (11.112), then we can calculate a good estimate for $|\langle 0|U|0\rangle|^2$ in time $10T/F$ (with the help from an all-powerful but untrustworthy Merlin). It is unlikely that Merlin can be of any help for this task for random circuits, as estimating $|\langle 0|U|0\rangle|^2$ for random circuits is a #P-hard problem [92], and it is believed #P is vastly more complex than AM (which is contained on the third level of the polynomial hierarchy [98]). Therefore we conclude that global white noise leads to no more than a linear decrease in fidelity in classical simulation time (which is in fact optimal as it is achieved by the method presented in Ref. [38]).

Ref. [104] proposed a similar, but more demanding, conjecture about the non-existence of certain AM protocols for estimating transition probabilities of random circuits. This conjecture was applied to show that the output bits of our supremacy experiment can be used to produce certifiable random bits.

We note Theorem 1 does not establish a lower bound on the classical computation cost of calculating a transition amplitude with additive error $\delta/2^n$, for small constant $\delta > 0$. What it does is to show that the sampling problem with unbiased noise is as hard as this task, up to a linear reduction in F in complexity.

Concerning the hardness of computing $|\langle 0|U|0\rangle|^2$ it is known that this problem is #P hard for random circuits to additive error $2^{-poly(n)}$ [92]. This implies that there is no subexponential-time algorithms for this task (unless #P collapses to P). For finite size bounds, which are more relevant to our experiment, the result of Ref. [99] is the most relevant. It shows that under the Strong Exponential Time Hypothesis (SETH) [105], there are quantum circuits on n qubits which require $2^{(1-o(1))n}$ time for estimating $|\langle 0|U|0\rangle|^2$ to additive error $2^{-(n+1)}$ [106]. Together with Theorem 1, we find there is a quantum circuit U on n qubits for which the distribution $r_{U,F}$ (given by Eq. (11.112)) cannot be sampled in time $F2^{(1-o(1)n)}$, unless SETH is false.

It is an open question to show a similar lower bound to the one proved in Ref. [99] for estimating the transition probability of random circuits. Even more relevant for this work, it would be interesting to study if one can show a lower bound of the form $2^{(1-o(1))\text{treewidth}}$ for a random quantum circuit, under a suitable complexity-theoretic assumption, as the depth of the construction in [99] is relatively high.

11.11.4 Proof of Theorem 1

The proof will follow along similar lines to previous work [90, 91, 95]. We will use approximate counting (which can be done in AM) to show that a sampling algorithm for $r_{U,F}$ running

in time T implies an AM protocol to compute $r_{U,F}(0)(1 \pm 1/L)$, with classical verification of order LT. Since the noise is unbiased, i.e. $r_{U,F}(0) = F\langle 0|U|0\rangle|^2 + (1-F)/2^n$, we can subtract it and find an AM protocol for estimating $|\langle 0|U|0\rangle|^2$ as stated in the theorem.

In more detail, suppose there is a classical algorithm for sampling from $r_{U,F}$ given by a function A mapping $m \in$ poly(n) bits $r = (r_1, \dots r_m)$ to n bits such that

$$\frac{1}{2^m}|\{(r_1, \dots, r_m) \text{ s.t. } A(r_1, \dots, r_m) = x\}| = r_{U,F}(x). \quad (11.117)$$

Let $a(r_1, \dots, r_m)$ be a function which is 1 if $A(r_1, \dots, r_m) = 0^n$ and zero otherwise.

We start with the following lemma, showing the existence of A implies an $AM[LT + 2Lm]$ protocol for estimating $r_{U,F}(0)$:

Lemma. Assume there is an algorithm A given by Eq. (11.117). Then for every θ and L there is an $AM[LT+2Lm]$ protocol which determines if (i) $r_{U,F}(0) \geq \theta(1+2/L)$ (YES instance) or (ii) $r_{U,F}(0) \leq \theta(1-2/L)$ (NO instance).

Proof: The protocol is the following:

1. For every $t \in [Lm]$, Arthur chooses a function at random $h_t \in H_{Lm,t}$ from a family $H_{Lm,t}$ of 2-universal linear hash functions from $\{0,1\}^{Lm}$ to $\{0,1\}^t$ [98]. Then he communicates his choice of $(h_1, \dots, h_{Lm})$ to Merlin.

2. Merlin sends an Lm-bitstring w to Arthur and an integer $s \in [Lm]$.

3. Arthur verifies that $h_s(w) = 0$ and

$$a(w_{1,1}, \dots w_{1,m}) \wedge \dots \wedge a(w_{L,1}, \dots w_{L,m}) = 0.$$

He rejects if any of the three equations is not satisfied. Then he checks if $\theta \leq 2^{-m} 20^{1/L} 2^{s/L} (1 + 2/L)^{-1}$, accepting if it is the case and rejecting otherwise.

The cost to compute $a(w_{1,1}, \dots w_{1,m})$ is T, and the cost to compute is $h_s(w)$ is less than $2Lm$, so the total verification time of the AM protocol is $LT + 2Lm$.

Let us analyze the completeness and soundness of the protocol.

Completeness: Suppose we have a YES instance, $r_{U,F}(0) \geq \theta(1+2/L)$. Let us show that Merlin can send w and s which makes Arthur accept with high probability.

Let M be the number of solutions of $a(r_1, \dots, r_m) = 0$ (i.e. $M = 2^m r_{U,F}(0)$). Then $a(r_{1,1}, \dots r_{1,m}) \wedge \dots \wedge a(r_{L,1}, \dots r_{L,m})$ has M^L solutions, M for each copy of the function a. As part of the proof Merlin sends s satisfying $20 \geq M^L/2^s \geq 10$ (such a value always exists as s can be an arbitrary integer less than or equal to Lm).

Let us apply Lemma 11.11.4 (stated below) with $q = Lm$, $t = s$, $\delta = 1/2$, and S the set of solutions, so $|S| = M^L$. Then indeed $|S|/2^s > 10 > 1/\delta^3$. Therefore, with high probability, the number of solutions of

$$a(x_{1,1}, \dots x_{1,m}) \wedge \dots \wedge a(x_{L,1}, \dots x_{L,m}) \wedge h_s(x) \quad (11.118)$$

is in the interval $[(1/2)M^L/2^s, 2M^L/2^s]$. Since $(1/2)M^L/2^s \geq 1$, there is a string w s.t. $a(w_{1,1}, \dots w_{1,m}) \wedge \dots \wedge a(w_{L,1}, \dots w_{L,m}) \wedge h_s(w) = 0$, which Merlin also sends to Arthur as part of the proof.

Since $M = 2^m r_{U,F}(0) \geq 2^m \theta(1 + 2/L)$ and $M^L/2^s \leq 20$,

$$20 \geq \frac{M^L}{2^s} \geq \frac{2^{Lm}}{2^s} \theta^L \left(1 + \frac{2}{L}\right)^L, \quad (11.119)$$

so indeed $\theta \leq 2^{-m}20^{1/L}2^{s/L}(1+2/L)^{-1}$ and Arthur will accept with high probability.

Soundness: Suppose we have a NO instance, $r_{U,F}(0) \leq \theta(1-2/L)$. Let us show that no matter which witnesses w, s Merlin sends, Arthur will only accept with a small probability. Merlin must send s such that

$$\theta^L \leq (20)2^{-Lm}2^s(1+2/L)^{-L}, \tag{11.120}$$

otherwise Arthur rejects. By Lemma 11.11.4 (stated below), the number of solutions of

$$a(x_{1,1},\ldots x_{1,m}) \wedge \ldots \wedge a(x_{L,1},\ldots x_{L,m}) \wedge h_s(x) \tag{11.121}$$

will be in the interval $[(1/2)M^L/2^s, 2M^L/2^s]$, with $M = 2^m r_{U,F}(0) \leq 2^m\theta(1-2/L)$. Since

$$\begin{aligned} & 2M^L/2^s \leq 2(2^{-s})2^{Lm}\theta^L(1-2/L)^L \\ \leq\ & 40(1-2/L)^L(1+2/L)^{-L} \leq 40e^{-4} < 1, \end{aligned} \tag{11.122}$$

there is no solution to Eq. (11.121) and thus there is no w which will make Arthur accept. This finishes the proof of Lemma 11.11.4.

Reduction to AM protocol for $|\langle 0|U|0\rangle|^2$: Finally let us show how to use Lemma 11.11.4 to build the AM protocol stated in Theorem 1. Since $r_{U,F}(0) = F|\langle 0|U|0\rangle|^2 + (1-F)/2^n$, on one hand:

$$|\langle 0|U|0\rangle|^2 \geq \lambda\left(1+\frac{2}{L}\right) + \frac{2(1-F)}{FL2^n} \tag{11.123}$$

implies that

$$r_{U,F}(0) \geq (F\lambda + (1-F)/2^n)\left(1+\frac{2}{L}\right). \tag{11.124}$$

On the other hand:

$$|\langle 0|U|0\rangle|^2 \leq \lambda\left(1-\frac{2}{L}\right) - \frac{2(1-F)}{FL2^n} \tag{11.125}$$

implies that

$$r_{U,F}(0) \leq (F\lambda + (1-F)/2^n)\left(1-\frac{2}{L}\right). \tag{11.126}$$

Setting $\theta = F\lambda + (1-F)/2^n$ we see that the AM protocol from before can also be used to decide if Eq. (11.123) or Eq. (11.125) hold true. This ends the proof of the theorem.

Lemma. [98] For $t \leq q$, let $H_{q,t}$ be a family of pairwise-independent linear hash functions mapping $\{0,1\}^q$ to $\{0,1\}^t$, and let $\delta > 0$. Let $S \subseteq \{0,1\}^n$ be arbitrary with $|S| \geq \delta^{-3}2^t$. Then with probability larger than 9/10 over the choice of $h \in H_{n,t}$,

$$(1-\delta)\frac{|S|}{2^t} \leq |\{x \in S | h(x) = 0^t\}| \leq (1+\delta)\frac{|S|}{2^t} \tag{11.127}$$

Moreover $h(x)$ can be evaluated in time $2n$, for every $h \in H_{n,t}$.

12 Quantum Probability and Quantum Statistics by Holevo

12.0.1 Introduction

0.1. Конечномерные системы.

Изложение теории вероятностей принято начинать с конечной схемы. Следуя этой традиции, рассмотрим конечное вероятностное пространство Ω. Имеют место три тесно связанных между собой факта, которые по-разному выражают классичность вероятностной схемы:

1. множество событий $A \subset \Omega$ образует булеву алгебру;

2. множество распределений вероятностей $[p_1, \ldots, p_N]$ на Ω является симплексом, т. е. выпуклым множеством, в котором каждая точка однозначно представляется в виде смеси (выпуклой комбинации) крайних точек;

3. множество случайных величин $[\lambda_1, \ldots, \lambda_N]$ на Ω образует коммутативную алгебру (относительно поточечного умножения).

Квантовым аналогом этой схемы является модель N-уровневой системы. Аналог распределения вероятностей- состоя ни е такой системы описывается м а трице й плотностиэрмитовой $N \times N$-матрицей S, удовлетворяющей условиям положительной определенности и единичности следа

$$S \geqslant 0, \operatorname{Tr} S = 1;$$

аналог случайной величины - на блюд а ем а я описывается произвольной эрмитовой $N \times N$-матрицей X. Пусть

$$X = \sum_{j=1}^{n} x_j E_j$$

- спектральное разложение эрмитовой матрицы X, где $x_1 < x_2 < \ldots$ - собственные числа, $E_1, E_2, \ldots$ - проекторы на соответствующие собственные подпространства. Набор $\mathbf{E} = \{E_j\}$ образует ортогональное разложение еди н и ц ы:

$$E_j E_k = \delta_{jk} E_j; \quad \sum_{j=1}^{n} E_j = \mathrm{I}$$

где I - единичная матрица. Из свойств (0.1), (0.3) следует, что соотношение

$$\mu_S^X(x_j) = \operatorname{Tr} S E_j; \quad j = 1, \ldots, n$$

задает распределение вероятностей на спектре $\mathrm{Sp}X = \{x_1, x_2, \ldots\}$ наблюдаемой X; в квантовой механике постулируется, что это есть распределение вероятностей наблюдаемой X в состоянии S.

В частности, среднее значение X в состоянии S есть

$$\mathrm{E}_S(X) = \operatorname{Tr} SX$$

Если в этой модели ограничиться рассмотрением только диагональных матриц

$$S = \begin{bmatrix} p_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & p_N \end{bmatrix}, \quad X = \begin{bmatrix} \lambda_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda_N \end{bmatrix},$$

то мы возвращаемся к классической схеме с N элементарными событиями, где, в частности, (0.5) сводится к $\mathbf{E}_S(X) = \sum_{j=1}^{N} p_j \lambda_j$. То же самое мы получили бы, рассматривая только одновременно диагонализуемые, т. е. коммутирующие (перестановочные между собой) матрицы. Поскольку имеются наблюдаемые, описываемые некоммутирующими матрицами, модель N-уровневой системы не сводится к классической схеме.

Роль индикаторов событий в квантовом случае играют наблюдаемые, принимающие значения 0 или 1, т. е. эрмитовы идемпотентные матрицы: $E^2 = E$. Вводя унитарное координатное пространство $\mathscr{H} = \mathbf{C}^N$, в котором действуют $N \times N$-матрицы, такую матрицу E можно рассматривать как ортогональный проектор на подпространство $\mathscr{E}$ в $\mathscr{H}$. Таким образом, кв ан тов ы е собы тия можно отождествить с подпространствами унитарного пространства . Множество квантовых событий, называемое кв а нтовой логикой, частично упорядочено (по включению) и наделено операциями $\mathscr{E}_1 \bigvee \mathscr{E}_2$ (линейная оболочка подпространств $\mathscr{E}_1, \mathscr{E}_2$), $\mathscr{E}_1 \wedge \mathscr{E}_2$ (пересечение подпространств $\mathscr{E}_1, \mathscr{E}_2$), $\mathscr{E}'$ (ортогональное дополнение) с известными свойствами. Неклассичность модели N-уровневой системы можно выразить тремя различными утверждениями:

1. квантовая логика событий не является булевой алгеброй, поскольку в ней не выполнено тождество дистрибутивности

$$\mathscr{E}_1 \wedge (\mathscr{E}_2 \backslash \mathscr{E}_3) = (\mathscr{E}_1 \wedge \mathscr{E}_2) \vee (\mathscr{E}_1 \wedge \mathscr{E}_3)$$

Вследствие этого, нет «элементарных событий», на которые однозначно распадалось бы любое квантовое событие;

2. выпуклое множество состояний не является симплексом, т. е. представление матрицы плотности в виде смеси крайних точек неоднозначно;

3. комплексная оболочка множества наблюдаемых является некоммутативной (ассоциативной) алгеброй.

В бесконечномерном случае вместо матриц приходится расчатривать операторы, действующие в некотором гильбертовом пространстве $\mathscr{C}$. Математически корректное изложение основных понятий квантовой механики в гильбертовом пространстве было впервые дано Дж. фон Нейманом [26]. Он, в частности, подчеркнул существенное различие между эрмитовыми (симметричными) и самосопряженными операторами, которое, ко- нечно, не проводилось в предшествовавших физических работах и указал, что именно условие самосопряженности обеспечивает в случае $\dim \mathscr{H} = \infty$ аналог спектрального разложения (0.2). Другой круг вопросов в случае $\dim \mathscr{H} = \infty$ связан с уточнением понятия следа и соответствующего класса операторов с конечным следом. Математическая схема, называемая ст андарт но й формулировкой квантовой механики в гильбертовом пространстве, рассматривается в гл. 1.

0.2. Общие постулаты статистического описания. Каждая из математических структур - квантовая логика событий, выпуклое множество состояний и алгебра квантовых наблюдаемых -может быть охарактеризована определенной системой аксиом, но возникающие при этом характеризационные проблемы оказываются совсем не тривиальными и по существу составляют отдельные направления исследований, обзор которых выходит за рамки настоящей статьи (см., в частности, Сигал [32], Макки [23], Варадарайан [160], Людвиг [125], Гаддер [95]). Имея дело с конкретным объектом - квантовой теорией вероятностей в гильбертовом пространстве, не приходится прибегать к тем или иным системам аксиом; более того, именно знание структурных особенностей этого объекта и дает основание для мотивировки той или иной аксиомы. Одним из полезных уроков аксиоматического подхода является, однако, указание на плодотворный параллелизм в описании классических и квантовых систем. Формулируемые ниже положения являются модификацией первых четырех аксиом Макки, одинаково применимых как к классическим, так и квантовым системам.

(I) Заданы множество (5, элементы которого называются состояниями и множество D, элементы которого называются (вещественными) наблюдаемыми. Для любой пары S, XS задано распределение вероятностей $\mu_{SX}(\,\mathrm{d}x)$ на σ-алгебре $\mathscr{B}(\mathbf{R})$ борелевских подмножеств вещественной прямой $\mathbf{R}$, называемое распределением вероятностей наблюдаемой X в состоянии S.

Состояние S интерпретируется как более или менее детальное описание приготовления ст а ти сти че ск ого а н с а м бля независимых индивидуальных представителей рассматриваемой системы, а наблюдаемая X - как величина, измеряемая определенным прибором для каждого представителя в данном ансамбле. Аксиома (1), таким образом, предполагает воспрои з в о д и мость индивидуальных экспериментов и устой ч и в о с т ь ч а с т о т при их независимых повторениях. Следующая аксиома выражает возможность с м е ш и в ан и я ансамблей.

(II) Для любых $S_1, S_2 \in$ и любого числа $p, 0 < p < 1$, существует $S \in$, takoe, что

$$\mu_S^X = p\mu_{s_1}^X + (1-p)\mu_{s_2}^X.$$

для всех $X \in \mathcal{N}$; S называется смесью состояний S_1, S_2 в пропорции $p : (1-p)$.

Следующая аксиома говорит о возможности преобразования информации, полученной при измерении наблюдаемой. Пусть f борелевская функция из $\mathbf{R}$ в $\mathbf{R}$. Если $X_1, X_2 \in \supset$ таковы, что для ВСеХ $S \in S$

$$\mu_S^{X_2}(B) = \mu_S^{X_1}\left(f^{-1}(B)\right); \quad B \in \mathscr{B}(\mathbb{R})$$

где $f^{-1}(B) = \{x : f(x) \in B\}$, то наблюдаемая X_2 функционально подинена наблюдаемой X_1. В этом случае будем писать $X_2 = f \circ X_1$.

(III) Для любой $X_1 \in S'$ и любой борелевской функции f существует $X_2 \in \mathcal{N}$, такая что $X_2 = f \circ X_1$.

Пару непустых множеств (,), удовлетворяющих аксиомам (I)-(III), назовем статистической моделью. Статистическая модель называется отделимой, если

(IV) Из того, что $\mu_S^{X_1} = \mu_S^{X_2}$ для всех $X \in \mathrm{Im}$ следует $S_1 = S_2$; из того, что $\mu_S^{X_1} = \mu_S^{X_2}$ для всех $S \in \subseteq$ следует $X_1 = X_2$.

Для отделимой модели операция смешивания в и отношение функциональной подчиненности в $\supseteq$ определены однозначно. Тем самым множество состояний $\subseteq$ наделяется выпуклой структурой, а множество наблюдаемых $\subseteq$ получает частичную упорядоченность.

Наблюдаемые $X_1, \ldots, X_m$ называются совместимьми, если они функционально подчинены некоторой наблюдаемой X, т. е. $X_j = f_j \circ X; j = 1, \ldots, m$. Совместимые наблюдаемые могут быть измерены в одном эксперименте. Наблюдаемые, совместимые со

всеми наблюдаемыми $X \in D$, образуют *центр* статистической мо-

дели. Запас элементов в центре определяет степень классичности модели.

0.3. Классические и квантовые системы. Пусть $(\Omega, (\Omega))$ - измеримое пространство, $\mathrm{Re}(\Omega)$ - выпуклое множество всех вероятностных мер на Ω, а $\Omega(\Omega)$ совокупность всех вещественных случайных величин с естественным отношением функциональной подчиненности. Пусть

$$\mu_P^X(B) = P\left(X^{-1}(B)\right) : B \in \mathscr{B}(\mathbf{R})$$

- распределение вероятностей $X \in D(\Omega)$ относительно $P \notin \mathrm{Re}(\Omega)$. Пара $(\mathfrak{P}(\Omega), \mathscr{D}^-(\Omega))$ образует отделимую статистическую модель, которую можно назвать колмогоров с кой. В этой модели все наблюдаемые совместимы и центр совпадает с $\Omega(\Omega)$. Для

простоты продемонстрируем совместимость наблюдаемых с конечным множеством значений. Всякая такая наблюдаемая имеет представление, аналогичное (0.2)

$$\therefore (\omega) = \sum_{j=1}^{n} x_j E_j(\omega)$$

где $E_j(\omega)$ есть индикатор множества $B_j = \{\omega_1 : X(\omega) = x_j\}$. Множества B_j образуют разбиение пространства Ω, а $\{E_j(\omega)\}$ яв- ляются аналогом ортогонального разложения единицы (0.3). Если $X_1, \ldots, X_m$ - произвольный набор таких наблюдаемых, то достаточно взять разбиение $\{B_j\}$ более мелкое, чем все разбиения, соответствующие наблюдаемым X_i, чтобы было возможно представить все X_i как функции наблюдаемой X, соответствующей такому разбиению $\{B_j\}$.

Статистическая модель N-уровневой квантовой системы фактически была описана в п. 1. Если наблюдаемая X имеет спектральное разложение (0.2), то наблюдаемая $f \circ X$ определяется как

$$f \circ X = \sum_{j=1}^{n} f(x_j) E_j$$

Квантовые наблюдаемые $X_1, \ldots, X_m$ совместимы тогда и только тогда, когда соответствующие матрицы перестановочны, т. е.

$$X_i X_j = X_j X_i; i, j = 1, \ldots, m$$

Центр такой модели тривиален: он состоит из матриц, кратных единичной, т. е. только из постоянных наблюдаемых.

Для совместимых наблюдаемых естественно вводится совместное распределение вероятностей относительно любого состояния S. Если же $X_1, \ldots, X_m$ несовместимы, то совместное распределение относительно произвольного состояния не существует. Это обстоятельство отражает квантовый п р инци п до пол н и те льности. Физические измерения над микрообъектами осуществляются макроскопическими экспериментальными установками, каждая из которых предполагает (ложную и специфичную организацию пространственно-временной среды. Разные способы такой организации, отвечающие разным наблюдаемым, могут быть взаимно исключающими (хотя и относятся к одному и тому же микрообъекту), т. е. дополнительными. Наличие обширного запаса несовместимых наблюдаемых - первое из основных отличий квантовой статистики от классической.

Один из наиболее спорных вопросов квантовой теории проблема скрытых параметров, т. е. вопрос о принципиальной возможности описания квантовой статистики в терминах классического вероятностного пространства. Первая попытка доказательства невозможности введения скрытых параметров была предпринята Дж. фон Нейманом в [26] и долгое время его аргументы рассматривались как решающие. В 1966 г. Дж. Белл обратил внимание на их неполноту и указал на другое фундаментальное свойство квантовомеханического описания, которое можно обозначить как свойство ц елостностй [11]. Математически оно связано с принципом суперпозиции и с тем обстоятель-

1. Английский термин - поп-separability. ством, что составные квантовые системы описываются с помощью тензорного, а не декартова произведения, как в классической теории вероятностей. Свойства дополнительности и целостности лежат в основе негативных результатов в проблеме скрытых параметров, которые обсуждаются в конце гл. 1.

0.4. Рандомизация в классической и квантовой статистике. Вернемся к колмогоровой модели и рассмотрим случайную величину (0.6). В каждой точке $\omega \in \Omega$ она с вероятностью 1 принимает одно из значений x_j. В математической статистике, в частности в теории статистических решений полезно рассмотрение «рандомизованных» случайных величин, которые определяются указанием вероятностей $M_j(\omega), (0 \leqslant M_j(\omega) \leqslant 1)$ принятия значения x_j для любого элементарного события ω. Набор функций $\mathbf{M} = \{M_j(\omega))$ характеризуется условиями

$$M_j(\omega) \geqslant 0; \quad \sum_{j=1}^{n} M_j(\omega) = 1; \quad \omega \in \Omega$$

и описывает неточное измерение случайной величины X, т. е. измерение со случайными ошибками. Распределение вероятностей такого измерения относительно вероятностной меры P дается формулой

$$\mu_P^M(x_j) = \int_\Omega P(d\omega) M_j(\omega)$$

В частности, измерение является точным (безошибочным), если $M_j(\omega) = E_j(\omega)$. Таким образом возникает другая классическая статистическая модель, которую по имени создателя теории статистических решений можно назвать моделью В альда.

Естественно рассмотреть квантовый аналог модели Вальда, в которой наблюдаемая с конечным множеством значений описывается конечным разложение м единицы, т. е. семейством матриц (операторов) $\mathbf{M} = \{M_j\}$, удовлетворяющим условням

$$M_j \geqslant 0; \quad \sum_{j=1}^{n} M_j == \mathrm{I}$$

Вероятность j-го исхода в состоянии S определяется формулой, аналогичной (0.9)

$$\mu_S^M(x_j) = \operatorname{Tr} S M_j$$

Эти определения естественно переносятся и на наблюдаемые с произвольным множеством значений. Так возникает обобщен ная с т а ти с тическая модель квантовой механики (см. §2.1).

Общие разложения единицы в квантовой теории появляются на рубеже 70 -х годов. К этому независимо приводят исследова- ния по квантовой аксиоматике (Г. Людвиг), по проблеме воспроизводимости, связанной с повторными измерениями (Э. Б. Дэвис и Дж. Льюис); по квантовой теории статистических решений (А. С. Холево) и другие работы. Обобщенная статистическая модель квантовой механики является логическим следствием ее вероятностной структуры и дает основу для рассмотрения ряда вопросов, не находящих удовлетворительного решения в рамках стандартной формулировки.

0.5. Выпуклая геометрия разложений единицы и фундаментальные пределы точности. Хотя описанное выше расширение понятия наблюдаемой формально аналогично введению рандovизованных величин в классической статистике, неортогональные разложения единицы имеют в квантовой теории принципиально более важное значение, нежели просто средство описания неточных измерений. Дело в том, что и с математической, и с физической точек зрения наибольший интерес представляют крайние точки выпуклого множества разложений единицы (0.10), описывающие статистику предельно точных и максимально информативных измерений. В классическом случае крайние точки множества (0.8) совпадают с нерандомизованными процедурами $\{E_j(\omega)\}$, соответствующими обычным случайным величннам. Однако в

квантовом случае крайние точки множества (0.10) при $n > 2$ уже не исчерпываются ортогональными разложениями единицы. Следовательно, для описания предельно точных квантовых измерений требуются, в общем случае, неортогональные разложения единицы.

С другой стороны, как показал М. А. Наймарк (1940), произвольное разложение единицы расширяется до ортогонального в некотором объемлющем гильбертовом пространстве. Это позволяет истолковать неортогональное разложение единицы как обычную наблюдаемую в расширении исходной квантовой системы, содержащем независимую дополнительную систему. Таким образом, измерение над расширением может быть более точным и информативным, чем любое прямое квантовое измерение. Этот парадоксальный с точки зрения классической статистики факт связан с затронутым в п. 3 квантовым свойством целостности.

В 1940 -50 годы в работах Д. Габора и Л. Бриллюэна было высказано предположение, что квантово-механическая природа канала связи должна налагать фундаментальные ограничения на скорость передачи и точность воспроизведения информации. Этот вопрос приобрел актуальность в 60-е годы с появлением квантовых каналов связи - систем передачи информации, основанных на свойствах когерентного лазерного излучения. В 70-е годы была создана последовательная квантовая теория статистических решений, которая дает принципиальную основу для рассмотрения вопросов предельной точности и информативности измерений (см. К. Хелстром [37], А. С Холево [43]).

В этой теории решающие процедуры - измерения описываются разложениями единицы в гильбертовом пространстве системы и решаются задачи об отыскании экстремума некоторого функционала (меры точности, шенноновской информации) в классе квантовых решающих процедур, обычно подчиненных дополнительным ограничениям (несмещенности, ковариантности и т. п.) (см. гл. 2).

0.6. Проблема соответствия. Одна из трудностей в стандартной формулировке квантовой механики состоит в невозможности сопоставления некоторым величинам, таким как время, угол, фаза и т. п. самосопряженного оператора в гильбертовом пространстве системы. Причина кроется в теореме единственности Стоуна-фон Неймана, которая налагает жесткие ограничения на спектры канонически сопряженных наблюдаемых.

К этому же кругу вопросов можно отнести и трудности с локализуемостью (т. е. введением ковариантных наблюдаемых положения) для релятивистских квантовых частиц с нулевой массой. Рассмотрение в качестве наблюдаемых неортогональных разложений единицы, подчиненных условиям ковариантности, аналогичных коммутационным соотношениям Вейля в теореме Стоуна-фон Неймана, позволяет в значительной степени избежать этих трудностей (см. гл. 2). В спектральной теории неортогональные разложения единицы возникают как обобщенные спектральные меры несамосопряженных операторов. В соответствии с этим, например, оператор, отвечающий наблюдаемой времени, оказывается максимальным эрмитовым (но не самосопряженным). Можно сказать, что обобщенная статистическая модель квантовой механики на новом математическом уровне оправдывает «наивное» представление о вещественной наблюдаемой, как об эрмитовом, но не обязательно самосопря. женным, операторе.

0.7. Повторные и непрерывные измерения. В колмогоровской модели преобразования состояний системы могут быть описаны с помощью условных вероятностей. Пусть в результате измерения случайной величины (0.6) получено значение x_j. При этом классическое состояние, т. е. вероятностная мера $P(d_\omega)$ на Ω преобразуется по формуле

$$P(A) \to P\left(A|B_j\right) = \frac{\int\limits_A P(d\omega)E_j(\omega)}{\int\limits_\Omega P(d\omega)E_j(\omega)}; \quad A \in \mathscr{B}(\Omega)$$

Очевидно, что если результат измерения не принимается во внимание, то состояние P вообще не изменяется:

$$P(A) \to \sum_{j=1}^{n} P\left(A|B_j\right) P\left(B_j\right) = P(A)$$

В квантовой статистике ситуация качественно более сложна. Аналогом преобразования (0.12) является знаменитый п роекц и он н ый п о с т у л а т Дж. фон Неймана

$$S \to S_j = \frac{E_j S E_{ij}}{\operatorname{Tr} S E_j}$$

где S оператор плотности состояния перед измерением, а S_j после измерения наблюдаемой (0.2), в результате которого получено значение x_j. Основанием для этого постулата служит феноменологическая гипотеза воспроизводимости, подразумевающая предельную точность и минимальность возмущения, вносимого измерением наблюдаемой X. Если результат измерения не принимается во внимание, то состояние S преобразуется по формуле, аналогичной (0.13):

$$S \to \sum_{j=1}^{n} S_j \mu_S^X\left(x_j\right) = \sum_{j=1}^{n} E_j S E_j$$

Однако в общем случае $\sum\limits_j E_j S E_j \neq S$; это означает, что изменение состояния в ходе квантового измерения не сводится только к преобразованию информации и отражает также принципиально неустранимое и необратимое физическое воздействие измерительного прибора на наблюдаемую систему. С проекционным постулатом связан целый ряд проблем; не затрагивая вопросов философского характера, которые выходят за пределы вероятностной интерпретации, остановимся на конкретных проблемах, которые успешно решаются в рамках обобщенной статистической модели квантовой механики.

Принципиальную трудность представляет формулировка проекционного постулата для наблюдаемых с непрерывным спектром. Для описания изменения состояния при произвольном квантовом измерении Э. Б. Дэвис и Дж. Льюис (1970) ввели понятие инструмента - меры со значениями в множестве преобразований квантовых состояний. Этим понятием охватываются и неточные измерения, не удовлетворяющие условию воспроизводимости, что позволяет включить и случай непрерывного спектра. С каждым инструментом связано разложение единицы, причем инструментам, возникающим из проекционного постулата, отвечают ортогональные разложения единицы. Понятие инструмента открывает возможность описания статистики любой последовательности квантовых измерений.

Новое освещение получает вопрос о траекториях, восходящий к фейнмановской формулировке квантовой механики. Процесс непрерывного (во времени) измерения квантовой наблюдаемой можно представить как предел «серий» последовательных неточных измерений. Математическое описание такого предела обнаруживает замечательные аналогии с классической схемой суммирования случайных величин, .

функциональными предельными теоремами в теории вероятностей и представлением Леви-Хинчина для процессов с независимыми приращениями (см. гл. 4).

0.8. Необратимая динамика. Обратимая динамика изолированной квантовой системы описывается уравнением

$$S \to U_t S U_t^{-1}; \quad -\infty < t < \infty,$$

где $\{U_t\}$-группа унитарных операторов. Если система является отк ры то й, т. е. взаимодействует с окружением, то ее эволюция является, как правило, необратимой. Пример такого необратимого изменения состояния, обусловленного взаимодействием с измерительным прибором, дается соотношением (0.15). Наиболее общий вид динамического отображения, задающего конечную эволюцию открытой системы, включает как (0.16), так и (0.15):

$$S \to \sum_j V_j S V_j^*$$

где $\sum\limits_j V_j^* V_j = \mathrm{I}$. Среди всевозможных аффинных преобразований выпуклого множества состояний, отображения (0.17) выделяются специфически некоммутативным свойством полно й по ложительности, возникшим и играющим важную роль в современной теории операторных алгебр.

Непрерывная марковская эволюция открытой системы описывается дин а ми че ской полугр у ппо й, т. е. полугруппой динамических отображений, удовлетворяющей определенным условиям непрерывности (см. Э. Б. Дэвис [78]). Динамические полугруппы являются некоммутативным аналогом марковских полугрупп в теории вероятностей. В 1976 г. Г. Линдблад и независимо, в конечномерном случае, В. Горини, А. Коссаковский и Э. Сударшан получили полное описание инфинитезимального оператора непрерывной по норме динамической полугруппы. Этот результат, лежащий в основе многих фактов теории квантовых случайных процессов, рассматривается в гл. 3.

0.9. Квантовые случайные процессы. Одним из стимулов возникновения теории квантовых случайных процессов послужила проблема р а сши рен и я динамической полугруппы до обратимой динамики «большой системы», включающей открытую систему и окружение. Возможность такого расширения означает, в частности, согласованность понятия динамической полугруппы с основным динамическим принципом квантовой механики, выраженным соотношением (0.16).

В теории вероятностей подобное расширение марковской полугруппы до группы временных сдвигов в пространстве траекторий, соответствующих марковскому случайному процессу, осуществляется известной конструкцией Колмогорова-Даниэля. Понятие квантового случайного процесса, играющее важнуюроль в проблеме расширения динамической полугруппы, было сформулировано Л. Аккарди, А. Фриджерио и Дж. Льюнсом (1980). Роль марковского свойства особенно подчеркивалась Л. Аккарди. В 80-е годы теория квантовых случайных процессов превратилась в обширное самостоятельное поле исследований (см., в частности, сборники [141]-[145]).

Аналитический аппарат кв антового стохастического и с ч и с ле н и я, позволяющий, в частности, строить нетривиальные классы квантовых случайных процессов и конкретные расширения динамических полугрупп, был предложен Р. Л. Хадсоном и К. Р. Партасарати (1982). Квантовое стохастическое исчисление возникает на пересечении двух концепций - временной фильтрации в смысле теории случайных процессов и вторичного квантования в пространстве Фока. В конце 60-х годов Р. Стритер и Х. Араки указали на структуру непрерывного тензорного произведения, которая лежит в основе связи между безграничной делимостью, процессами с независимыми приращениями и

пространством Фока. Благодаря этому, пространство Фока оказывается носителем процессов «квантового шума», которые дают универсальную модель окружения открытой квантовой системы. Квантовое стохастическое исчисление представляет интерес и с точки зрения классической теории случайных процессов. Оно перебрасывает мост между исчислением Ито и вторичным квантованием, открывает неожиданные связи между непрерывными и скачкообразными процессами, позволяет по-новому взглянуть на понятие стохастического интеграла. Наконец, на этой основе развиваются потенциально важные приложения, относяшиеся к теории управления и фильтрации для квантовых случайных процессов (см. гл. 5).

12.1 Standard Statistical Model of Quantum Mechanics

12.1.1 1. Basic Concepts

1.1. Операторы в гильбертовом пространстве.

Изложению теории операторов в гильбертовом пространстве, в значительной мере стимулированной проблемами квантовой механики, посвящено много прекрасных книг (см., в частности, [2], [30]). Ниже мы лишь напоминаем некоторые факты и фиксируем обозначения.

Далее $\mathscr{C}$ обозначает сепарабельное комплексное гильбертово пространство. Для скалярного произведения в $\mathscr{C}$ используется дираковское обозначение $\langle\varphi|\psi\rangle$, причем считается, что форма $\langle\varphi|\psi\rangle$ линейна по ψ и антилинейна по φ. Символ $|\psi\rangle\langle\varphi|$ обозначает оператор, действующий на вектор $\chi \in \mathscr{H}$ по формуле

$$|\psi\rangle\langle\varphi|\chi = \psi\langle\varphi|\chi\rangle.$$

В частности, если $\langle\psi|\psi\rangle = 1$, то $|\psi\rangle\langle\psi|$ есть проектор на вектор $\psi \in \mathscr{H}$. Линейная оболочка множества операторов вида $|\psi\rangle\langle\varphi|$ совпадает с множеством операторов конечного ранга в $\mathscr{H}$.

Если X-ограниченный оператор в $\mathscr{H}$, то X^* обозначает $c0$ пряженный оператор, определяемый соотношением

$\langle\varphi|X^*\psi\rangle = \langle X\varphi|\psi\rangle; \varphi, \psi \in \mathscr{H}$.

$$\langle\varphi|X^*\psi\rangle = \langle X\varphi|\psi\rangle; \quad \varphi, \psi \in \mathscr{H}$$

вал огех огиченных операторов в $\mathscr{C}$ является банаховой алгеброй с инволюцией *. Оператор $X \in \mathscr{B}(\mathscr{B})$ эрмитов, если $X = X^*$. Унитарныц оператором называется оператор U, такой что $U^*U = UU^* = \mathrm{I}$, где I- единичный оператор. Проектором называется эрмитов оператор E, такой что $E^2 = E$. Эрмитов оператор X положителен ($X \geqslant 0$), если $\langle\psi|X\psi\rangle \geqslant 0$ для всех $\psi \in \mathscr{H}$. Для положительного оператора однозначно определен положительный квадратный корень.

Для всякого ограниченного положительного оператора T однозначно определен след

$$\operatorname{Tr} T = \sum_{i=1}^{\infty} \langle e_i|Te_i\rangle \leqslant +\infty$$

где $\{e_i\}$ произвольный ортонормированный базис. Оператор T называется ядерныц (оператором со следом), если он является линейной комбинацией положительных операторов с конечным следом. Для такого оператора след определяется однозначно, как сумма абсолютно сходящегося ряда вида (1.1). Множество ядерных операторов $\mathfrak{T}(\mathscr{H})$ является банаховым пространством относительно нормы $\|T\|_1 = \operatorname{Tr}\sqrt{T^*T}$, причем множество операторов конечного ранга плотно в $\mathfrak{I}(\mathscr{H})$.

Множество $\mathfrak{I}(\mathscr{C})$ образует двусторонний идеал в алгебре $\mathfrak{B}(\mathscr{H})$. Сопряженное к банахову пространству $\mathfrak{T}(\mathscr{C})$ изоморфно $\mathfrak{B}(\mathscr{G})$, причем двойственность определяется билинейной формой

$$\langle T, X\rangle = \operatorname{Tr} TX; \quad T \in \mathfrak{T}(\mathscr{H}), \quad X \in \mathscr{B}(\mathscr{H}).$$

Нижний индекс h в обозначении множества операторов означает, что рассматривается соответствуюшее подмножество эрмитовых операторов, например, $\mathfrak{B}_h(\mathscr{H})$ есть вещественное банахово пространство ограниченных эрмитовых операторов в $\mathscr{C}$. Отметим, что $\mathfrak{T}_h(\mathscr{H})* = \mathfrak{V}_h(\mathscr{C})$, причем двойственность по-прежнему задается формой (1.2).

Кроме сходимости по операторной норме в $\mathscr{O}(\mathscr{H})$, часто используются более слабые понятия сходимости. Последовательность $\{X_n\}$ сходится к X сильно, если $\lim \|X_n\psi - X\psi\| = 0$ для всех $\psi \in \mathscr{H}$, слабо, если $\lim_{n\to\infty} \langle\varphi|X_n\psi\rangle = \langle\varphi|X\psi\rangle$ для всех $\varphi, \psi \in \mathscr{C}$, и w^*-слабо (ультраслабо), если $\lim \operatorname{Tr} TX_n = \operatorname{Tr} TX$ для, всех $T \in \mathfrak{Z}(\mathscr{Z})$. Если $\{X_n\}$ ограниченная по норме последовательность операторов, такая что $X_n \leqslant X_{n+1}$, то X_n сходится сильно, слабо и w* - слабо к ограниченному оператору X (обозначается $X_n \uparrow X$).

1.2 Оператор плотности.

Так называется всякий положительный оператор S с единичным следом:

$$S \geqslant 0; \operatorname{Tr} S = 1.$$

Множество операторов плотности $\subseteq$ $(\mathscr{H})$ является выпуклым подмножеством вещественного линейного пространства $\mathfrak{T}_h(\mathscr{C})$; более, того, оно является основанием конуса положительных элементов, порождающего $\mathfrak{T}_h()$. Точка S выпуклого множества $\odot$ называется крайней, если из того, что $S = pS_1 + (1-p)S_2$, где $S_1, S_2 \in \mathcal{G}, 0 < p < 1$, следует $S_1 = S_2 = S$. Крайними точками множества $\odot(\mathscr{H})$ являются одномерные проекторы

$$S_\psi = |\psi\rangle\langle\psi|,$$

где $\psi \in \mathscr{H}, \langle\psi|\psi\rangle = 1$. Всякий оператор плотности представим в виде счетной выпуклой комбинации

$$S = \sum_{j=1}^{\infty} p_j \,|\psi_j\rangle\,\langle\psi_j|$$

где $\langle\psi_j|\psi_j\rangle = 1, p_j \geqslant 0, \sum\limits_{j=1}^{\infty} p_j = 1$. Одно из таких представлений дается спектральным разложением оператора S, когда ψ_j явля ются его собственными векторами, а p_j соответствующими собственными числами.

Рассмотрим множество $\mathscr{E}(\mathscr{H})$ проекторов в $\mathscr{H}$, изоморфное квантовой логике событий (замкнутых линейных подпространств $\mathscr{H}$). *Вероятностной мерой* на $\mathfrak{E}(\mathscr{H})$ называется вещественная функция μ со свойствами: 1)$0 \leqslant \mu(E) \leqslant 1, E \in (\mathscr{H})$; 2) если $\{E_j\} \subset\Subset (\mathscr{H})$, причем $E_jE_k = 0$ при $j \neq k$ и $\sum\limits_j E_j = \mathrm{I}$, то

$$\sum_j \mu\,(E_j) = \mathrm{I}$$

Отвечая на вопрос Макки, Глисон (1957) доказал следуюшую теорему.

Т е о ре ма. Пусть $\dim \mathscr{H} \geqslant 3$. Тогда всякая вероятностная мера на $\leftleftarrows$ () имеет вид

$$\mu(E) = \operatorname{Tr} SE$$

где S - однозначно определяемый оператор плотности.

Случай $\dim \mathscr{H} = 2$ является особым - для него легко указать меры, не представимые в виде (1.4), однако они не используются в квантовой теории. Доказательство теоремы Глисона совершенно нетривиально и породило целое направление в некоммутативной теории меры, посвященное всевозможным обобщениям и упрощениям этой теоремы (см. обзор Кручиньского в [141]).

По поводу некоммутативной теории меры и интегрирования см. обзоры Ш. А. Аюпова и А. Н. Шерстнева и другие статьи в сборниках [18], [34].

1.3 Спектральная мера.

Пусть $\mathscr{X}$ множество с б-алгеброй измеримых подмножеств $\mathscr{B}(\mathscr{L})$. Ортогональжым разложением единиц в $\mathscr{H}$ называется проекторно-значная мера на $\mathscr{B}(\mathscr{X})$,

т. е. функция множеств $\mathbf{E} : \mathscr{B}(\mathscr{X}) \to \mathfrak{C}(\mathscr{H})$, удовлетворяющая

условиям:

1. если $B_1, B_\varepsilon \in \mathscr{B}(\mathscr{H})$ и $B_1 \cap B_2 = \varnothing$, то $E(B_1)\, E(\mathrm{B}_2) = 0$;

2) если $\{B_j\}$ - конечное или счетное разбиение $\mathscr{X}$ на попарно-непересекающиеся измеримые подмножества, то

где ряд сходится сильно.

$$\sum_j E(B_j) = \mathrm{I}$$

Пусть X-оператор с плотной областью определения $\mathscr{D}(X) \subset \mathscr{O}$. Обозначим $\mathscr{D}(X^*)$ множество векторов φ таких, что существует $\chi \in \mathscr{C}$, для которого

$$\langle \varphi | X\psi \rangle = \langle \chi | \psi \rangle; \psi \in \mathscr{D}(X)$$

Определим оператор X^* с областью определения $\mathscr{D}(X^*)$, полагая $X^*\varphi = \chi$. Оператор X называется эрмитовым (симметрическим), если $X \subseteq X^*$, и самосопрянженным, если $X = X^*$.

Спектральная те орем а (фон Нейман, Стоун, Рисс, 1929-1932) устанавливает взаимно однозначное соответствие между ортогональными разложениями единицы $\mathbf{E}$ на σ-алгебре $\mathscr{B}(\mathbf{R})$ борелевских подмножеств вещественной прямой $\mathbf{R}$ и самосопряженными операторами в $\mathscr{H}$ по формуле

$$X = \int_{-\infty}^{\infty} xE(dx)$$

где интеграл понимается в подходящем смысле (см. [30]). Разложение единицы E называется спектральной мерой оператора X. Для любой борелевской функции f определен самосопряженный оператор

$$f \circ X = \int_{-\infty}^{\infty} xE(dx)$$

спектральная мера $\mathbf{F}$ которого связана со спектральной мерой оператора X соотношением

$$F(B) = E\left(f^{-1}(B)\right), B \in \mathscr{B}(\mathbf{R})$$

Совокупность всех самосопряженных операторов в $\mathscr{H}$ обозначим $D(\mathscr{H})$.

1.4. Статистический постулат. С каждой квантовомеханической системой связывается сепарабельное комплексное гильбертово пространство $\mathscr{H}$. Состояния системы описываются операторами плотности в $\mathscr{H}$. Вещественной наблюдаемой называется лю- бой самосопряженный оператор в $\mathscr{C}$. Распределение вероятностей наблюдаемой X в состоянии S задается соотношением

$$\mu_S^X(B) = \operatorname{Tr} SE(B), \quad B \in \mathscr{B}(\mathbf{R})$$

где $\mathbf{E}$ - спектральная мера X. Определенную таким образом отделимую статистическую модель $((\mathscr{H}), \mathscr{D}(\mathscr{C}))$ будем называть стандартной статистической моделью квантовой механики.

Из (1.5), (1.6) вытекает, что среднее значение наблюдаемой X в состоянии S,

$$\mathrm{E}_s(X) = \int_{-\infty}^{\infty} x\mu_S^X(dx)$$

равно

$$\mathbf{E}_s(X) = \operatorname{Tr} SX$$

(по крайней мере, для ограниченных наблюдаемых).

Крайние точки множества $\subseteq (\mathscr{C})$, описываемые операторами плотности (1.3), называются чистыми состояниями, а вектор ψ называется вектором состояния. Среднее значение наблюдаемой X в таком состоянии равно

$$\mathbf{E}_{s_\psi}(X) = \langle\psi|X\psi\rangle.$$

Допуская вольность речи, ограниченной наблюдаемой иногда называют произвольный $X \in \mathscr{B}(\mathscr{C})$. Соотношение (1.7) определяет линейный положительный нормированный $(\mathrm{E}_s(\mathrm{I}) = 1)$ функционал на алгебре $\mathscr{O}(\mathscr{C})$, т. е. состоян и е в смысле теории алгебр (предыдущие рассуждения поясняют происхождение этого математического термина). Состояние на $\mathscr{B}(\mathscr{C})$, определяемое оператором плотности по формуле (1.7), является нормальным в том смысле, что если $X_n \uparrow X$, то $\mathbf{E}_s(X_n) \to \mathbf{E}_s(X)$.

Алгеброй фон Неймана называется всякая алгебра огранченных операторов в $\mathscr{C}$, содержащая единичный оператор, замкнутая относительно инволюции и предельного перехода в сильной (слабой) операторной топологии. С любой алгеброй фон Неймана $\mathscr{P}$, как и с $\mathfrak{B}(\mathscr{H})$, ассоциируется статистическая модель, в которой состояниями являются нормальные состояния на $\mathscr{P}$, а наблюдаемыми - самосопряженные операторы, присоединенные к $\mathscr{B}$. Такие модели занимают промежуточное положение между квантовой и классическими (соответствующими коммутативным алгебрам $\mathfrak{B}$), и играют важную роль в теории квантовых систем с бесконечно большим числом степеней свободы - полей и сред (см. [7], [9], [51]).

1.5. Совместимые наблюдаемые. Коммутатором ограниченных операторов X, Y называется оператор

$$[X, Y] = XY - YX$$

Операторы $X, Y \in \mathscr{B}(\mathscr{H})$ - перестановочны (коммутируют), если $[X, Y] = 0$. Самосопряженные операторы X, Y называются пере- становочными, если перестановочны их спектральные меры. Следующие утверждения эквивалентны:

1. Наблюдаемые $X_1, \ldots, X_n$ совместимь, т. е. существует наблюдаемая X и борелевские функции $f_1, \ldots, f_n$ такие, что $X_j = f_j \circ X; j = 1, \ldots; n$.

2. Операторы $X_1, \ldots, X_n$ перестановочны.

Если $E_1, \ldots, E_n$ - спектральные меры совместимых наблюдаемых $X_1, \ldots, X_n$, то соотношение

$$E\left(B_1 \times \ldots \times B_n\right) = E_1\left(B_1\right) \cdot \ldots \cdot E_n\left(B_n\right); B_j \in \mathscr{B}$$

однозначно определяет ортогональное разложение единицы $\boldsymbol{E}$ на $\mathscr{B}\left(\mathbf{R}^n\right)$, называемое совместной спектральной мерой операторов $X_1, \ldots, X_n$. Для любого оператора плотности S определено совместное распределение вероятностей наблюдаемых $X_1, \ldots, X_n$

$$\mu \mathrm{iS}_1^{X_1, \ldots, X_n(B)} = \operatorname{Tr} SE(B), B \in \mathscr{B}\left(\mathbb{R}^n\right)$$

Для любой борелевской функции $f\left(x_1, \ldots, x_n\right)$ определена наблюдаемая

$$f\left(x_1, \ldots, \ddot{X}_n\right) = \int_{-\infty}^{\infty} \ldots \int_{-\infty}^{\infty} f\left(x_1, \ldots, x_n\right) E\left(dx_1 \ldots dx_n\right)$$

причем

$$\mathbf{E}_S\left(f\left(\dot{x}_1, \ldots, x_n\right)\right) = \int_{-\infty}^{\infty} \ldots \int_{-\infty}^{\infty} f\left(x_1, \ldots, x_n\right) \times$$
$$\times \mu_{is}^{X_1 \ldots, X_n\left(dx_1 \ldots dx_n\right).}$$

Сушествование несовместимых наблюдаемых отражает квантовый принцип дополнительности. Количественное выражение этого принципа дает соотношение неопределенностей. Для наблюдаемых X, Y, имеющих конечный второй момент относительно состояния S, корректно определяются билинейные формы

$$\langle X, Y\rangle_S = \operatorname{Re} \operatorname{Tr} YSX, [X, Y]_S = 2 \operatorname{Im} \operatorname{Tr} YSX$$

(см. [43, гл. II]). Пусть $\mathbf{X} = [X_1, \ldots, X_n]$ - набор произвольных наблюдаемых с конечным вторым моментом. Введем вещественные матрицы

$$\mathbf{D}_S(\mathbf{X}) = \left[\left\langle X_i - \mathrm{I} \cdot \mathbf{E}_S\left(X_i\right), X_j - \mathrm{I} \cdot \mathbf{E}_S\left(X_j\right)\right\rangle_S\right]_{i,j=1}, \ldots, n$$
$$\mathbf{C}_S(\mathbf{X}) = \left[\left[X_i, X_j\right]_S\right]_{i,j=1}, \ldots, n$$

Из положительной определенности полуторалинейных форм $X, Y \rightarrow \operatorname{Tr} Y^* SX, \operatorname{Tr} XSY^*$ вытекает неравенство [1)]

$$\mathrm{D}_s(\mathrm{X}) \geqslant \pm \frac{i}{2} \mathrm{C}_s(\mathrm{X})$$

1. Впервые такое неравенство было указано Робертсоном (1934); впоследствни оно неоднократно переоткрывалось (см. [17]). где левая и правая части рассматриваются как комплексные эрмитовы матрицы. Для двух наблюдаемых $X = X_1, Y = X_2$ неравенство (1.8) равносильно соотношению неопределенностей Шрёдингера-Робертсона

$$\mathbf{D}_s(X)\cdot\mathbf{D}_s(Y)\geqslant\langle\langle X-\mathrm{I}\cdot\mathbf{E}_s(X),Y-\mathrm{I}\cdot\mathbf{E}_s(Y)\rangle^2+$$
$$+\frac{1}{4}[X,Y]_s^2,$$

где

$$\mathbf{D}_s(\dot{X})=\int\limits_{-\infty}^{\infty}(x-\mathbf{E}_s(X))^2\,\mu_s^X(dx)$$

- дисперсия наблюдаемой X в состоянии S. Если X,Y-совместимые наблюдаемые, то величина

$$\langle X-\mathrm{I}\cdot\mathbf{E}_S(X),Y-\mathrm{I}\cdot\mathbf{E}_s(Y)\rangle_s=$$
$$=\int\limits_{-\infty}^{\infty}\int\limits_{-\infty}^{\infty}(x-\mathbf{E}_S(X))\,(y-\mathbf{E}_s(Y))\,\mu_S^{X,Y}(dxdy)$$

представляет собой ковариацию X,Y в состоянии S; при этом $[X,Y]_S=0$ и (1.9) превращается в неравенство Коши-Шварца для ковариации случайных величин.

Детальный обзор многообразных вариантов и обобщений соотношения неопределенностей см. в [17].

Заметим, что если X,Y - произвольные (ограниченные) операторы, то

$$\langle X,Y\rangle_S=\operatorname{Tr}SX\circ Y$$

где

$$X\circ Y=\frac{1}{2}(XY+YX)$$

- йорданово (симметризованное) произведение операторов X,Y. Величина вида (1.10) в квантовой статистической механике называется корреляцией, хотя если наблюдаемые X,Y не совместимы, она не связана каким-либо простым образом с измерениями X,Y.

1.6. Простейший пример. Пусть $\dim\mathscr{H}=2$. Базис в $\mathscr{D}(\mathscr{C})$ образован матрицами

$$\mathrm{I}=\begin{bmatrix}1&0\\0&1\end{bmatrix},\sigma_1=\begin{bmatrix}0&1\\1&0\end{bmatrix},\quad\sigma_2=\begin{bmatrix}0&-i\\i&0\end{bmatrix},\quad\sigma_3=\begin{bmatrix}1&0\\0&-1\end{bmatrix}$$

где σ_i-матрищь Паули. Полагая $X(\mathbf{a})=\sum\limits_{i=1}^{3}a_i\boldsymbol{\sigma}_i$, где $\mathbf{a}=(a_1,a_2,a_3)\in R^3$, имеем

$$X(\mathbf{a})\cdot X(\mathbf{b})=(\mathbf{a}\cdot\mathbf{b})\mathrm{I}+iX(\mathbf{a}\times\mathbf{b})$$

a, b. Отсюда

$$\operatorname{Tr}X(\mathbf{a})X(\mathbf{b})=2\mathbf{a}\cdot\mathbf{b}$$

Всякая матрица плотности однозначно записывается в виде

$$S(\mathrm{a})=\frac{1}{2}(\mathrm{I}+X(\mathrm{a}))$$

где $|a| \leqslant 1$. Таким образом, $\mathfrak{S}(\mathscr{H})$ как выпуклое множество изоморфно единичному шару в $\mathbf{R}^3$, причем чистые состояния соответствуют точкам сферы $|\mathbf{a}| = 1$. В этом случае

$$S(\mathrm{a}) = |\psi(\mathrm{a})\rangle\langle\psi(\mathrm{a})|$$

где $\psi(a)$-единичный вектор состояния. Поскольку $\langle\psi(a)|\psi(-a)\rangle = 0$, то соотношение

$$X(a) = |\psi(a)\rangle\langle\psi(a)| - |\psi(-a)\rangle\langle\psi(-a)|, (|a| = 1)$$

дает спектральное разложение наблюдаемой $X(\mathbf{a})$. Итак, наблюдаемая $X(\ \mathrm{a})$ принимает значения \pm 1, причем вероятность значения \pm 1 в состоянии $S(\mathbf{b})(|\mathbf{b}| \leqslant 1)$ есть

$$\operatorname{Tr} S(\mathbf{b})S(\pm\mathbf{a}) = \frac{1}{2}(1 \pm \mathbf{a}\cdot\mathbf{b})$$

так что $X(a)$ имеет распределение Бернулли.

В физике конечномерное гильбертово пространство обычно описывает внутренние (спиновые) степени свободы квантовой системы. Случай $\dim\mathscr{H} = 2$ отвечает минимальному спину 1/2. Матрица $\frac{1}{2}X(\mathbf{a})$ описывает наблюдаемую спина в направлении a, а оператор плотности $S(\mathbf{a})(|\mathbf{a}| = 1)$ - «полностью поляризованное состояние», в котором спин в направлении a имеет точное значение $\frac{1}{2}$. Операторы плотности с $|\mathbf{a}| < 1$, представляющие собой смеси полностью поляризованных состояний, описывают «частично поляризованные» состояния, в частности, $\mathrm{a} = 0$ соответствует хаотическому состоянию $S(0) = \frac{1}{2}\mathrm{I}$.

Из соотношения (1.11) следует, что наблюдаемые $X(a)$, X (b) совместимы тогда и только тогда, когда a и $\mathbf{b}$ коллинеарны. С другой стороны, для всех $\mathbf{a}, \mathbf{b} \in \mathbf{R}^3$

$$X(\mathbf{a})X(\mathbf{b}) + X(\mathbf{b})X(\mathbf{a}) = 2(\mathbf{a}\cdot\mathbf{b})\mathrm{I}$$

Фиксируем некоторое состояние и рассмотрим соотношение

$$X(\mathrm{a}) + X(\ \mathrm{b}) = X(\mathrm{a} + \mathrm{b}).$$

Оно показывает, что распределение Бернулли устойчиво по отношению к сложению наблюдаемых, подчиненных соотношению антикоммутации (1.14), и что в квантовой теории вероятностей существует векторное пространство бернуллиевских случайных величин размерности, большей единицы (в обычной теории вероятностей таким свойством обладают только гауссовские случайные величины).

На самом деле такое пространство существует для любой конечной размерности n. Пусть $\mathscr{C}(n)$ - конкретная алгебра Клиффорда, т. е. комплексная алгебра матриц, порождаемая эрмитовыми образующими $X_1, \ldots, X_n$, удовлетворяющими соотношениям

$$X_j^2 = \mathrm{I}, \lambda_j\bar{\Lambda}_k + X_kX_j = 0; k \neq j; k, j = 1, \ldots, n$$

Более точное определение и дальнейшие сведения об алгебрах Клиффорда см., например, в [160]. Полагая $X(\mathrm{a}) = \sum_{j=1}^{n} a_jX_j$ для $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbf{R}^n$, соотношения (1.16) можно записать в форме (1.14). При этом, конечно, выполняется (1.15). Наблюдаемые $X(\mathbf{a}), \mathbf{a} \in \mathbf{R}^n$, принимают только значения $\pm|\mathbf{a}|$ и поэтому имеют распределение Бернулли относительно любого состояния на алгебре $\mathscr{C}(n)$.

На алгебре Клиффорда естественно определяется «бернуллиевское состояние», подобное многомерному гауссовскому распределению в обычной теории вероятностей (т. н. квазисвободное состояние канонических антикоммутационных соотношений [58], [150]).

12.1.2 2. Symmetries, Kinematics, Dynamics

2.1. Группы симметрий.

Рассмотрим отделимую статистическую модель $(\mathfrak{S}, \mathfrak{D})$. Пусть задана пара взаимно однозначных преобразований: Ψ, отображающее ς на $\mathcal{S}$ и Φ, отображающее D на $\mathfrak{D}$, причем

$$\mu_{\Psi(S)}^{\Phi(X)}(B) = \mu_S^X(B); B \in \mathscr{B}(\mathbf{R})$$

для всех $S \in \subseteq, X \in \mathfrak{D}$. Отсюда следует, что Ψ является аффинным отображением, т. е.

$$\Psi\left(\sum_{i=1}^n p_i S_i\right) = \sum_{i=1}^n p_i \Psi\left(S_i\right)$$

если $p_i \geqslant 0, \sum_{i=1}^n p_i = 1$. Преобразование Ψ назовем симметрией в пространстве состояний.

Т е орем а (Вигнер, 1931). Всякая симметрия пространства квантовых состояний имеет вид

$$\Psi(S) = USU^*$$

где U унитарный или антиунитарный оператор в $\mathscr{G}$.

Для средних значений наблюдаемых имеем

$$\operatorname{Tr} \Psi(S)X = \operatorname{Tr} S\Psi^*(X)$$

где

$$\Psi^*(X) = U^*XU$$

С точки зрения наблюдаемой статистики преобразование (2.1) состояний эквивалентно преобразованию (2.2) наблюдаемых. В первом случае говорят о картине Шрёдингера, а во второмо картине Гейзенберга.

Пусть G - группа и $g \to \Psi_g$ - представление G в группу симметрий $\odot(\mathscr{H})$, так что

$$\Psi_{g_1 \cdot g_2} = \Psi_{g_1} \cdot \Psi_{g_2}; g_1, g_2 \in G$$

Если G-связная топологическая группа, а представление $g \to \Psi_g$ непрерывно, то Ψ_g представляется в виде

$$\overset{\Psi}{g}_g(S) = U_g S U_g{}^*$$

где $g \to U_g$ - проективное унит арное представление группы G в пространстве $\mathscr{C}$, т. е. операторы U_g унитарны и удовлетворяют уравнению

$$U_{g_1} U_{g_2} = \omega\left(g_1, g_2\right) U_{g_1 \cdot g_2}$$

где $\omega\left(g_1, g_2\right)$ - множитель представления - комплексная функция, удовлетворяющая определенным алгебраическим соотношениям (см., например, Варадарайан [160]).

2.2. Однопараметрические группы. В случае $G = \mathbf{R}$, как показали Вигнер и Баргманн, всегда можно выбрать $\omega\left(g_1, g_2\right) = 1$, так что однопараметрическая группа симметрий определяется унитарным представлением R в $\mathscr{C}$.

Т е о р е м а (Стоун, 1932). Пусть $t \to U_t, t \in \mathbf{R}$ - сильно непрерывная группа унитарных операторов в $\mathscr{H}$, так что

$$U_{t_1} U_{t_2} = U_{t_1+t_2}; t_1, t_2 \in \mathbf{R}.$$

Тогда существует самосопряженный оператор A в $\mathscr{H}$, такой что $U_t = e^{itA}$. Обратно, для любого самосопряженного оператора A семейство $e^{itA}, t \in \mathbf{R}$, образует сильно непрерывную однопараметрическую группу.

Итак, предположив, например, что статистическое описание изолированной квантовой системы инвариантно относительно выбора начала отсчета времени, мы приходим к выводу, что в $\mathscr{H}$ существует самосопряженный оператор H такой, что состояние системы в момент времени t описывается формулой

$$S_t = e^{-iHt} S_0 e^{iHt}$$

Оператор H называется гамильтонианом (или наблюдаемой энергии) системы. Из (2.4) следует уравнение эволюции (в картине Шрёдингера)

$$i\frac{dS_t}{dt} = [H, S_t]$$

Если $S_0 = |\psi_0\rangle \langle\psi_0|$ - чистое состояние, то $S_t = |\psi_t\rangle \langle\psi_t|$, где $\{\psi_t\}$ - семейство векторов в $\mathscr{H}$, удовлетворяющее уравнению шрёдингера

$$i\frac{d\psi_t}{dt} = H\psi_t$$

Как правило, H - неограниченный оператор (полуограниченный снизу), так что в соотношениях (2.5), (2.6) следует позаботиться об областях определения.

Уравнение эволюции в картине Гейзенберга имеет вид

$$X_t = e^{iHt} \check{\Lambda}_0 e^{-iHt}; i\frac{dX_t}{dt} = [X_t, H]$$

Аналогично, из предположения о пространственной однородности вытекает существование самосопряженного оператора P, такого что состояние квантовой системы в системе отсчета, сдвинутой на расстояние x вдоль данной координатной оси, определяется уравнением

$$S_x = e^{-iPx} S_0 e^{iPx}$$

Оператор P называется оператором импульса вдоль этой оси. Вообще, всякой однопараметрической группе симметрий геометрического или кинематического характера отвечает самосопряженный оператор, порождающий по формулам типа (2.4), (2.7) преобразования квантовых состояний.

2.3. Соотношения Г. Вейля. инематика нерелятивистских систем как классических, так и квантовых, основана на прин. ципе относительности Галилея, согласно которому описание изолированной системы одинаково во всех инерциальных системах отсчета. Пусть $W_{\alpha,\nu}$ - унитарный оператор, порождающий преобразование состояний при переходе в систему отсчета, сдвинутую на расстояние x и движушуюся относительно исходной со скоростью v вдоль выделенной координатной оси. Тогда $(x, v) \to W_x, v$ есть проективное представление группы $G = \mathbf{R}^2$ в гильбертовом пространстве $\mathscr{H}$. Можно доказать, что соотношение (2.3) приводится к виду

$$W_{x_1,v_1} W_{x_2,v_2} = \exp\left[-\frac{im}{2}(x_1 v_2 - x_2 v_1)\right] W_{x_1+x_2, v_1+v_2}$$

где m - вещественный параметр (связанный с массой частицы) и далее строго положительный. Выделяя однопараметрические подгруппы - группу пространственных сдвигов $V_x = W_{x,0}$ и группу «галилеевых бустов» $U_v = W_{0,v}$, соотношение (2.8) можно переписать в виде

$$U_v V_x = e^{imxv} V_x U_v; \quad x, v \in \mathbf{R},$$

причем $W_{x,v} = e^{imxv/2} V_x U_v$. Соотношение (2.9) называется жанониеским коммутационным соотношением (ККС) Г. Вейла [10].

Согласно теореме Стоуна,

$$U_v = e^{imvQ}, \quad V_x = e^{-ixP},$$

где Q, P - самосопряженные операторы в $\mathscr{H}$. Рассматривая Q как вещественную наблюдаемую, заметим, что соотношение

$$V_x^* E(B + x) V_x = E(B); B \in \mathscr{B}(\mathbf{R})$$

для спектральной меры $\mathbf{E}$ оператора Q. Это же равносильно тому, что распределение вероятностей наблюдаемой преобразуется ковариантно при пространственных сдвигах (2.7):

$$\mu^Q_{s_x}(B + x) = \mu^Q_{S_0}(B); \quad B \in \mathscr{B}(\mathbf{R})$$

для любого состояния S_0. Это дает основание назвать Q наблюдаемой координаты вдоль выделенной оси. Симметричное рассуждение показывает, что P/m есть наблюдаемая скорости изолированной квантовой системы.

Представлением ККС считается любая конкретная пара (V, U), удовлетворяющая соотношениям (2.9). Представление называется неприводимым, если в $\mathscr{C}$ нет замкнутого подпространства, инвариантного относительно V_x, U_v. Неприводимым является представление Шрёдингера в $\mathscr{C} = L^2(\mathrm{R})$

$$V_x \psi(\xi) = \psi(\xi - x), U_v \psi(\xi) = e^{imv\xi} \psi(\xi)$$

В этом представлении Q задается оператором умножения на ξ, а P - оператором $i^{-1} \frac{d}{d\zeta^\circ}$.

Операторы P, Q имеют общую плотную инвариантную область определения и удовлетворяют на ней KKC Гейзенберга [1)]:

$$[P, Q] = i\mathrm{I}$$

Операторы P, Q называются каноническими наблюдаемыми. Обратный переход от соотношения Гейзенберга к соотношению Вейля (экспоненциирование) имеет ряд аналитических тонкостей, связанных с неограниченностью операторов P, Q и породил обширную математическую литературу (см. Иоргенсен, Мур [112]).

Принципиальное значение для квантовой механики имеет тот факт, что ККС определяют канонические наблюдаемые P, Q практически однозначно.

Теорем а (Стоун-фон Нейман, 1931). Всякое сильно непрерывное представление ККС− водимых представлений, каждое из которых унитарно эквивалентно представлению Шрёдингера.

В частности, в любом представлении ККСP, Q, как и в представлении Шрёдингера, неограничены и имеют лебегов спектр, простирающийся на всю вещественную прямую. С этим связана известная трудность с установлением разумного принципа соответствия в квантовой механике. Вопрос состоит в определении канонически сопряженных квантовых наблюдаемых, аналогичным обобщенным координатам и импульсам в

1. Соотношение (2.111) впервые было рассмотрено в 50-х годах прошлого века ирландским математиком Грейвсом, который развил соответствующее символическое исчисление. гамильтоновом формализме квантовой механики, и связан с: проблемой квантования классических систем. Так, в классической механике время и энергия, подобно координате и импульсу, являются канонически сопряженными величинами. Однако наблюдаемая энергии H имеет ограниченный снизу спектр, поэтому из теоремы Стоуна-фон Неймана вытекает, что не существует самосопряженного оператора времени T, которым был бы связан с H каноническим коммутационным соотношением. Эти трудности, возникающие и для других канонических пар, разрешаются в рамках обобщенной статистической модели квантовой механики (см. гл. 2, §3).

Аналогично формулируются ККС для систем с пронзвольным числом степеней свободы. Пусть $\{Z, \Delta\}$-симплектическое пространство, т. е. вещественное линейное пространство с билинейной кососимметричной формой $\Delta(z, z'); z, z' \in Z$. Представлением ККС называется семейство $z \to W(z)$ унитарных операторов в гильбертовом пространстве $\mathscr{H}$, удовлетворяющее KKC ВейляСигала

$$W(z)W(z') = \exp \frac{i}{2}\Delta(z, z')\, W(z + z')$$

Если форма Δ невырождена, а Z конечномерно, то оно имеет четную размерность d, и существует базис, в котором

$$\Delta(z, z') = \sum_{j=1}^{d} \left(x_j y'_j - x'_j y_j\right)$$

При этом операторы сильно непрерывного представления Вейля записываются в виде

$$W(z) = \exp i \sum_{j=1}^{d} (x_j P_j + y_j Q_j)$$

где самосопряженные операторы P_j, Q_j удовлетворяют многмерному аналогу ККС Гейзенберга (2.11)

$$[P_j, Q_k] = i\delta_{jk}\mathrm{I}; [P_j, P_k] = 0, [Q_j, Q_k] = 0$$

В этом случае теорема единственности Стоуна-фон Неймана сохраняет силу.

Для систем с бесконечным числом степеней свободы единственность нарушается и сушествует континуальное множество неэквивалентных представлений, что является причиной «инфракрасных расходимостей» в квантовой теории поля (см. [7], [32], [51]).

Неединственность представлений ККС тесно связана с неэквивалентностью вероятностных мер в бесконечномерных пространствах и послужила одним из первоначальных стимулов для изучения этого вопроса, занимающего большое место в классической теории случайных процессов.

2.4. Гауссовские состояния. Неравенство (1.9) и ККС (2.11) влекут соотношение неопределенностей Гейзенберга

$$\mathbf{D}_s(P)\mathbf{D}_{\boldsymbol{s}}(Q) \geqslant 1/4$$

из которого видно, что не существует состояния S, в котором P и Q одновременно принимали бы некоторые точные значения c вероятностью 1. Состояния, для которых

в (2.14) достигается равенство, называются состояниями минимальной неопределенности. Это чистые состояния $S_{x,v}$, определяемые векторами

$$\psi_{x,v} = W_{x,v}\psi_{0,0}; (x,v) \in \mathbf{R}^2$$

где $\psi_{0,0}$ - вектор основного состояния, в представлении Шрёдингера имеющий вид

$$\psi_{0,0}(\xi) = \left(2\pi\sigma^2\right)^{-1/4} \exp\left(-\xi^2/4\sigma^2\right)$$

Состояния $S_{x,v}$ характеризуются тремя параметрами

$$x = \mathbf{E}_{s_{x,v}}(Q), \quad v = \mathbf{E}_{s_{x,v}}(P),$$
$$\sigma^2 = \mathbf{D}_{s_{x,v}}(Q) = \left[4\mathbf{D}_{s_{x,v}}(P)\right]^{-1}.$$

При фиксированном σ^2 векторы $\psi_{x,v}$ образуют семейство, известное в квантовой оптике как семейство когерентных состояний [12], [21]. Для этих состояний

$$\left\langle Q - \mathbf{E}_{s_{x,v}}(Q)\cdot \mathrm{I}, \quad P - \mathrm{E}_{s_{x,v}}(P)\cdot \mathrm{I}\right\rangle_{s_{x,v}} = 0.$$

Более широкий класс образуют чистые состояния, для оторых достигается равенство в соотношении неопределенностей (1.9) (для P и Q), но условие (2.16) не обязано выполняться. Эти состояния широко обсуждались в физической литературе под именем сжатых (squeezed) состояний (см., например, [140]). С математической точки зрения все эти состояния входят в класс состояний, являющихся естественным квантовым аналогом гауссовских распределений в теории вероятностей.

Пусть $\{Z, \Delta\}$ - конечномерное симплектическое пространство с невырожденной кососимметричной формой Δ и $z \to W(z)$ - неприводимое представление ККС в гильбертовом пространстве $\mathscr{H}$. Характеристическая функция оператора плотности S в $\mathscr{H}$ определяется соотношением

$$\varphi(z) = \operatorname{Tr} SW(z); \quad z \in Z$$

и обладает рядом свойств, аналогичных свойствам характеристических функций в теории вероятностей [43, гл. V]. В частности, аналог условия положительной определенности имеет вид

$$\sum_{j,k} \bar{c}_j c_k \varphi\left(z_j - z_k\right) \exp\frac{i}{2}\Delta\left(z_j, z_k\right) \geqslant 0$$

для всех конечных наборов $\{c_j\} \subset \mathbf{C}, \{z_j\} \subset Z$. Состояние S называется гауссовским, если его характеристическая функция име32 ет вид

$$\varphi(z) = \exp\left[im(z) - \frac{1}{2}\alpha(z,z)\right]$$

где $m(z)$ - линейная, а $\alpha\left(z, z'\right)$ - билинейная формы на Z. Эго соотношение задает характеристическую функцию тогда и только тогда, когда выполнено условие

$$\alpha(z,z)\alpha\left(z',z'\right) \geqslant \frac{1}{4}\Delta\left(z,z'\right)^2; \quad z, z' \in Z$$

непосредственно связанное с (2.18). Общее определение для бесконечномерного Z было дано в [127]. В квантовой теории поля такие состояния описывают квазнсвободные (обобщенносвободные) поля и носят такое же название. В статистической механике они возникают как равновесные состояния бозе-систем с квадратичным гамильтонианом (см., например, [70], [51]).

12.1.3 3. Composite Systems

3.1. Тензорное произведение гильбертовых пространств.

Пусть $\mathscr{C}_1, \mathscr{H}_2$ - гильбертовые пространства со скалярными пронзведениями $\langle\cdot|\cdot\rangle_1$ и $\langle\cdot|\cdot\rangle_2$. В множестве $\mathscr{L}$ формальных линейных комбинаций элементов $\psi_1 \times \psi_2 \epsilon_2 \mathscr{C}_1 \times \mathscr{H}_2$ введем положительно определенную эрмитову форму, полагая

$$\langle\varphi_1 \backslash \langle\varphi_2|\psi_1 \backslash \psi_2\rangle = \langle\varphi_1|\psi_1\rangle_1 \langle\varphi_2|\psi_2\rangle_2$$

и продолжая ее на $\mathscr{L}$ по линейности. Пополнение (факторизованного по нулевому подпространству формы) пространства $\mathscr{L}$ является гильбертовым пространством, которое называется тензорным произведением $\mathscr{H}_1, \mathscr{C}_2$ и обозначается $\mathscr{H}_1 \otimes \mathscr{H}_2$. Вектор пространства $\mathscr{C}_1 \otimes \mathscr{H}_2$, соответствующий классу эквивалентности векторов $\psi_1 \backslash \psi_2 \in \mathscr{L}$, обозначается $\psi_1 \otimes \psi_2$.

Если $\mathscr{H}_j = L^2(\Omega_j, \mu_j); j = 1, 2$, то пространство $\mathscr{H}_1 \otimes \mathscr{H}_2 = L^2(\Omega_1 \times \Omega_2, \mu_1 \times \mu_2)$ состоит из всех функций $\psi(\omega_1, \omega_2)$, квадратично интегрируемых по мере $\mu_1 \times \mu_2$, причем вектор $\psi_1 \otimes \psi_2$ определяется функцией $\psi_1(\omega_1)\psi_2(\omega_2)$.

Тензорное произведение операторов $X_1 \otimes X_2$, где X_j - оператор в $\mathscr{H}_j$, определяется формулой

$$(X_1 \otimes X_2)(\psi_1 \otimes \psi_2) = X_1\psi_1 \otimes X_2\psi_2$$

Если $\mathscr{C}_j$ - конечномерные (комплексные) гильбертовы пространства, то

$$\dim \circlearrowleft (\mathscr{H}_1 \otimes \mathscr{H}_2) = \dim \curvearrowleft (\mathscr{H}_1) \dim \circlearrowleft (\mathscr{H}_2).$$

Если же $\mathscr{C}_j$ - вещественные гильбертовы пространства, то здесь имеет место знак $>$, а для кватернионных гильбертовых пространств (при некотором разумном определении $\mathscr{H}_1 \otimes \mathscr{H}_2$), знак $<$. Это обстоятельство рассматривается как косвенный аргумент в пользу поля комплексных чисел в аксиоматической квантовой механике.

Аналогично определяется тензорное произведение любого конечного числа гильбертовых пространств $\mathscr{C}_1 \otimes \ldots \otimes \mathscr{H}_n$. В квантовой механике $\mathscr{H}_1 \otimes \ldots \otimes \mathscr{H}_n$ описывает систему из n различимых частиц. В статистической механике приходится рассматривать системы неразличимых частиц - бозонов нли фермионов. В n-кратном тензорном пронзведении $\mathscr{H}^{\otimes n}$ выделяются два подпространства: симметричное тензорное произведение $\mathscr{H}^{sn}$, описывающее бозоны, и антисимметричное тензорное произведение $\mathscr{H}^{an}$, описывающее фермноны (в случае $\mathscr{H} = L^2(\Omega, \mu)$ первое состоит из симметричных, а второе - из антисимметричных функций $\psi(\omega_1, \ldots, \omega_n)$ аргументов $\omega_1, \ldots, \omega_n \in \Omega$). Системы из переменного (неограниченного) числа частиц описываются пространствами Фока: симметричным пространством $\Gamma_a(\mathscr{C}) = \sum_{n=0}^{\infty} \bigoplus \oplus \mathscr{H}^{\mathrm{sn}}$ в случае бозонов и антисимметричным пространством $\Gamma_a(\mathscr{G}) = \sum_{n=0} \oplus \mathscr{H}^{an}$ в случае фермнонов. В этих пространствах действует специальное представление канонических коммутационных (соответственно, антикоммутационных) соотношений, связанное с процедурой вторичного квантования (см. [6], [51], [70]).

3.2. Произведение квантовых состояний. Если S_j - операторы плотности в $\mathscr{C}_j$, то $S_1 \otimes S_2$ - оператор плотности в $\mathscr{C}_1 \otimes \mathscr{H}_2$, причем

$$\operatorname{Tr}(S_1 \otimes S_2)(X_1 \otimes X_2) = \operatorname{Tr} S_1X_1 \cdot \operatorname{Tr} S_2X_2; X_j \in \mathscr{P}(\mathscr{H}_j)$$

Операторы вида $X \otimes \mathrm{I}_2$, где $X \in \mathscr{P}(\mathscr{H}_1)$, а I_2 - единичный оператор в $\mathscr{C}_2$, образуют подалгебру $\mathfrak{P}_1 \subset \mathfrak{P}(\mathscr{C}_1 \otimes \mathscr{H}_2)$, нзоморфную $\mathfrak{B}(\mathscr{C}_1)$. Формула

$$\mathscr{E}\left(X_1 \otimes X_2\right) = X_1 \otimes \left(\operatorname{Tr} S_2 X X_2\right) I_2$$

определяет отображение $\mathscr{E}$ из $\mathscr{P}\left(\mathscr{C}_1 \otimes \mathscr{H}_2\right)$ на $\mathscr{P}\left(\mathscr{H}\mathscr{C}_1\right)$, обладающее свойством у словного о жид ан ия

$$\mathbf{E}_{\boldsymbol{s}}(XY) = \mathbf{E}_{\boldsymbol{B}}(\mathscr{E}(X)Y); X \in \mathscr{B}\left(\mathscr{H}_1 \otimes \mathscr{H}_2\right), Y \in \mathscr{B}_1,$$

относительно состояния $S = S_1 \otimes S_2$. В квантовой теории вероятностей условные ожидания играют меньшую роль, чем в классnческой, поскольку в общем случае условное ожидание на данную подалгебру $\mathscr{B}$ относительно данного состояния S существует лишь при весьма ограничительном соотношении между и S, в определенной мере, сводящем ситуацию к классической; точнее см. п. 3.1.3.

Если S - произвольный оператор плотности в $\mathscr{C}_1 \otimes \mathscr{H}_2$, то в $\mathscr{G}_1$ найдется единственный оператор плотности S_1, такой что

$$\operatorname{Tr} S_1 X = \operatorname{Tr} S\left(X \otimes \mathrm{I}_2\right); X \in \mathscr{B}\left(\mathscr{H}_1\right).$$

Это же верно для любой линейной комбинации операторов плотности, т. е. для любого ядерного оператора T в $\mathscr{H}_1 \otimes \mathscr{H}_2$. Отображение $T \to T_1$ называется частичным следом оператора T (обозначается $T_1 = \operatorname{Tr} \mathscr{H}_2 T$). Операция частичного следа аналогична нахождению маргинального распределения в теории вероятностей.

3.3. Независимасть и предельные теоремы. Рассмотрим сначала ситуацию, соответствующую одномерной центральной предельной теореме в теории вероятностей. Пусть S - фиксированное состояние. Вещественные наблюдаемые $X_1, \ldots, X_n, \ldots$ называются независимыми, если

$$\begin{aligned}&\mathbf{E}_s\left(\varphi_1\left(X_{i_1}\right)^* \ldots \varphi_m\left(X_{j_m}\right)\right) = \\ =&\mathbf{E}_{\boldsymbol{s}}\left(\varphi_1\left(X_{j_1}\right)\right)^{\cdot} \ldots \mathbf{E}_{\boldsymbol{s}}\left(\varphi_m\left(X_{i_m}\right)\right)\end{aligned}$$

для любых $m = 1, 2, \ldots$, любых ограниченных борелевских функщий $\varphi_1, \ldots, \varphi_m$ и любых номеров $j_1, \ldots, j_m$, таких что $j_k \neq \dot{j}_l$ при $k \neq l$. Предполагается, что X_j одинаково распределены и имеют второй момент, причем $\mathbf{E}_s\left(X_j\right) = 0, \mathbf{D}_s\left(X_j\right) = 1$. Что можно сказать о предельном распределении нормированных сумм

$$S_n = \frac{1}{\sqrt{n}} \sum_{j=1}^{n} x_j^{\times}$$

Если $X_1, \ldots, X_n, \ldots$-попарно перестановочны, то

$$\exp it\left(X_1 + \ldots + X_n\right) = \exp \text{ it } X_1 \ldots \exp itX_n; t \in \mathbb{R}$$

и применение характеристических функций сводит вопрос k классической центральной предельной теореме, со стандартным нормальным распределением в качестве предельного. В общем случае (3.3) не выполняется и предельное поведение сумм существенно зависит от алгебраических свойств последовательности слагаемых. Пусть, например, $X_1, \ldots, X_n, \ldots$ - а н т и п е р е с т ан о в о ны в том смысле, что

$$X_j X_k = -X_k X_j \text{ при } j \neq k.$$

Тогда прямой подсчет (в предположении конечности 4-го момента X_j) показывает, что

$$\mathbf{E}_{\mathcal{B}}\left(S_n^4\right) - \left(\mathbf{E}_{\mathbf{B}}\left(S_n^2\right)\right)^2 \to 0$$

откуда следует, что ${S_n}^2 \to 1$ по вероятности. Поскольку $\mathbf{E}_{\boldsymbol{s}}(S_n) = 0$, то распределение S_n стремится к симметричному распределению Бернулли, сосредоточенному в точках ± 1[11]. Это согласуется с наблюдением, что распределение Бернулли устойчиво относительно сложения антиперестановочных наблюдаемых (n. 1.6).

Богатство новых возможностей, открывающихся в некоммутативной теории, демонстрируют понятие свободной независимо-

1. Это рассуждение сообщено автору В. фон Вальденфельсом. .сти и соответствующая предельная теорема, открытые Войкулеску [162] (см. также Шпайхер [151]). Вещественные наблюдаемые $X_1, \ldots, X_n, \ldots$ называются свободно независимыми, если соотношения (3.2) выполняются для всех номеров $j_1, \ldots, j_m$, та. ких что $j_k \neq j_{k+1}, k = 1, \ldots, m-1$.

Те орема. Пусть X_j - свободно независимые наблюдаемые, $\|X_j\| \leqslant c; j = 1, \ldots, n, \ldots$ Пусть X_j одинаково распределены и $\mathbf{E}_{\boldsymbol{s}}(X_j) = 0, \mathbf{D}_{\boldsymbol{s}}(X_j) = 1/4$. Тогда распределение нормированных сумм S_n сходится при $n \to \infty$ к полукруговому закону Вигнера с. Плотностью

$$p(x) = \begin{cases} \frac{2}{\pi}\sqrt{1-x^2}, & |x| \leqslant 1 \\ 0, & |x| > 1 \end{cases}$$

Доказательство этой теоремы методом моментов требует довольно сложных комбинаторных подсчетов. Другой метод доказательства - использование преобразования Коши, которое играет роль логарифма характеристической функции для сво'бодно независимых' величин [163].

При переходе к многомерной предельной теореме возникает принципиально новая ситуация, обусловленная возможностью различных алгебраических соотношений между компонентами каждого из слагаемых. В работе Кашена, Хадсона [77] (соответственно, Хадсона [106]) предполагается, что компоненты слагаемых подчинены каноническим коммутационным (антикоммутационным) соотношениям и доказывается; что состояния, описы:вающие нормированную сумму, сходятся к квазисвободному состоянию канонических коммутационных (антикоммутационных) соотношений, т. е. к квантовому гауссовскому (бернуллиевскому) состоянию. При этом в случае антикоммутационных соотношений вместо обычного тензорного произведения алгебр, порожденных компонентами каждого слагаемого, необходимо использовать так называемое градуированное тензорное произведение, обобщающее понятие антиперестановочности. Более интересны результаты работ Гири, фон Вальденфельса [90] и Вальденфельса [164], в которых показано, что квазисвободное состояние на алгебре канонических коммутационных (соответственно, антикоммутационных) соотношений возникает в квантовой центральной предельной теореме без априорных предположений об алгебраической природе слагаемых, а лишь в зависимости от выбора обычного (или градуированного) тензорного произведения. Однако метод доказательства в этих работах, основанный на вычислении моментов, предполагает ограничительное в аналитическом плане условие существование моментов всех порядков.

В ряде работ рассматривался случай слабо зависимых наблюдаемых. М. Ш. Гольдштейн доказал сходимость к нормальному распределению в случае последовательности вещественных наблюдаемых $X_1, \ldots, X_n, \ldots$, удовлетворяющей условиям сла- бой зависимости и асимптотической перестановочности типа условия Розенблатта (см. обзор В. В. Аншелевича и М. Ш. Гольдштейна в сборнике [34] и книгу Т. А. Сарымсакова [31]). Обобщение результатов фон Вальденфельса об асимптотической квазисвободности на случай слабо зависимых слагаемых даны в работе

Аккарди и Баха [53] (алгебру $\mathscr{B}$ в этой работе следует считать коммутативной). Наиболее полный результат для слабо зависимых (перестановочных) слагаемых получен Годерисом, Вербером, Ветсом [92]. Следует отметить, что истоком работ [90], [92] послужили известные работы Хеппа и Либа о флуктуациях в мазере Дикке, которые дают некоторую физическую мотивацию квантовой центральной предельной теоремы для перестановочных слагаемых.

Различные алгебраические обобщения центральной предельной теоремы (связанные, в частности, с понятием безграничной, делимости) рассматривались также Хегерфельдтом [97], Партасарати и Шмидтом [138], Фаннесом и Куагебером (статья в сборнике [142]).

12.1.4 4. The Problem of Hidden Parameters

Проблема скрытых параметров - это вопрос о принципиальной возможности описания квантовой механики в терминах классического фазового пространства. Несмотря на устоявшееся среди физнков мнение о невозможности такого описания, конструирование теорий со скрытыми параметрами не прекращается (одной из недавних и наиболее интересных попыток является стохастическая механика [132]). Этой проблеме посвящена обширная литература (см., например, [14]). Здесь мы ограничимся обсуждением наиболее существенных логических аргументов против «скрытых параметров».

4.1. Скрытые параметры и квантовая дополнительность. С математической точки зрения в проблеме скрытых параметров речь ндет о возможности установления соответствий $S(d\omega) \to \hat{S}, X(\omega) \to \hat{X}$ между классическими состояниями, т. е. распределениями вероятностей $S(d\omega)$ на измеримом «фазовом пространстве» $(\Omega, \mathscr{B}(\Omega))$ и операторами плотности $\hat{S}$ в гильбертовом пространстве $\mathscr{H}$ квантовой системы, и между случайными величинами $X(\omega)$ и наблюдаемыми $\hat{X}$ в $\mathscr{H}$, которые воспроизводили бы статистические предсказания квантовой теории и удо-: влетворяли некоторым физически мотивированным. условиям. Такими условиями, естественно возникающими из общего понятия статистической модели (п. 0.2), в первую очередь являются сохранение функциональной подчиненности в пространстве наблюдаемых, а также выпуклой структуры в множестве состояний. Обзор с этой точки зрения основных «доказательств невозможности» скрытых параметров дан в [45]. Так, результаты

Белла [66] и Кошена, Шпеккера [115] равносильны следующему утверждению.

Пр едложение. Пусть $\dim \mathscr{H} \geqslant 3$. Не существует однозначного отображения $X \to X(\omega)$ множества наблюдаемы X $\mathcal{D}(\mathscr{H})$ в множество случайных величин на каком-либо измеримом пространстве Ω, удовлетворяющего условню:

1. если $X \to X(\omega)$, то $f \circ X \to f(X(\omega))$ для любой борелевской функции f.

Дока зательство. Можно считать, что $\dim \mathscr{H} < \infty$. Пусть такое отображение существует, тогда из 1) выводятся следующие свойства

2. $X(\omega) \in \operatorname{Sp} X$ для любого $\omega \in \Omega$;

3. Если $\hat{X}_j$ - совместимые наблюдаемые и $\hat{X}_j \to X_j(\omega)$, то $\sum\limits_j \hat{X}_j \to \sum\limits_j X_j(\omega)$.

Фиксируем $\omega \in \Omega$ и рассмотрим функцию проекторов $\mu(E) = E(\omega)$, где $E \to E(\omega)$. Из 2), 3) вытекает, что μ является вероятностной мерой на $\mathbb{E}(\mathscr{H})$, принимающей только значения 0,1. По теореме Глисона $\mu(E) = \operatorname{Tr} \hat{S}E$, где $\hat{S}$ - оператор плотности, но такая функция не может быть двузначной мерой.

Недостаток аргументации фон Неймана [26] состоит в том, что он требовал выполнения свойства 3) для п роизвольны **x**, а не только совместимых наблюдаемых $\boldsymbol{X}_j$. Рассуждение

с аддитивностью средних значений, которое он привел для обоснования этого требования, по существу, заранее исключает теории со скрытыми параметрами [45], [14].

Приведенное выше доказательство означает невозможность введения скрытых параметров по схеме частичной наблюдаемости, реализуемой, например, в классической статистической механике, где имеется взаимно однозначное соответствие между «макроскопическими» наблюдаемыми и некоторыми функциями на фазовом пространстве. Однако оно не исключает более сложных конструкций, в которых одна и та же квантовая наблюдаемая $\boldsymbol{X}$ может быть измерена множеством разных способов и соответствие $X(\omega) \to X$, таким образом, не взаимно однозначно. На самом деле в квантовой механике имеется по крайней мере столько различных способов измерения наблюдаемой $\bar{X}$, сколько есть представлений $\bar{X} = f \circ \bar{Y}$ в виде функций от других наблюдаемых $\vec{P}$. Если $\mathbb{X}$ имеет кратное собственное значение, то заведомо найдутся несовместимые наблюдаемые $\vec{P}_1$ и $\vec{P}_2$ такие, что $\mathbb{X} = f_1 \circ \widehat{P}_1 = f_2 \circ \hat{Y}_2$. Требование взаимной однозначности входит тогда в прямое противоречие с квантовым свойством дополнительности [1)]. Отсюда вытекает, что в теориях

1). Если $\dim \mathscr{H} = 2$, то наблюдаемые с кратным спектром - это постоянные величины; тогда такого противоречия не возникает, и теория со скрытыми параметрами, удовлетворяющая условиям доказанного предложенння, строится явным образом [66]. со скрытыми параметрами следует оставить возможность для различных классических представлений одной и той же квантовой наблюдаемой (такого рода теории Дж. Белл назвал ко н текстуальным и). Аналогичное замечание можно отнести и представление квантовых состояний. А. С. Холево дал явное описание такой формальной конструкции, сохраняющей структуры статистической модели [45], [101].

Предложение. Пусть $\mathscr{H}$ - гильбертово пространство. Существует измеримое пространство Ω и отображения $X(\omega) \to \dot{X}$ некоторого множества случайных величин на $\mathfrak{O}(\mathscr{C})$ и $S(d\omega) \to S$ некоторого множества вероятностных мер на $\mathfrak{S}(\mathscr{C})$ такие, что

1. Если $S_j(d\omega) \to \hat{S}_j$ и $\{p_j\}$-конечное распределение вероят. ностей, то $\sum\limits_j p_j S_j(d\omega) \to \sum\limits_j p_j \hat{S}_j$;
2. Если $\dot{X}(\omega) \to \hat{\lambda}^*$ и f-борелевская функция, то $f(X(\omega)) \to \to f \circ \hat{X}$
3. Если $\ddot{\dot{X}}(\omega) \to \hat{\lambda}$ и $S(d\omega) \to \hat{S}$, то

$$\int\limits_{\Omega} X(\omega) S(d\omega) = \operatorname{Tr} \hat{S}\hat{X}$$

В случае $\dim \mathscr{H} \geqslant 3$ отображения $X(\omega) \to X, S(d\omega) \to \hat{S}$ с необходимостью не являются взаимно однозначными. Этот результат показывает, что принцип дополнительности препятствует классическому описанию квантовой статистики лишь при дополнительном требовании взаимной однозначности (неконтекстуальности).

4.2. Скрытые параметры и квантовая целостность. Рассмотрим квантовую систему, состоящую из двух компонент $\mathscr{H}_1, \mathscr{H}_2$. Чистые состояния такой системы задаются единичными векторами $\psi \in \mathscr{C}_1 \otimes \mathscr{H}_2$, которые являются линейными комбинациями (суперпозициями) факторизуемых векторов $\psi_1 \otimes \psi_2$. Если $\psi = \psi_1 \otimes \psi_2$, то обе компоненты системы находятся в однозначно определенных чистых состояниях; если же ψ нефакторизуемо, то между компонентами обнаруживаются специфические корреляции, которые невозможно смоделировать никаким класснческим механизмом случайности. На это обратил внимание Белл, показавший, что даже в контекстуальной

теории со скрытыми параметрами нельзя удовлетворить естественному требованию, названному им «эйнштейновской локальностью» [66][11]. Обсудим близкое, но более общее условие р азделимости [45].

1. В этой связи см. также статью Э. Вигнера «Скрытые параметры и квантовомеханические вероятности» в сб. [11].

Рассмотрим наблюдаемые

$$\hat{X}_j = \hat{X}_j^{(1)} \otimes \hat{I}^{(2)}, j_k = 1 \ldots, n$$
$$\hat{Y}_k = \hat{I}^{(1)} \otimes \hat{Y}_j^{(2)}, k = 1, \ldots, m$$

где $\hat{\mathrm{I}}^{(j)}$-единичный оператор в $\mathscr{H}_j$, так что

$$\left[\hat{X}_j, \hat{Y}_k\right] = 0$$

т. е. каждая наблюдаемая $\hat{X}_j$ совместима с каждой $\hat{Y}_k$. Поэтому для любого состояния $\hat{S}$ в $\mathscr{C}_1 \otimes \mathscr{H}_2$ определены квантовые корреляции $\left\langle \hat{X}_j, \hat{Y}_k \right\rangle_{\hat{s}}$. Матрица $\mathbf{C} = \left[\left\langle \hat{X}_j, \hat{Y}_k \right\rangle_{\hat{s}}\right]_{j=1,\ldots,n,k=1,\ldots,m}$ описывает статистические результаты nm различных экспериментов, вообще говоря, несовместимых между собой.

П р едложе ние. Пусть $n, m \geqslant 2$. Не существует измеримого пространства Ω и отображений $S(d\omega) \to \hat{S}, X(\omega) \to \hat{X}$ таких, что:

1. если $X(\omega) \to \hat{X}$, то $X(\omega) \in \mathrm{Cp}\, \hat{X}$;
2. для любого $\hat{S}$ и любых $\hat{X}_1, \ldots, \hat{X}_n; \hat{Y}_1, \ldots, \hat{Y}_m$ вида найдутся $X_j(\omega), Y_k(\omega)$ такие, что $X_j(\omega) \to \hat{X}_j, Y_k(\omega) \to \hat{Y}_k$ и $\left\langle \hat{X}_j, \hat{Y}_k \right\rangle_{\hat{s}} = \int\limits_{\Omega} X_j(\omega) Y_j(\omega) S(d\omega)$; $j = 1, \ldots, n$, $k = 1, \ldots, m$, для какого-либо $S(d\omega) \to \hat{S}$.

Доказательств о. Достаточно ограничиться случаем $n = m = 2$. Рассмотрим наблюдаемые $\hat{X}_1, \hat{X}_2, \hat{Y}_1, \hat{Y}_2$ вида (4.1) и такие, что

$$\left\|\hat{X}_j\right\| \leqslant 1, \left\|\hat{Y}_k\right\| \leqslant 1$$

Предположим, что указанные отображения существуют и пусть. X_j, Y_k - соответствующие случайные величины на вероятностном пространстве $(\Omega, \mathscr{B}(\Omega), \quad S(d\omega))$. В силу условия 1), $|X_i(\omega)| \leqslant 1, |Y_n(\omega)| \leqslant 1$, откуда

$$X_1(\omega)Y_1(\omega) + X_1(\omega)Y_2(\omega) + X_2(\omega)Y_1(\omega) - X_2(\omega)Y_2(\omega) \leqslant 2, \quad \omega \in \Omega$$

Усредняя по $S(d\omega)$ и используя условие 2), получаем неравенство Белла-Клаузера-Хорна-Шимони (БКХШ)

$$\left\langle \hat{\lambda}_1, \hat{Y}_1 \right\rangle_{\hat{s}} + \left\langle \hat{X}_1, \hat{Y}_2 \right\rangle_{\hat{s}} + \left\langle \hat{X}_2, \hat{Y}_1 \right\rangle_{\hat{s}} - \left\langle \hat{\Lambda}_2, \hat{Y}_2 \right\rangle_{\hat{s}} \leqslant 2.$$

Остается указать квантовле наблюдаемые $\hat{X}_j, \hat{Y}_k$ и состояние $\hat{S}$, для которых неравенство (4.4) нарушается. Рассмотрим систему из двух частиц со спином 1/2, так что $\dim \mathscr{H}_1 = \dim \mathscr{H}_2 = 2$. (см. п. 1.6). Пусть $\hat{S}$-чистое состояние состав- ной системы с вектором

$$\psi = \frac{1}{\sqrt{2}} [\psi_1(\mathrm{e}) \otimes \psi_2(-\mathrm{e}) - \psi_1(-\mathrm{e}) \otimes \psi_2(\mathrm{e})]$$

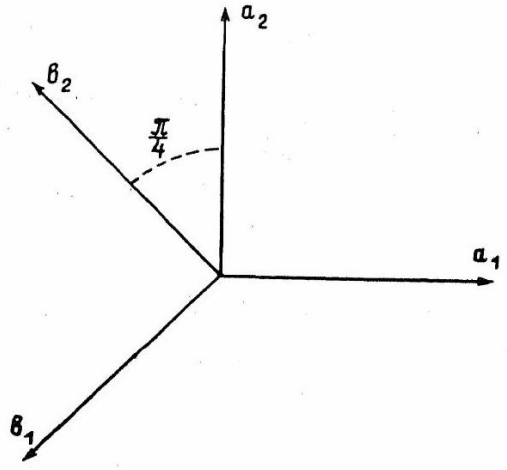
где $\psi_j(\mathrm{e})$-единичный вектор j-й компоненты, описывающй полностью поля ризованное состояние с направлением спина e. Положнм

$$\hat{\lambda}'(\mathrm{a}) = \hat{X}^{(1)}(\mathrm{a}) \otimes \hat{\mathrm{I}}^{(2)}, \quad \hat{Y}(\ \mathrm{b}) = \hat{\mathrm{I}}^{(1)} \otimes \hat{\lambda}^{*(2)}(\mathrm{b})$$

где $\hat{\mathbf{\Lambda}}^{(j)}(\mathrm{a})$ - наблюдаемые спина в $\mathscr{H}_j$ (см. П. 1.6). Корреляции между компонентами имеют вид

$$\langle \hat{X}(\mathbf{a}), \hat{Y}(\mathbf{b}) \rangle_{\hat{s}} = \left\langle \psi | \hat{\Lambda}^{(1)}(\mathbf{a}) \otimes \hat{X}^{(2)}(\mathbf{b}) \psi \right\rangle = -\mathbf{a} \cdot \mathbf{b}.$$

Пусть векторы $\mathbf{a}_j, \mathbf{b}_k$ образуют конфигурацию, обозначенную на рисунке, тогда значение левой части неравенства (4.4) для наблюдаемых $\hat{X}_j = \hat{X}\,(\mathrm{a}_j)\,, \hat{Y}_k = \hat{Y}\,(\ \mathrm{b}_k)$ равно $2\sqrt{2}$, что противоречит неравенству и доказывает предложение [1].



В [114] указано общее неравенство

$$\left(\hat{X}_1\hat{Y}_1 + \hat{X}_1\hat{Y}_2 + \hat{X}_2\hat{Y}_1 - \hat{A}_2\hat{Y}_2\right)^2 \leqslant 4\hat{I} - \left[\hat{X}_1, \hat{\lambda}_2\right] \cdot \left[\hat{Y}_1, \hat{Y}_2\right]$$

справедливое лля любэх операторов, удовлетворяющих условиям (4.2), (4.3). Из него вытекает как неравенство БКХШ (при $\left[\hat{X}_1, \hat{X}_2\right] = \left[\hat{Y}_1, \hat{Y}_2\right] = 0$), так и граница

$$\left\| \hat{X}_1\hat{Y}_1 + \hat{X}_1\hat{Y}_2 + \hat{X}_2\hat{Y}_1 - \hat{\hat{X}}_2\hat{Y}_2 \right\| \leqslant 2\sqrt{2}$$

из которой видно, что в построенном примере неравенство БКХШ нарушается максимальным образом.

1. Работы Дж. Белла стимулировали ряд экспериментов, в которых нарушение неравенства БКХШ получило подтверждение (см., например, [14]).

Поскольку компоненты составной системы могут представлять собой частицы, пространственно отделенные друг от друга макроскопическим расстоянием, то описывающая их теория со скрытыми параметрами должна быть существенно нелокальной [1)]. В работе Саммерса и Вернера [156] показано, что положение не спасает и переход к локальной квантовой теории поля, где неравенство БКХШ также нарушается максимальным образом.

4.3. Структура множества квантовых корреляций. В работе Б. С. Цирельсона [48] было изучено выпуклое множество $\mathrm{Cor}(n,m)$ квантовопредставимых матриц $\mathbf{C} = [c_{jk}]_{k=1,\ldots,n,m}^{j=1,\ldots,n}$, элементы которых представимы как корреляции $c_{jk} = \left\langle \hat{X}_j, \hat{Y}_k \right\rangle_{\hat{s}}$ каких-либо квантовых наблюдаемых $\mathcal{X}_j, P_k$, удовлетворяющих условиям (4.2), (4.3). Оказывается, что формально более сильное, чем (4.2). (и физически содержательное), условие (4.1) приводит к тому же множеству корреляционных матриц C. Это видно из доказательства следующей теоремы, которая дает прозрачное геометрическое описание множества $\mathrm{Cor}(n,m)$.

Т е о рема. Матрица C принадлежит множеству Cor (n,m) тогда и только тогда, когда в евклидовом пространстве размерности $\min(n,m)$ сушествуют векторы $\mathbf{a}_1,\ldots,\mathbf{a}_n;\mathbf{b}_1,\ldots,\mathbf{b}_m$ такие, что $\|\mathbf{a}_j\| \leqslant 1, \|\mathbf{b}_k\| \leqslant 1$ и $\mathbf{a}_j \cdot \mathbf{b}_k = c_{jk}$ для всех j,k.

Дадим набросок конструкции, существенной для доказательства. Пусть $\mathscr{C}(n)$ - комплексная алгебра Клиффорда с n эрмитовыми образующими $X_1,\ldots,X_n$, удовлетворяющими соотношениям

$$X_j^2 = 1, \quad X_jX_k + X_kX_j = 0; \quad j,k = 1,\ldots,n, \quad j \neq k$$

Поскольку элементы $X_j \otimes X_j$ алгебры $\mathscr{B}(n) \otimes \mathscr{B}(n)$ перестановочны и их спектр состоит из \pm 1, то 1 является точкой спектра элемента

$$A = \frac{1}{n}\left(X_1 \otimes X_1 + \ldots + X_n \otimes X_n\right)$$

(кратности 1). Пусть π - неприводимое представление алгебры $\mathscr{C}(n) \otimes \mathscr{C}(n)$, тогда в пространстве представления сушествует единственный с ' точностью до множителя вектор ψ, такой что $\pi(A)\psi = \psi$. Доказывается, что

$$\langle \psi | \pi(X(a) \otimes X(b))\psi \rangle = \mathbf{a} \cdot \mathbf{b}; \mathbf{a}, \mathbf{b} \in \mathbf{R}^n.$$

Вектор ψ определяет состояние $\hat{S}$ в точном представлении алгебры $\mathscr{B}(n) \otimes \mathscr{B}(n)$ такое, что

$$\left\langle \hat{\lambda}_j, \hat{Y}_k \right\rangle_{\hat{s}} = \mathbf{a}_j \cdot \mathbf{b}_k$$

1. По поводу нелокальности в стохастической, механике см. статью Э. Нельсона [132].
тде $\hat{X}_j = X\left(\mathbf{a}_j\right) \otimes \mathrm{I}, \hat{Y}_k = \mathrm{I} \otimes X\left(\mathbf{b}_k\right)$ удовлетворяіот условию (4.1) а значит, и (4.2).

Из этой теоремы в [48] получено описание крайних точек множества $\mathrm{Cor}(n,m)$, а также указаны неравенства, задающие множество Cor $(2,2)$.

Обозначая $\mathrm{Cor}_1(n,m)$ множество классически-представимых матриц C, таких что

$$c_{jk} = \int X_j(\omega)Y_k(\omega)S(d\omega),$$

где X_j, Y_k - случайные величины, такие что $|X_j(\omega)| \leqslant 1$, $|Y_k(\omega)| \leqslant 1$, имеем, очевидно,

$$\mathrm{Cor}_1(n,m) \subsetneq \mathrm{Cor}(n,m).$$

Несовпадение этих множеств математически выражает свойство квантовой целостности. Неравенство БХШ задает граничную гиперплоскость, отделяющую многогранник $\mathrm{Cor}_1(2,2)$ от квантово-реализуемой матрицы $\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \in \mathrm{Cor}(2,2)$. Естественно поставить вопрос, насколько Cor (n,m) превосходит $\mathrm{Cor}_1(n,m)$. Пусть $K(n,m)$ - наименьшее число, обладающее свойством

$$\mathrm{Cor}(n,m) \subset K(n,m)\,\mathrm{Cor}_1(n,m)$$

Последовательность $K(n,m)$ возрастает с ростом n,m. Как отмечается в [48], из геометрического описания множества Cor (n,m) вытекает, что $K = \lim K(n,m)$ совпадает с известной в теории нормированных пространств константой Гротендика $K_G \leqslant \frac{\pi}{2\ln\left(1+\sqrt{2}\right)} \approx 1,782$.

12.2 Statistics of Quantum Measurements

12.2.1 1. Generalized Observables

1.1. Разложения единицы.

Пусть $(\mathscr{L}, \mathscr{B}(\mathscr{X}))$ - измеримое пространство. В дальнейшем часто $\mathscr{L}$ с танд артно е измеримое пространство, т. е. борелевское подмножество полного сепарабельного метрического пространства. Стандартные измеримые пространства одинаковой мощности изоморфны (см., например, [160, гл. V]), поэгому с точки зрения теории меры они эквивалентны борелевским подмножествам вещественной прямой $\mathbf{R}$.

Разложением единицы в гильбертовом пространстве $\mathscr{H}$ называется нормированная положительная операторнозначная ме- ра на $\mathscr{B}(\mathscr{X})$, т. е. функция множеств $\mathbf{M} : \mathscr{B}(\mathscr{X}) \to \mathscr{B}(\mathscr{C})$, удовлетворяющая условиям:

1. $M(B)$ - положительный оператор в $\mathscr{H}$ для любого $B \in \mathscr{B}(\mathscr{H})$;
2. Если $\{B_j\}$ - конечное или счетное разбиение $\mathscr{Z}$ на попарно-непересекающиеся измеримые подмножества, то

$$\sum_j M\left(B_j\right) = \mathrm{I}$$

где ряд сходится сильно.

Если $M(B)^2 = M(B)$ для всех $B \in \mathscr{B}(\mathscr{D})$, то $\mathbf{M}$ - ортогональное разложение единицы (см. п. 1.1.3). Неортогональные разложения единицы (на R) появились в работе арлемана (1923), в связи с проблемой спектрального разложения несамосопряженных операторов и были детально изучены в 1940-60-е годы (см., например, [2], [30], [68]).

Т е о ре м а (М. А. Наймарк, 1940). Всякое разложение единицы в $\mathscr{C}$ может быть расширено до ортогонального разложения единицы, т. е. существует гильбертово пространство $\tilde{\mathscr{H}} \supset \mathscr{H}$ и ортогональное разложение единицы $\mathrm{E} : \mathscr{B}(\mathscr{X}) \to (E)(\widetilde{\mathscr{C}})$ в $\widetilde{\mathscr{H}}$ такое, что

$$M(B) = PE(B)P; \quad B \in \mathscr{B}(\mathscr{R})$$

где P-проектор из $\tilde{\mathscr{H}}$ на $\mathscr{H}$. Если $\mathscr{H}$ - сепарабельно, а $\mathscr{X}$ - стандартно, то $\tilde{\mathscr{H}}$ можно выбрать сепарабельным. Существует единственное с точностью до унитарной эквивалентности минимальное расширение, характеризующееся тем свойством, что множество $\{E(B)P\psi; B \in \mathscr{B}(\mathscr{X}), \psi \in \mathscr{C}\}$ плотно в $\widetilde{\mathscr{H}}$.

Если существует σ-конечная мера μ, такая что $\|M(B)\| \leqslant \leqslant C\mu(B)$, то

$$M(B) = \int\limits_B P(x)\mu(dx); \quad B \in \mathscr{B}(\mathscr{X})$$

где $P(x)$ - измеримая ограниченная функция со значениями в $\mathscr{P}(\mathscr{C})$, называемая плотностью $\mathbf{M}$ относительно меры μ (интеграл сходится в сильной операторной топологии). Если $\dim \mathscr{H} = \infty$, то ортогональное разложение единицы не может иметь. плотности относительно какой-либо б-конечной меры.

Пр им ер. Переполненной системой [21], [6] в $\mathscr{C}$ называется семейство $\{e_x; x \in \mathscr{Q}\} \subset \mathscr{H}$, удовлетворяющее условию

$$\|\psi\|^2 = \int\limits_{\mathscr{Q}} |\langle e_x|\psi\rangle|^2 \, \mu(dx); \quad \psi \in \mathscr{E}$$

где μ - некоторая σ-конечная мера на $\mathscr{B}(\mathscr{L})$, т. е.

$$\int\limits_{\mathscr{X}} |e_x\rangle \langle e_x| \, \mu(dx) = 1$$

Частным случаем переполненной системы является полная ортогональная система в $\mathscr{C}$, однако в обшем случае векторы $e_{\boldsymbol{x}}$ могут быть не ортогональны и линейно зависимы. Всякий вектор $\psi \in \mathscr{H}$ имеет разложение

$$\psi = \int\limits_{\mathscr{Q}} \langle e_x|\psi\rangle \, e_{x\mu}(dx)$$

по векторам переполненной системы. Соотношение

$$M(B) = \int\limits_{B} |e_x\rangle \langle e_x| \, \mu(dx)$$

.орределяет разложение единицы с плотностью $P(x) = |e_x\rangle \langle e_x|$. Дадим для него явную конструкцию минимального расширения Наймарка (см. [78, гл. 8]). Определим ортогональное разложение единицы $\mathbf{E}$ в $\tilde{\mathscr{H}} = L^2(\mathscr{X}, \mu)$ соотношением

$$E(B)f(x) = 1_B(x)f(x); x \in \mathscr{B},$$

где $1_B(\cdot)$ - индикатор множества $B \in \mathscr{B}(\mathscr{X})$. В (1.2), (1.3) следует, что соотношение

$$(V\psi)(x) = \langle e_x|\psi\rangle$$

задает изометрическое вложение $\mathscr{H}$ в $\mathscr{C}$, причем

$$M(B) = V^* E(B) V$$

Образ $V\mathscr{H}$ пространства $\mathscr{H}$ в $L^2(\mathscr{L}, \mu)$ является гильбертовым пространством с воспроизводящим ядром $\mathscr{K}(x, y) = \langle e_x|e_y\rangle$, т. е. проектор P из $L^2(\mathscr{Q}, \mu)$ на $V\mathscr{H}$ является интегральным оператором с ядром $\mathscr{K}(x, y)$.

1.2

Обобщенная статистическая модель квантовой механики. Это отделимая статистическая модель (см. п. 0.2), в которой состояния описываются операторами плотности, а вещественные наблюдаемые - разложениями единицы на $\mathscr{B}(\mathbf{R})$ в гильбертовом пространстве $\mathscr{C}$. Функциональная подчнненность наблюдаемых определяется соотношением $(f \circ M)(B) = M\,(f^{-1}(B))$. Если $\mathscr{X}$ - измеримое пространство, то обобщенной наблюдаемой (наблюдаемой) со значениями в $\mathscr{X}$ называется произвольное (ортогональное) разложение единицы $\boldsymbol{M}$ на $\mathscr{B}(\mathscr{X})$.

Распределение вероятностей обобщенной наблюдаемой $\mathbf{M}$ в состоянии S определяется формулой

$$\mu_S^M(B) = \operatorname{Tr} SM(B); \quad B \in \mathscr{B}(\mathscr{X}).$$

Основанием для этих определений служит

П редлож ен и е ([143, гл. 2]). Соответствие $S \to \mu_S^M$ является аффинным отображением выпуклого множества квантовых состояний $\subseteq (\mathscr{C})$ в множество вероятностных мер $\mathfrak{B}(\mathscr{L})$. Обратно, всякое аффинное отображение из $(\mathscr{H})$ в $\mathfrak{B}(\mathscr{X})$ имеет вид $S \to \mu_S^M$, где $\mathbf{M}$ - однозначно определенное разложение единицы на $\mathscr{B}(\mathscr{X})$.

Аффинность означает, что смесь состояний переходит в соответствующую смесь распределений

$$\mu^M_{\sum p_j s_j} = \sum_j p_j \mu^M_{s_j}$$

для любых $S_j \in \operatorname{Im}(\mathscr{H}); p_j \geqslant 0, \Sigma_j p_j = 1$, и имеет прямое истолкование в терминах статистических ансамблей. Можно сказать, что разложение единицы дает наиболее общее описание статистики исходов квантового измерения, совместимое с вероятностной интерпретацией квантовой механики.

Опираясь на теорему Наймарка, можно доказать, что для любого разложения единицы $\mathbf{M}$ в $\mathscr{C}$ найдутся гильбертово пространство $\mathscr{C}_0$, оператор плотности S_0 в $\mathscr{C}_0$ и ортогональное разложение единицы E в $\mathscr{H} \otimes \mathscr{H}$, такие что

$$\mu_S^M(B_3) = \operatorname{Tr}(S \otimes S_0) E(B); \quad B \in \mathscr{B}(\mathscr{Q})$$

для всех $S \in ((\mathscr{H})$ или $M(B) = \mathscr{E}_0(E(B))$, где $\mathscr{E}_0$ - условное ожндание относительно состояния S_0, определяемое аналогично формуле (1.3.1). Таким образом, разложение единицы описывает статистику измерения обычной наблюдаемой в некотором расширении исходной системы, содержащем вспомогательную независимую систему в состоянии S_0, что говорит о согласованности понятия обобщенной наблюдаемой со стандартной формулировкой квантовой механики.

Пр и м е р. Векторы состояний минимальной определенности (1.2.15) образуют переполненную систему в $\mathscr{H} = L^2(\mathbf{R})$,

$$\frac{m}{2\pi} \int\limits_{R^2} \int\limits_{x,v} |\psi_x\rangle \langle\psi_{x,v}| \, dxdv = \mathrm{I}$$

([12], [21]), что позволяет определить обобщенную наблюдаемую. со значениями в $\mathbf{R}^2$

$$M(B) = \frac{m}{2\pi} \iint_B |\psi_{x,v}\rangle \langle\psi_{x,v}| \, dxdv$$

Укажем конструкцию, которая связывает M с приближенным совместным измерением координаты и скорости квантовой частицы. Пусть $\mathscr{C}_0 = L^2(\mathbf{R}), P_0, Q_0$ - канонические наблюдаемые в $\mathscr{C}_0$ и $S_0 = |\psi_{0,0}\rangle \langle\psi_{0,0}|$ - основное состояние в $\mathscr{C}_0$. Самосопряженные операторы

$$\tilde{Q} = Q \otimes \mathrm{I}_0 - \mathrm{I} \otimes Q_0, \quad \frac{1}{m}\widetilde{P} = \frac{1}{m}\left[P \otimes \mathrm{I}_0 + \mathrm{I} \otimes P_0\right]$$

в $\mathscr{H} \otimes \mathscr{H}_0$ перестановочны [1)], а значит, имеют совместную спектральную меру $E(dxdv)$. Используя аппарат характеристических

1. На эо указал Н. Бор в статье «О понятиях причинности и дополнительности» (1948) (см. Избранные научные труды.- М.: Наука, 1971.- 2.С. 391 – 398). функций из п. 1.2.4, можно доказать, что для любого состояния: распределение вероятностей обобщенной наблюдаемой (1.6)

$$\mu_S^M(B) = \frac{m}{2\pi} \int\limits_B \int\limits_{x,v} \langle \psi_x \psi_{x,v} \rangle \, dxdv$$

удовлетворяет соотношению (1.5), т. е. совпадает с совместным распределением вероятностей наблюдаемых $\widetilde{Q}, \widetilde{P}/m$ в состоянии $S \otimes S_0$ (см. [43, гл. 3]). Относительно приближенных измерений Q, P см. также [78], [37], [159] и цитированные там работы.

1.3

Геометрия множества обобщенных наблюдаемых. Аналогом обобщенной наблюдаемой в классической статистике является рандомизованная случайная величина, т. е. переходная вероятность $\Pi(B|\omega)$ из пространства элементарных событий Ω в пространстве значений X. Будем далее предполагать, что $\mathscr{X}$ - стандартное пространство. Тогда соотношение

$$\Pi(B|\omega) = 1_B(f(\omega)); \quad \omega \in \Omega$$

устанавливает взаимно однозначное соответствне между случайными величинами f со значениями в $\mathscr{X}$ и де те р мини ров анными переходными вероятностями, такими что $\Pi(B|\omega) = 0$ или 1, т. е. $\Pi(B|\omega)^2 = \Pi(B|\omega)$. Переходные вероятности из Ω в $\mathscr{L}$ образуют выпуклое множество, крайними точками которого являются детерминированные переходные вероятности и только они (см., например, [41, гл. II]).

Соотношение между наблюдаемыми и обобщенными наблюдаемыми в квантовом случае значительно сложнее и интереснее. Обозначим $\mathfrak{M}(\mathscr{Q})$ выпуклое множество обобщенных наблюдаемых со значениями в $\mathscr{Q}$, $\operatorname{Extr}\mathfrak{M}(\mathscr{X})$ множество его крайних точек, $\operatorname{Conv}\mathfrak{M}$ выпуклую оболочку подмножества $\mathfrak{R} \subset \mathfrak{M}(\mathscr{Q})$. В $\mathfrak{M}(\mathscr{Q})$ вводится естественная топология: последовательность $\left\{\mathbf{M}^{(n)}\right\} \subset \mathfrak{M}(\mathscr{Z})$ сходится к $\boldsymbol{M}$, если для любого состояния S последовательность вероятностных мер $\mu_s^{(n)}(B) = \operatorname{Tr} SM^{(n)}(B)$ сходится по вариацин к $\mu_{\mathcal{S}}(B) = \operatorname{Tr} SM(B); \overline{\mathfrak{M}}$ означает замыкание подмножества $\mathfrak{M}$ в этой топологии. Пусть $\mathfrak{M}_0(\mathscr{Q})$ - подмножество обычных наблюдаемых и $\mathfrak{R}_1(\mathscr{Q})$ - подмножество обобщенных наблюдаемых $\mathbf{M}$, таких что $[M(B_1), M(B_2)] = 0$ для всех $B_1, B_2 \in \mathscr{B}(\mathscr{X})$. В работе А. С. Холево [38] показано, что $\boldsymbol{M} \in \mathbb{R}_1(\mathscr{X})$ тогда и только тогда, когда

$$M(B) = \int\limits_{\mathscr{X}_1} \Pi(B|x_1) \, E(dx_1)$$

где $\mathbf{E}$ - наблюдаемая со значениями в некотором пространстве $\mathscr{Q}_1, \Pi(B|x_1)$ - переходная вероятность из $\mathscr{X}_1$ в $\mathscr{X}$. По аналогии с классической статистикой, наблюдаемые, описываемые ортогональными разложениями единицы $\mathbf{E}\,(E(B)^2 = E(B))$, можно рассматривать как де терминированны е (более точное обсуждение см. в [101]). Наблюдаемые из $\mathfrak{R}_1(\mathscr{Q})$, кото- рые задаются перестановочными разложениями единицы, являются классически-рандомизованными в том смысле, что $M \in \mathbb{R}_1(\mathscr{Q})$ получается из обычной наблюдаемой путем преобразования (1.8), содержащего внешний классический источник неопределенности. Всякую обобщенную наблюдаемую $\boldsymbol{M} \in \mathfrak{M}(\mathscr{Z})$ можно рассматривать как квантово-рандомизованжую в смысле представления (1.5): она

эквивалентна обычной наблюдаемой в расширении исходной системы, включающем независимую квантовую систему. Наконец, точки из $\operatorname{Extr}\mathfrak{R}(\mathscr{Q})$ представляют собой обобщенные наблюдаемые, в которых неопределенность, обусловленная процедурой измерения, сведена к минимуму.

Обозначим m мощность множества значений $\mathscr{X}$.

Т е о рема. Если $m=2$, то $\mathfrak{R}_0(\mathscr{Q})=\operatorname{Extr}\mathfrak{M}(\mathscr{D})$ и $\mathfrak{M}_1(\mathscr{Q})=\overline{\operatorname{Conv}\mathfrak{R}_0(\mathscr{L})}=\mathfrak{R}(\mathscr{L})$. Если $m>2$, то $\mathfrak{R}_0(\mathscr{L})\subsetneq\operatorname{Extr}\quad\mathfrak{R}(\mathscr{X})$ и

$$\mathfrak{M}_1(\mathscr{B})\subsetneq\overline{\operatorname{Conv}\mathfrak{M}_0(\mathscr{B})}\subset\mathfrak{M}(\mathscr{B}),\quad\text{причем}\quad\text{если}\quad\dim\mathscr{H}<\infty,\quad\text{то}$$

последнее включение точн. Если же $\dim\mathscr{H}=\infty$, то $\overline{\mathfrak{M}_0(\mathscr{B})}=\mathfrak{M}(\mathscr{Q})$.

Таким образом, ситуация аналогична классической лишь в случае обобщенных наблюдаемых с двумя значениям [1)]. В этом случае $\boldsymbol{M}=\{M_0,M_1\}$, где $M_1=\mathrm{I}-M_0$ и $\mathfrak{R}(\mathscr{Q})$ как выпуклое подмножество изоморфно порядковому интервалу $\{M_0: M_0\mathfrak{L}_h(\mathscr{H}),\ 0\leqslant M_0\leqslant\mathrm{I}\}$, крайние точки которого совпадают с проекторами в $\mathscr{H}$ (см., например, [78, гл. 2]).

Чтобы доказать, что $\mathfrak{D}_0(\mathscr{P})\neq\operatorname{Extr}\mathfrak{M}(\mathscr{L})$ при $m>2$, достаточно сделать это в случае $m=3$ и $\dim\mathscr{H}=2$ (см. [43, §1.6]). Рассмотрим неортогональное разложение единицы

$$M_k=\frac{1}{3}\left|\psi\left(\mathrm{e}_k\right)\right\rangle\left\langle\psi\left(\mathrm{e}_k\right)\right|;k=1,2,3$$

где $\psi\left(\mathrm{e}_k\right)$ - векторы состояний системы со спином $1/2$ (см. п. 1.1.6), причем $\mathrm{e}_k, k=1,2,3$, образуют правильный треугольник. Тот факт, что (1.9) является крайней точкой, можно установить непосредственно, либо воспользовавшись критерием из статьи Штермера.в [85]: конечное разложение единицы $\mathbf{M}=\{M_1,\ldots,M_m\}$ является крайней точкой тогда и только тогда, когда для любых $X_1,\ldots,X_m\in\mathscr{B}(\mathscr{H})$ из $\sum\limits_{i=1}^{m}E_iX_iE_i=0$ следует $E_iX_iE_i=0$, где E_i - носитель M_i, т. е. проектор на ортогональное дополнение к нулевому подпространству M_i. Если $\dim\mathscr{H}<\infty$, то из наличия крайних точек, не попадающих в $\mathfrak{D}_0(\mathscr{Q})$, следует, что $\overline{\operatorname{Conv}\mathfrak{M}_0(\mathscr{X})}\neq\mathfrak{M}(\mathscr{X})$.

Интересный пример крайней точки дает неортогональное разложение единицы (1.6).

1. Такие наблюдаемые, называемые «эффектами», играют центральную роль в аксноматическом подходе Людвнга [125], [118].

Доказательство того, что $\overline{\mathfrak{R}_0(\mathscr{X})}=\mathfrak{M}(\mathscr{Q})$ в случае $\dim\mathscr{H}=\infty$, основывается на теореме M. А. Наймарка. Пусть $\mathrm{M}\in\mathrm{M}(\mathscr{R})$ и $\left\{P^{(n)}\right\}$ - последовательность конечномерных проекторов в $\mathscr{H}$, снльно сходящаяся к I. Тогда $M^{(n)}(B)=P^{(n)}M(B)P^{(n)}$ - разложение единицы в конечномерном пространстве $\mathscr{C}^{(n)}=P^{(n)}\mathscr{H}$, которое можно расширить до ортогонального разложения единицы $\mathbf{E}^{(n)}$ в сепарабельном гильбертовом пространстве $\tilde{\mathscr{G}}^{(n)}\supset\supset\mathscr{H}^{(n)}$. Поскольку $\dim\mathscr{H}=\infty$, можно считать, что $\tilde{\mathscr{H}}^{(n)}=\mathscr{H}$. Имеет место оценка

$$\operatorname{var}\left(\mu_B^{(n)}-\mu_B\right)\leqslant 6\left\|\left(I-P^{(n)}\right)S\right\|_1,$$

где $\mu_s^{(n)}(B)=\operatorname{Tr}SE^{(n)}(B)$, $\mu_s(B)=\operatorname{Tr}SM(B)$ [44], доказывающая утверждение. Итак, в случае $\dim\mathscr{H}=\infty$, все обобщенные наблюдаемые являются предельными точками множества наблюдаемых.

12.2.2 2. The Quantum Theory of Statistical Solutions

2.1. Проверка гипотез.

В гильбертовом пространстве $\mathscr{H}$ наблюдаемой квантовой системы заданы операторы плотности S_θ; $\theta=1,\ldots,m$, описывающие одно из возможных состояний снстемы. Выбор

одной из гипотез $\theta = 1, \ldots, m$ осуществляется на основе решающего правила, задаваемого разложением единицы $\mathbf{M} = \{M_1, \ldots, M_m\}$. При этом вероятность принятия гипотезы $u = 1, \ldots, m$, если система находится в состоянии S_θ, равна

$$\xi_{\theta\theta}^M(u) = \operatorname{Tr} S_A M_u.$$

Как и в классической статистике, задается некоторый функционал от вероятностей (2.1) и вопрос состоит в нахождении экстремума этого функционала в том или ином классе решающих правил. В физических задачах квантовая система является носителем информации, состояния которого S_θ зависят от «передаваемого сигнала» θ. «Приемник» осуществляет квантовое измерение, статистика которого описывается разложением единнцы M в $\mathscr{C}$. Речь идет об отыскании квантовых ограничений на качество измерения и о его оптимизации.

При байесовском подходе задаются априорные вероятности гипотез π_θ и функция отклонения $W_\theta(u); \theta, u = 1, \ldots, m$. Байесовский риск определяется обычной формулой

$$\mathscr{R}\{M\} = \sum_{\theta=1}^m \pi_\theta \sum_{u=1}^m W_\theta(u) \mu_\theta^M(u)$$

Решающее правило, минимизирующее $\mathscr{R}\{\mathbf{M}\}$, называется байесовским. Часто рассматривают случай $W_\theta(u) = 1 - \delta_{\theta u}$ и $\pi_\theta = 1/\mathrm{m}$. Тогда речь идет о максимизации средней вероятности правильного решения

$$\mathscr{P}\{\boldsymbol{M}\} = \frac{1}{m} \sum_{\theta=1}^m \mu_\theta^{\boldsymbol{M}}(\theta)$$

что является дискретным аналогом метода максимального правдоподобия. Наконец, важной мерой качества решающего правила является шенноновская информация

$$\mathscr{I}\{M\} = \sum_{\theta=1}^m \pi_\theta \sum_{u=1}^m \mu_\theta^M(u) \ln \frac{\mu_\theta^M(u)}{\sum\limits_{\lambda=1}^m \pi_\lambda \mu_\lambda^M(u)}.$$

Первоначальная постановка квантовой задачи различения гипотез (Хелстром, 1967) основывалась на стандартном квантово-механическом формализме, в соответствии с которым решающие правила описывались ортогональными разложениями единицы. Формулировка квантовой теории статистических решений, основанная на обобщенных наблюдаемых, была предложена А. С. Холево (1972). Обозначим $\mathfrak{P}$ класс всех решающих правил $\boldsymbol{M} = \{M_1, \ldots, M_m\}, \mathfrak{D}_1$ - класс классически-рандомизированных правил (т. е. таких, что $M_j M_k = M_k M_j$) и $\mathfrak{D}_0$ - класс детерминированных решающих правил ($M_j M_k = \delta_{jk} M_j$).

П р и м е р ([38]). Рассмотрим задачу различения равновероятных гипотез

$$S_\theta = |\psi(\mathrm{e}_\theta)\rangle \langle \psi(\mathrm{e}_\theta)|; \quad \theta = 1, 2, 3$$

где $\psi(\mathrm{e}_\theta)$ - векторы состояний системы со спином $1/2$, возникающие в (1.9). Тогда

$$\max_{\mathbb{N}_0} \mathscr{P}\{\boldsymbol{M}\} = \max_{\mathfrak{N}_1} \mathscr{P}\{\boldsymbol{M}\} = \frac{1}{6}(2 + \sqrt{3}) < \frac{2}{3} = \max_{\mathscr{N}} \mathscr{P}\{\boldsymbol{M}\}$$

причем максимум достигается на решающем правиле (1.9). Более того,

$$\max_{\mathfrak{M}_0} \mathscr{F}\{\mathbf{M}\} = \max_{\mathfrak{M}_1} \mathscr{F}\{\mathbf{M}\} < \max_{\mathscr{N}} \mathscr{F}\{\mathbf{M}\}$$

Этот и другие подобные примеры (см. [80]) демонстрируют неожиданный с классической точки зрения факт: квантовая рандомизация может увеличивать информацию о состоянии системы. Хотя этот эффект проявляется только в конечномерных гильбертовых пространствах (см. предыдущий пункт), он ясно указывает на необходимость использования обобщенных наблюдаемых.

2.2. Байесовская задача. Байесовский риск (2.2) представляется в виде

$$\mathscr{R}\{\mathbf{M}\} = \operatorname{Tr} \sum_{u=1}^{m} \hat{W}_u M_u$$

где $\hat{W}_u = \sum\limits_{\theta=1}^{m} \pi_\theta W_\theta(u) S_\theta$-операторная апостериорная функция отклонения. Поскольку $\mathscr{R}\{\boldsymbol{M}\}$ - аффинный функционал на выпуклом множестве $\mathfrak{M}$, задача о его минимизации может быть рассмотрена с помощью методов линейного программирования.

Т е о рем а (А. С. Холево, Юн). Имеет место соотношение двойственности

$$\min_{\mathfrak{M}} \mathscr{R}\{M\} = \max \left\{ \operatorname{Tr} \Lambda : \Lambda \in \mathfrak{T}(\mathscr{C}), \Lambda \leqslant \hat{W}_u; u = 1, \ldots, m \right\}$$

Следующие утверждения эквивалентны:

0. $\mathbf{M}^0 = \{{M_u}^0\}$ - байесовское решающее правило;

1. существует $\Lambda^0 \in \mathfrak{E}(\mathscr{H})$, такой что

$$\Lambda^0 \leqslant \hat{W}_u; \quad \left(\hat{W}_u - \Lambda^0\right) M_u^0 = 0; \quad u = 1, \ldots, m$$

2. оператор $\Lambda^0 = \sum\limits_{u=1}^{m} \hat{W}_u {M_u}^0$ эрмитов и $\Lambda^0 \leqslant \hat{W}_u; u = 1, \ldots, m$.

Задача в правой части (2.5) имеет единственное решение, которым является оператор Λ^0, входящий в условия 1), 2).

Наиболее часто используется достаточность условня 1), которая доказывается элементарно: для любого $\mathbf{M} = \{M_u\}$

$$\mathscr{R}\{\mathbf{M}\} = \operatorname{Tr} \sum_{u=1}^{m} \hat{W}_u M_u \geqslant \operatorname{Tr} \Lambda \sum_{u=1}^{m} M_u^0 = \operatorname{Tr} \sum_{u=1}^{m} \hat{W}_u M_u^0 = \mathscr{R}\left\{\mathbf{M}^0\right\}$$

С помощью этого условия легко проверяется оптимальность решающего правила (1.9) в примере предыдущего пункта,

П риме р 1. Пусть операторы $\hat{W}_u - \hat{W}_v; u, v = 1, \ldots, m$, перестановочны, т. е. $\hat{W}_u = C + {\hat{W}_u}^0$, где $\hat{W}_u^0$ - перестановочные операторы. Тогда существует самосопряженный оператор. $\ddot{\wedge}$ и функции $\hat{W}_u^0(x)$ на R, такие что

$$\hat{W}_u^0 = \hat{W}_k^0()$$

Пусть $\{\mathscr{X}_k\}$-разбиение R, такое что $\hat{W}_k^0(x) \leqslant {\hat{W}_j}^0(x)$ при $x \in \mathscr{X}_k, \quad j \neq k$, и положим $\Lambda^0 = C + \min_k {\hat{W}_k}^0(X), {M_k}^0 = 1\mathscr{X}_k(X)$. Тогда условия 1) выполнены. Если $C^k = 0$, то это соответствует вычислению байесовского решающего правила в классической статистике: правило является детерминированным и для каждого x предписывает выбирать решение u, для которого апостериорное отклонение $\hat{W}_u(x)$ минимально [37, гл. IV].

П р и м е р 2. Условия предыдущего примера автоматически выполняются в случае двух гипотез S_0, S_1. Для простоты рассмотрим функцию потерь $W_\theta(u) = 1 - \delta_{\theta u}$, так что речь идет минимизации средней ошибки. Байесовское решающее правило имеет 'вид

$$M_0^0 = 1_{(0,\infty)}\left(\pi_0 S_0 - \pi_1 S_1\right), \quad M_1^0 = 1_{(-\infty,0]}\left(\pi_0 S_0 - \pi_1 S_1\right)$$

и минимальная ошибка

$$\mathscr{R}\left\{\mathbb{M}^0\right\} = \frac{1}{2}\left(1 - \left\|\pi_0 S_0 - \pi_1 S_1\right\|_1\right)$$

Если S_0, S_1-чистые состоя ния с векторами ψ_0, ψ_1, то

$$\mathscr{R}\left\{\mathbf{M}^0\right\} = \frac{1}{2}\left(1 - \sqrt{1 - 4\pi_0\pi_1\left|\langle\psi_0|\psi_1\rangle\right|^2}\right).$$

В общем случае уравнения оптимальности сводятся к сложной нелинейной задаче, часто геометрического характера. Много интересных явно решаемых случаев, в которых условия примера 1 не выполняются, рассмотрено Хелстромом [37], Р. Л. Стратоновичем [155] и В. П. Белавкиным [63]. Остано.вимся на задаче различения m чистых состояний с линейно независимыми векторами ψ_θ и априорными вероятностями $\pi_\theta > 0$. Можно считать, что $\mathscr{H}$ порождается векторами $\psi_\theta; \theta = 1, \ldots, m$. Кеннеди показал, что в этом случае байесовское решающее.правило имеет вид

$$M_u = |e_u\rangle\langle e_u|; u = 1, \ldots, m$$

где $\{e_u\}$ - некоторый ортонормированный базис в $\mathscr{H}$ (см. [37, гл. IV]). Таким образом, задача сводится к нахождению ортонормированного базиса, наилучшим образом приближающего систему $\{\psi_u\}$ в смысле критерия

$$\mathscr{R}\{\mathbf{M}\} = \sum_{\theta=1}^{in} \pi_\theta\left(1 - \left|\langle\psi_\theta|e_\theta\rangle\right|^2\right)$$

В [63] из общих условий оптимальности 1), 2) получено нелинейное уравнение для базиса $\{e_u\}$ и указан случай, когда оно решается явно. Пусть диагональные элементы матрицы $Q^{1/2}$, где $Q = \left[\sqrt{\pi_j\pi_k}\langle\psi_j|\psi_k\rangle\right]_{j,k=1}, \ldots, m$, совпадают и равны $\sqrt{q}$. Тогда оптимальный базис

$$e_k = \sum_{j=1}^{m} \sqrt{\pi_j}\lambda_{jk}\psi_j$$

где $[\lambda_{jk}] = Q^{1/2}$, причем минимальная ошибка

$$\min \mathscr{R}\{\boldsymbol{M}\} = 1 - mq$$

В частности, в «равноугольном» случае, когда $\langle\psi_j|\psi_k\rangle \equiv \gamma$ при $j \neq k$, а $\pi_\theta = 1/m$, получается формула Юна-Лэкса

$$\min \mathscr{R}\{\mathbf{M}\} = \frac{m-1}{m^2}(\sqrt{1 + (m-1)\gamma} - \sqrt{1-\gamma})^2$$

А. С. Холево заметил [42], что в случае р а в н о в е роятны Х чистых состояний имеет место оценка

$$\mathscr{R}\{M\} \leqslant \frac{1}{m}\sum_{\theta=1}^{m} \left\|\psi_\theta - e_\theta\right\|^2$$

Базис, минимизирующий правую часть, имеет вид

$$e_k = \sum_{j=1}^{m} a_{kj}\psi_j$$

где $[a_{yk}] = \Gamma^{-1/2}$ и $\Gamma = [\langle\psi_j|\psi_k\rangle]$, причем

$$\min_{\{e_\theta\}} \sum_{\theta=1}^{m} \|\psi_\theta - e_\theta\|^2 = \operatorname{Tr}\left(I - \Gamma^{1/2}\right)^2 = 2\operatorname{Tr}\left(I - \Gamma^{1/2}\right)$$

(теорема М. Г. Крейна). Отсюда.

$$\min \mathscr{R}\{M\} \leqslant \frac{1}{m}\operatorname{Tr}\left(I - \Gamma^{1/2}\right)^2$$

Решающее правило, отвечающее базису (2.8), асимптотическі оптимально в пределе почти ортогональных состояний, $\Gamma \to \mathrm{I}_3$ причем правая часть в (2.9) дает первый член асимптотики. В «равноугольном» случае (2.9) обращается в равенство.

2.3. Пропускная способность квантового канала связи. Набор операторов плотности $\{S_\theta\}$ определяет простейшую модель квантового канала связи (см. [39], [98]), для которого θ играет роль «сигнала», пробегающего входной алфавит $1, \ldots, \mathrm{m}$. Ко^2 дирование задается распределением вероятностей $\pi = \{\pi_\theta\}$: на входном алфавите, а декодирование-разложением единицы $\mathbf{M} = \{M_u\}$, где u пробегает выходной алфавит $1, \ldots, p$. Вероятность получить на выходе символ u при условии, что на входе сигнал θ, дается формулой (2.1). Таким образом, квантовый канал связи можно рассматривать как обычный канал со специфическими ограничениями на переходные вероятности, неявно выраженными формулой (2.1). Чему равна пропускная способность такого канала связи?

Рассмотрим информационное количество $\mathscr{I}_1(\pi, \mathbf{M})$, определяемое формулой типа (2.4) (где $\boldsymbol{u}$ пробегает от 1 до p) и величину $C_1 = \sup \mathscr{I}_1(\pi, M)$, где супремум берется по всевозможным кодированиям и декодированиям. В раниих работах для оценки пропускной способности использовалась величина

$$\bar{C} = \sup_{\pi}\left[H\left(\sum_{\theta=1}^{m}\pi_\theta S_\theta\right) - \sum_{\theta=1}^{m}\pi_\theta H\left(S_\theta\right)\right]$$

где $H(S) = -\operatorname{Tr} S\ln S$-энтропия фон Неймана квантового состояния S. В [40], [121] показано, что для любого кодиро- вания π и декодирования M

$$\mathscr{I}_1(\pi, \mathrm{M}) \leqslant H\left(\sum_{\theta=1}^{m}\pi_\theta S_\theta\right) - \sum_{\theta=1}^{m}\pi_\theta H\left(S_\theta\right)$$

причем если операторы S_θ неперестановочны, то неравенство строгое [1)]. По-видимому, при том же условии $C_1 \overline{< C}$, хотя в полной общности это не было установлено. Однако как показывают следующие рассуждения, величина C_1 также не может рассматриваться как пропускная способность.

Правильное определение пропускной способности должно быть связано с предельной скоростью асимптотически безошибочной передачи информации. Рассмотрим n-ю степень канала в пространстве $\mathscr{H}_n = \mathscr{C}^{\otimes^n}$, определя емую состояниями $S_v = S_{\theta_1} \otimes \ldots \otimes S_{\theta_n}$, где $v = (\theta_1, \ldots, \theta_n)$ - всевозможные слова входного алфавита длины n. Пусть $\mathscr{I}_n(\pi, \mathbf{M})$ и $C_n = \sup_{\pi;\mathrm{M}} \mathscr{I}_n(\pi, \mathbf{M})$ -

величины, определяемые для n-й степени канала аналогично $\mathscr{I}_1(\pi,\ \mathrm{M})$ и C_1. Информационное количество $\mathscr{I}_n(\pi,\ \mathrm{M})$ о бладает свойством аддитивности [40]

$$\sup_{M^{(n)},M^{(m)}} \mathscr{I}_{n+m}\left(\pi^{(n)}\times\pi^{(m)}, M^{(n)}\otimes M^{(m)}\right) =$$
$$= \sup_{M^{(n)}} \mathscr{I}_n\left(\pi^{(n)}, M^{(n)}\right) + \sup_{M^{(m)}} \mathscr{I}_m\left(\pi^{(m)}, M^{(m)}\right),$$

откуда следует, что последовательность $\{C_n\}$ субаддитивна, $C_n + C_m \leqslant C_{n+m}$, а следовательно, существует

$$C = \lim_{n\to\infty} C_n/n = \sup_n C_n/n.$$

Основываяссь на классической теореме кодирования, можно доказать, что при $R < C$ сушествугт такие кодирования и декодирования объема $N = \left[2^{nR}\right]$, что средняя ошибка

$$\bar{\lambda}(n,N) = \frac{1}{N}\sum_{j=1}^{N}\left(1 - \operatorname{Tr} S_{v_j} M_j\right)$$

стремится к нулю при $n\to\infty$, тогда как при $R > C$ она не стремится к нулю при любом выборе кодирования и декодирования [42]. Это дает основание назвать величину C пропускной способностью данного квантового канала связи.

Следует отметить, что для соответствующего классического канала «без памяти» последовательность $\{C_n\}$ аддитивна и поэтому $C \equiv C_n/_n = C_1$. Оказывается, что в квантовом случае возможно строгое неравенство

$$C_1 < C$$

1. Это утверждение было высказано Л. Б. Левитиным в 1969 г. что соответствует парадоксальному с классической точки зрения наличию «памяти» в произведении независимых каналов. Измерение в таком произведении может нести больше информации, чем сумма информаций, получаемых в каждой компоненте. Этот факт, разумеется, обусловлен необычными статистическими свойствами составных квантовых систем и является еще одним проявлением квантовой целостности.

Доказательство этого факта, данное в работе А. С. Холево [42], использует следующую оценку пропускной способности C для канала с чистыми состояниями $S_\theta = |\psi_\theta\rangle\langle\psi_\theta|$:

$$C \geqslant \tilde{C} \equiv -\ln\min_{\pi}\left[\sum_{j,k=1}^{m}\pi_j\pi_k\left|\langle\psi_j|\psi_k\rangle\right|^2\right]$$

в основе которой лежит неравенство (2.9) для средней ошибки и модифнкация метода случайных кодов, предложенная Р. Л. Стратоновичем и А. Г. Ванцян в [36]. Для двоичного канала ($m = 2$)

$$\widetilde{C} = 1 - \ln\left(1+\varepsilon^2\right) > 1 - \varepsilon^2/\ln 2,$$

где $\varepsilon = |\langle\psi_1|\psi_2\rangle|$. В случае «почти ортогональных состояний»

$$C_1 \leqslant 1 + \frac{1}{8}\varepsilon^2\ln\varepsilon^2 + o\left(\varepsilon^2\ln\varepsilon^2\right), \varepsilon\to 0$$

откуда следует (2.13) для достаточно малых ε.

В этой области остается ряд трудных нерешенных вопросов [98]. Определенная формулой (2.12) пропускная способность не вычислена в точном виде даже для двоичного канала. Ввиду серьезных аналитических трудностей, представляют большой

интерес всевозможные оценки и приближенные результаты (см. Бенджбаллах и Чарбит [67], В. П. Белавкин [63], Ингарден [110], Линдблад [121], Чемберс [74]). В общем случае $C \leqslant \bar{C}$, однако неизвестно, достигается ли здесь равенство для неперестановочных операторов плотности S_θ.

2.4. Общая формулировка. Как и в классической теории статистических решений [50], задается множество значений Θ неизвестного параметра θ, множество $\mathscr{X}$ решений x (часто $\mathscr{X} = \Theta$) и функция отклонения $W_\theta(x)$, определяющая качество решения x при данном значении параметра θ. Множество $\mathscr{X}$ измеримое (обычно стандартное) пространство и $W_\theta(x)$ ограничена снизу и измерима по x при фиксированном $\theta \in \Theta$.

Каждому значению θ соответствует оператор плотности S_θ в гильбертовом пространстве рассматриваемой квантовой системы, а решающее правило задается разложением единицы $\boldsymbol{M} : \mathscr{B}(\mathscr{X}) \to \mathscr{P}(\mathscr{C})$ в $\mathscr{H}$. Ортогональные разложения единицы описывают детерминированные решающие правила. При данном значении параметра θ и данном решающем правиле $\mathbf{M}$ решение выбирается в соответствии с распределением вероятно- стей

$$\mu_\theta^M(B) = \operatorname{Tr} S_\theta M(B); B \in \mathscr{B}(\mathscr{Q}).$$

Среднее отклонение, определяемое формулой

$$\mathscr{R}_\theta\{\mathbf{M}\} = \int\limits_{\mathscr{Q}} W_\theta(x)\mu_\theta^M(dx)$$

является для каждого $\theta \in \Theta$ аффинным функционалом на выпуклом множестве решающих правил $\mathfrak{R}(\mathscr{Q})$.

Решающее правило называется байесовским, если оно минимизирует байесовский риск

$$\mathscr{R}_\pi\{\mathbf{M}\} = \int\limits_{\Theta} \mathscr{R}_\theta\{\mathbf{M}\}\pi(d\theta)$$

для данного априорного распределения π на Θ, и минимаксньц, если оно минимизирует максимальное среднее отклонение $\max_\theta \mathscr{R}_\theta\{\mathbf{M}\}$. Как классическая, так и квантовая теории статистических решений включаются в общую схему, в которой состояния описываются точками произвольного выпуклого множества $\mathcal{S}$, причем значительная часть результатов классической теории Вальда переносится на эту схему, достигая естественных границ общности (А. С. Холево [41]). При минимальных требованиях на функцию отклонений установлены общие условия существования байесовского (Озава [133]) и минимаксного решающих правил, полнота класса байесовских решающих правил (Н. А. Богомолов [8]), аналог теоремы Ханта-Стейна [43], [8]. Обобщения понятия достаточности изучали Умегаки [158], А. С. Холево [41], Петц [139]. В силу ограниченности понятия условного ожидания, в квантовой теории статистических решений достаточность играет гораздо меньшую роль, чем в классической, зато на первый план выходят свойства инвариантности относительно подходящих групп симметрий (см. 3).

На основе соответствующего аппарата интегрирования в [41] получены необходимые и достаточные условия оптимальности и соотношение двойственности в байесовской задаче с произвольными $\Theta, \mathscr{X}$, обобщающие теорему из п. 2.2. Эти условия позволяют, в частности; дать исчерпывающее решение многомерной байесовской задачи оценивания среднего значения гауссовских состояний (В. П. Белавкин, Б. А. Гришанин [5], А. С. Холево [41]), которое иллюстрируется здесь одним при- мером.

В задаче оценивания $\Theta = \mathscr{Q}$ является конечномерным многообразием, в частности, областью в $\mathbf{R}^n$. В этом случае детерминированное решающее правило может быть

задано набором совместимых вещественных наблюдаемых $X_1, \ldots, X_n$ в $\mathscr{H}$. Согласно п. 1.2, произвольное решающее правило задается на56 бором совместимых наблюдаемых $X_1, \ldots, X_n$ в расширении $\mathscr{H}$ вида $\mathscr{H} \otimes \mathscr{H}_0$, где $\mathscr{H}_0$ - вспомогательное гильбертово пространство с оператором плотности S_0. При таком способе задания решающее правило называется оценкой многомерного параметра $\theta = (\theta_1, \ldots, \theta_n)$. В квантовой задаче оценивания, в отличие от классической, байесовские оценки могут оказаться существенно недетерминированными.

Пр и м е р. Пусть $\{S_{\alpha,\beta}; (\alpha, \beta) \in \mathbb{R}^2\}$ - семейство гауссовских состояний (см. п. 1.2.4) с характеристической функцией

где P, Q - канонические наблюдаемые, $\sigma^2 \geqslant \frac{1}{2}$. Рассмотрим байесовскую задачу оценивания параметра $\theta = (\alpha, \beta)$ с функцией отклонения

$$W_{\alpha,\beta}(\alpha', \beta') = g_1 (\alpha - \alpha')^2 + g_2 (\beta - \beta')^2$$

и гауссовским априорным распределением вероятностей с плот ностью $(2\pi)^{-1} \exp\left(-\frac{\sigma_0^2}{2}(\alpha^2 + \beta^2)\right)$. Решение этой задачи качественно зависит от величины g_1/g_2. Если $g_1/g_2 \leqslant (2s^2)^{-2}$ или $g_1/g_2 \geqslant\geqslant (2s^2)^2$, где $s^2 = \sigma^2 + \sigma_0^2$, то байесовские оценки детерминированы, т. е. задаются парой перестановочных самосопряженных операторов A, B в $\mathscr{C}$. В первом случае $A = \left(\frac{\sigma_0}{s}\right)^2 P, B = 0$, а во втором $A = 0, B = \left(\frac{\sigma_0}{s}\right)^2 Q$. Если же $(2s^2)^{-2} \leqslant g_1/g_2 \leqslant (2s^2)^2$, то оценки задаются перестановочными операторами

$$A = k_1 (P \otimes \mathrm{I}_0) + k_2 (\mathrm{I} \otimes P_0), B = k_2 (Q \otimes \mathrm{I}) - k_1 (\mathrm{I} \otimes Q_0)$$

в $\mathscr{H} \otimes \mathscr{H}_0$ (ср. (1.7)), где k_1, k_2-коэффициенты, нелинейно зависящие от s^2, g_1, g_2, а оператор плотности S_0 в $\mathscr{H}_0$ гауссовский и имеет характеристическую функцию

$$\operatorname{Tr} S_0 \exp[i (P_0 x + Q_0 y)] =$$
$$= \exp\left[-\frac{1}{4}\left(\sqrt{\frac{g_2}{g_1}}\frac{k_1}{k_2} x^2 + \sqrt{\frac{g_1}{g_2}}\frac{k_2}{k_1} y^2\right)\right]$$

Соответствующее разложение единицы в $\mathscr{H}$ отличается от (1.7) линейной заменой переменных. В отличие от аналогичной классической задачи, зависимость байесовского риска от весов g_1, g_2 также имеет существенно нелинейный характер.

2.5. Квантовые неравенства Рао-Крамера. Рассмотрим задачу оценивания в семействе состояний $\{S_\theta\}$, где $\theta = (\theta_1, \ldots \ldots, \theta_k) \in \mathbf{R}^k$. Решающее правило $\mathbf{M}$ назовем несмещенным, если для всех $\theta \in \Theta$

$$\int \ldots \int x_j \mu_\theta^M (dx_1 \ldots dx_k) = \theta_j; \quad j = 1, \ldots, k.$$

В предположении конечности вторых моментов определена матрица ковариации
$\mathbf{D}_\theta\{\boldsymbol{M}\} = \left[\int \ldots \int (x_i - \theta_i)(x_j - \theta_j) \mu_\theta^M (dx_1 \ldots dx_{*k})\right]; i, j = 1, \ldots, k.$

В классической статистике хорошо известно неравенство РаоКрамера, ограничивающее снизу матрицу ковариации несмещенных оценок. Входящая в эту границу информационная матрица Фишера однозначно определяется метрической геометрией симплекса «классических состояний», т. е. распределений вероятностей на пространстве элементарных событий Ω [50]. В квантовой статистике имеется много неэквивалентных неравенств типа Рао-Крамера, что связано с существенно более сложной геометрией множества состояний.

Поскольку неравенство Рао-Крамера имеет локальный характер, достаточно предполагать, что семейство состояний определено в окрестности фиксированной точки θ. Введем вещественное гильбертово пространство $L^2(S_\theta)$, определяемое как пополнение

множества $\mathfrak{P}_h(\mathscr{C})$ ограниченных вещественных наблюдаемых относительно скалярного произведения

$$\langle X, Y\rangle_\theta = \operatorname{Re}\operatorname{Tr} Y S_\theta X \equiv \operatorname{Tr} S_\theta X \circ Y,$$

где $X \circ Y = \frac{1}{2}(XY + YX)$ - йорданово произведение X, Y. Предположим, что

1. семейство $\{S_\theta\}$ сильно дифференцируемо в точке θ как функция со значениями в $\mathfrak{T}(\mathscr{C})$;
2. линейные функционалы $X \to \operatorname{Tr}\frac{dS_\theta}{d\theta}X$ непрерывны относительно скалярного произведения (2.15).

При этих условиях по теореме Ф. Рисса существуют симметризованнье логарифмические производные $L_\theta{}^j \in L^2(S_\theta)$, определяемые из условий

$$\operatorname{Tr}\frac{\partial S_\theta}{\partial \theta_j}X = \left\langle L_\theta^j, X\right\rangle, \quad \overline{X \in \mathfrak{B}_h}(\mathscr{H})$$

Формально,

$$\frac{\partial S_\theta}{\partial \theta_j} = S_{\theta^\circ L_\theta^j}$$

Тогда для любого решающего правила $\mathbf{M}$, имеющего конечные вторые моменты и удовлетворяющего условию лок а льной нес мещен но с ти

$$\int \ldots \int x_i \frac{\partial \mu_\theta^M}{\partial \theta_j}(dx_1 \ldots dx_k) = \delta_{ij}; \quad i, j = 1, \ldots, k$$

где $\frac{\partial \mu_\theta^M}{\partial \theta_j}(B) = \operatorname{Tr}\frac{\partial S_\theta}{\partial \theta_j}M(B)$, имеет место неравенство

$$\mathbf{D}_{\mathrm{e}}\{\mathbf{M}\} \geqslant \mathbf{J}_\theta^{-1}.$$

Здесь $\mathbf{J}_\theta = \left[\langle L_\theta{}^i, L_\theta{}^j\rangle_\theta\right]_{i,j=1,\ldots,k}$ - вещественная симметричная матрица - аналог информационной матрицы Фишера для симметризованной логарифмической производной.

С другой стороны, введем комплексные гильбертовы пространства $L_\pm{}^2(S_\theta)$ как пополнения $\mathscr{B}(\mathscr{H})$ относительно скалярных произведений

$$\langle X, Y\rangle_\theta^+ = \operatorname{Tr} X^* S_\theta Y, \langle X, Y\rangle_\theta^- = \operatorname{Tr} Y S_\theta X^*$$

и определим правую и левую логарифмические производнье $L_\theta{}^{\pm j}$ как решения уравнений

$$\operatorname{Tr}\frac{\partial S_\theta}{\partial \theta_j}X = \left\langle L_\theta^{\pm j}, X\right\rangle_\theta^\pm, \quad X \in \mathfrak{B}(\mathscr{H})$$

(существующие при тех же условиях 1), 2)). Формально

$$\frac{\partial S_\theta}{\partial \theta_j} = S_\theta L_\theta^{+j} = L_\theta^{-j} S_\theta$$

Тогда, при условии (2.18)

$$\mathbf{D}_\theta\{\mathbf{M}\} \geqslant \left(\mathbf{J}_\theta^\pm\right)^{-1}$$

где $\mathbf{J}_\theta^\pm = \left[\left\langle L_\theta^{\pm i}, L_\theta^{\pm j}\right\rangle_\theta^\pm\right]_{i,j=1,\ldots,k}$-комплексные эрмитовы матрицы, и (2.20) рассматривается как неравенство для эрмитовых матриц.

Формальное определение (2.17), симметризованной логарифмической пронзводной и неравенство (2.19) принадлежит Хелстрому, а неравенство (2.20) - Юну и Лэксу (см. [37, гл. VIII]). Другие неравенства были получены Р. Л. Стратоновичем [155]. Математически корректные определения логарифмических производных и вывод соответствующих неравенств дан в книге [43, гл. VI]. Пространства L^2, ассоциированные с квантовым состоянием, полезны и в других вопросах. Элементы этих пространств могут быть интерпретированы как (классы эквивалентности) неограниченных операторов в $\mathscr{C}$ ([43, гл. II]).

Неравенства (2.19), (2.20) дают существенно разлнчные, несравнимые границы для $\mathbf{D}_\theta\{\mathbf{M}\}$. В случае одномерного параметра ($k = 1$) всегда $J_\theta \leqslant J_\theta^\pm$, причем равенство имеет место тогда и только тогда, когда $\left[S_\theta, \frac{dS_\theta}{d\theta}\right] = 0$. В этом случае неравенство, основанное на симметризованной логарифмической произ- водной, оказывается наилучшим [37, гл. VIII]. С другой стороны; для двупараметрического семейства гауссовских состояний (2.14) неравенство (2.19) дает $\operatorname{Tr}\mathbf{D}_\theta\{\boldsymbol{M}\} \geqslant 2\sigma^2$, тогда как из. (2.20) вытекает $\operatorname{Tr}\mathbf{D}_\theta\{\mathbf{M}\} \geqslant 2\sigma^2 + 1$. Последняя граница достигается для несмещенных оценок, определяемых операторами типа (1.7). Неравенство (2.20), основанное на правой (или левой) логарифмической производной, вообще лучше приспособлено к задачам оценивания, в которых параметр допускает естественную комплексификацию (в последнем примере $\theta = \alpha + i\beta$).

Выражение

$$d\left(S_1, S_2\right) = \sqrt{2\left(1 - \left\|\sqrt{S_1}\sqrt{S_2}\right\|_1\right)}$$

определяет метрику в множестве операторов плотности $\subseteq (\mathscr{H})$. В более широком контексте алгебр фон Неймана эта метрика, известная как расстояние Бюреса, подробно изучалась Араки, Ульманом и др. (см. обзор Раджио в [141]). Если $\{S_\theta\}$-семейство, удовлетворяющее условиям 1), 2), то при $\Delta\theta \to 0$

$$d\left(S_\theta, S_{\theta+\Delta\theta}\right)^2 \approx \frac{1}{4}\sum_{i,j=1}^{k}\left\langle L_\theta^i, L_\theta^j\right\rangle_\theta \Delta\theta_i\Delta\theta_j$$

Таким образом, расстояние Бюреса эквивалентно в малом римановой метрике, определяемой квантовым аналогом информационной матрицы Фишера. Е. А. Морозова и И. Н. Ченцов в [35] описали всевозможные римановы метрики в $\subseteq (\mathscr{G})$ ($\dim\mathscr{H} < \infty$), монотонно инвариантные в категории марков-

ских морфизмов (аффинных отображений $\mathscr{C}(\mathscr{H})$ в себя). Ми-

нимальной в этом классе является риманова метрика в правой части (2.21).

12.2.3 3. Covariant Observables

3.1. Формулировка проблемы.

Пусть G - локально компактная группа, действующая непрерывно на транзитивном G-пространстве $\mathscr{X}$ и $\mathbf{V} : g \to V_g, g \in G$, - непрерывное (проективное) унитарное представление группы G в гильбертовом пространстве $\mathscr{H}$. Разложение единицы M: $B \to M(B), B \in \mathscr{B}(\mathscr{X})$ в $\mathscr{H}$ ковариантно по отношению k$\mathbf{V}$, если

$$V_g * M(B)V_g = M\left(g^{-1}B\right); g \in G, B \in \mathscr{B}(\mathscr{X})$$

В квантовой механике $\mathscr{L}$ является пространством значений физического параметра (обобщенной координаты) x, обладающего группой симметрий (движений) G. Фиксируем $x_0 \in \mathscr{X}$ и оператор плотности S_0. Соотношение

$$S_x = V_g S_0 V_g^*, \quad \text{где} \quad x = gx_0$$

описывает преобразование квантового состояния, отвечающее движению g. Рассмотрим обобщенную наблюдаемую M, удовлетворяющую условию ковариантности (3.1), и пусть $\mu_{:x}^M(B) = \operatorname{Tr} S_x M(B)$ - ее распределение вероятностей в состоянии S_x. Тогда условие (3.1) равносильно следующему:

$$\mu_{gx_0}^{\mathrm{M}}(gB) = \mu_{x_0}^{\mathrm{M}}(B); \quad B \in \mathscr{B}(\mathscr{X}), g \in G$$

для любого состояния S_0. Это означает, что статистика наблюдаемой M преобразуется согласно движениям g в пространстве обобщенной координаты $\mathscr{X}$ (см. пример в п. 1.2.3). Условие ковариантности, таким образом, дает правило для установления соответствия между классическими параметрами и квантовыми наблюдаемыми.

Такое соответствие является, конечно, далеко не однозначным. Среди множества ковариантных обобщенных наблюдаемых основной интерес представляют те, которые описывают предельно точные измерения соответствующего параметра. Рассмотрим задачу оценивания параметра $x \in \mathscr{X}$ в семействе состояний (3.2). Пусть на множестве $\mathscr{Z} = \Theta$ задана функция отклонения $W_\theta(x)$, такая что $W_{g\theta}(gx) = W_\theta(x)$. Среднее отклонение

$$\mathscr{R}_\theta\{M\} = \int_{\mathscr{X}} W_\theta(x) \mu_\theta^M(dx)$$

при условии (3.1) не зависит от θ. Минимум аффинного функционала (3.4) достигается в крайней точке выпуклого множества $\mathfrak{M}^{G,V}(\mathscr{P})$ ковариантных обобщенных наблюдаемых. Обозначим $\mathfrak{R}_0{}^{G,V}(\mathscr{Q})$ подмножество ковариантных наблюдаемых, задаваемых ортогональными разложениями единицы. Проглема соответствия в математическом плане сводится к изучению запаса элементов и структуры множеств $\mathfrak{M}_0^{G,V}(\mathscr{L}), \mathfrak{R}^{G,V}(\mathscr{X})$. В общем случае

$$\mathfrak{M}_0^{G,\mathrm{v}}(\mathscr{X}) \subsetneqq \operatorname{Extr} \mathfrak{M}^{G,\mathrm{v}}(\mathscr{X})$$

Целый ряд парадоксов в стандартной формулировке квантовой механики обусловлен тем, что множество $\mathfrak{M}_0{}^{G.V}(\mathscr{X})$ оказывается пустым. С другой стороны, Extr $\mathfrak{R}^G, V'(\mathscr{X})$ имеет значительно более обширный запас элементов, среди которых и находится обобщенная квантовая наблюдаемая, отвечающая данному классическому параметру.

3.2. Структура ковариантного разложения единицы. При специальных предположениях относительно $G, \mathscr{X}, \mathrm{V}$ можно дать прямое решение уравнения ковариантности (3.1), проливающее свет и на общий случай.

Пусть G - унимодулярна, а $G_0 = G/\mathscr{X}$ компактна, тогда на G существует σ-конечная инвариантная мера μ, а на $\mathscr{X}$ конечная инвариантная мера v, такая что $v(B) = \mu\left(\lambda^{-1}(B)\right)$, где $\lambda : g \to gx_0$.

Т е о рем а ([78], [43]). Пусть $\mathbf{V}$ - конечномерное представление группы G. Для любого ковариантного разложения единицы M найдется положительный оператор P_0, такой что $[P_0, V_g] = 0, g \in G_0$ и

$$M(B) = \int_B P(x) v(dx)$$

где плотность $P(x)$ определяется соотношением

$$P(gx_0) = V_g P_0 V_g^*$$

Дока з а тел и ство. Из тождества

$$\int_G \operatorname{Tr} V_g S V_g^* M(B)\mu(dg) = v(B), \quad S \in \Subset (\mathscr{H})$$

(см. [43, гл. IV]), полагая $S = (\dim \mathscr{H})^{-1}$ I, получаем $\operatorname{Tr} M(B) = (\dim \mathscr{H})^{-1} v(B)$. Поэтому существует плотность $P(x)$ со значениями в $\mathfrak{I}(\mathscr{H})$. Соотношение (3.5) вытекает из условия ковариантности.

Ограничение на P_0, вытекающее из условия нормировки $M(\mathscr{X}) = \mathrm{I}$, иногда удается выразить явно. Очень просто устроено множество $\mathfrak{R}^{G,V}(\mathscr{X})$ в случае, когда V есть неприводимое квадратично-интегрируемое представление ($\dim \mathscr{H} \leqslant +\infty$) унимодулярной группы $G = \mathscr{Q}$. Из соотношений ортогональности для V (см. [126]) следует, что при надлежащей нормировке μ

$$\int_G V_g S_0 V_{g\mu}^* (dg) = I$$

для любого оператора плотности S_0. Таким образом, формула

$$M(B) = \int_B V_g S_0 V_{g\mu}^* (dg)$$

устанавливает взаимно однозначное аффинное соответствие между $\mathfrak{R}^G$, $\mathrm{V}(G)$ и $\mathcal{S}(\mathscr{C})$. В частности, крайние точки множества $\mathfrak{R}^{G,V}(G)$ описываются формулой

$$M(B) = \int_B |\psi(g)\rangle\langle\psi(g)|\mu(dg)$$

где $\psi(g) = V_g\psi_0$, а ψ_0 - произвольный единичный вектор в $\mathscr{H}$. Семейство $\{\psi(g); g \in G\}$ образует переполненную систему, называемую в физике обобщенными когерентными состоямиями (обычные когерентные состояния отвечают неприводимому представлению ККС и специальному выбору вектора ψ_0, см. п. 1.2.4).

3.3. Обобщенные системы импримитивности. Если M в соотношении (3.1) ортогональное разложение единицы, то пара (V, M) называется системой импримитивности. Это понятие, введенное Дж. Макки (см. [126]), играет важную роль в теории представлений групп: представление V продолжается до системы импримитивности тогда и только тогда, когда оно индуцировано с подгруппы $G/\mathscr{X}$. Если же $\mathbf{M}$ - произвольное ковариантное разложение единицы, то (V, M) называется обобщенной системой импримитивности. Имеет место следующее обобщение теоремы М. А. Наймарка о расширении.

Те оре м а ([72], [148]). Пусть G - локально компактная группа, удовлетворяющая второй аксиоме счетности, $(\mathscr{X}, \mathscr{R}(\mathscr{D}))$ - стандартное измеримое пространство. Пусть $(\mathbf{V}, \mathbf{M})$ - обобщенная система импримитивности в $\mathscr{H}$, тогда существуют изометрическое вложение W пространства $\mathscr{C}$ в некоторое гильбертово пространство $\widetilde{\mathscr{H}}$ и система импримитивности $(\tilde{\mathbf{V}}, \mathrm{E})$ в $\widetilde{\mathscr{H}}$, такие что

$$V_g = W^* \tilde{V}_g W; \quad M(B) = W^* E(B) W$$

Если множество $\{E(B)W\psi|B \in \mathscr{B}(\mathscr{X}), \psi \in \mathscr{H}\}$ плотно в $\widetilde{\mathscr{H}}$, то $(\widetilde{V}, \mathrm{E})$ унитарно эквивалентно системе импримитивности, продолжающей представление в $\widetilde{\mathscr{H}} = L^2_{\mathscr{F}}(\mathscr{X},$ щ), индуцированное с подгруппы $\boldsymbol{G}/\mathscr{Q}^{1)}$.

Для иллюстрации рассмотрим пару $(\mathbf{V}, \mathbf{M})$, где $\mathbf{V}$ - неприводимое квадратично интегрируемое представление, $\boldsymbol{M}$ дается формулой (3.6). Искомое расширение в $\mathscr{C} = L^2(G, \mu)$ является модификацией конструкции для произвольной переполненной системы (см. п. 2.1.1), именно

$$\tilde{V}_g f(x) = f(gx); \quad E(B)f(x) = 1_B(x)f(x),$$

причем вложение W действует по формуле $W\psi(g) = \langle\psi(g)|\psi\rangle$. Подпространство $W\mathscr{H} \subset L^2(G, \mu)$ связано с воспроизводящим ядром $\mathscr{K}(g, g') = \langle\psi(g)|\psi(g')\rangle = \langle\psi_0|V(g^{-1}g')\psi_0\rangle$. Связь между обобщенными когерентными состояниями и индуцированными представлениями подробно исследовал Скутару [148]. В общем случае Каттанео [73] показал, что $\mathbf{M}$ имеет ограниченную плотность $P(x)$ относительно квазнинвариантной меры μ на $\mathscr{X}$ тогда и только тогда, когда подпространство $W\mathscr{H} \subset L^{\overset{\mathscr{K}}{2}}(\mathscr{X}, \mu)$ является гильбертовым пространством с воспроизводящим ядром (со значениями в $\mathscr{Y}(\mathscr{K})$).

3.4. Случай абелевой группы. Случай, когда $G = \mathscr{X}$ - абелева локально компактная группа, представляет интерес, в частности, в связи с проблемой канонической сопряженности в квантовой механике. Полное описание ковариантных разложений единицы для произвольного (непрерывного) представления V дается в терминах преобразования Фурье; при этом значения «плотности» $P(x)$ оказываются, вообще говоря, неограниченны-

1. $L^2\mathscr{K}(\mathscr{L}, \mu)$ обозначает гильбертово пространство функций на $\mathscr{L}$ со значениями в некотором гильбертовом пространстве $\mathscr{K}$, квадратично интегрируемых по мере μ. ми положительно-определенными формами. Излагаемые далее результаты могут быть получены как прямыми методами гармонического анализа, так и с помощью теоремы о расширении из предыдущего пункта (см. статью А. С. Холево в [141]). Обобщение на неабелевы группы типа I дано в работе [46].

Пусть $\hat{G}$-двойственная группа, $d\hat{g}$ - мера Хадра в $\hat{G}$.

Предложение 1. $\mathfrak{M}^{G,V}(G) \neq \varnothing$ тогда и только тогда,

когда спектр $\mathbf{V}$ абсолютно непрерывен относительно $d\hat{g}$.

Если это выполнено, то $\mathbf{V}$ разлагается в прямой интеграл факторных представлений, именно

$$\mathscr{H} = \int\limits_{\Lambda} \oplus \mathscr{H}(\lambda) d\lambda$$

где Λ-измеримое подмножество $\hat{G}, \{\mathscr{G}(\lambda); \lambda \in \Lambda\}$-измеримое семейство гильбертовых пространств с $\dim \mathscr{H}(\lambda) > 0$ для п. в. $\lambda \in \Lambda$, причем

$$V_g\psi = \int\limits_{\Lambda} \oplus \overline{\lambda(g)}\psi(\lambda)d\lambda, \text{ если } \psi = \int\limits_{\Lambda} \oplus \psi(-\lambda)d\lambda.$$

Здесь $\lambda(g)$−-начение характера $\lambda \in \hat{G}$ на элементе $g \in G$. Следующее утверждение вытекает из теоремы импримитивности Макки, которая обобщает теорему единственности Стоуна фон Неймана (п. 1.2.3).

Предложение 2. $\mathfrak{m}_0^{G,V}(G) \neq \varnothing$ тогда и только тогда, когда $\Lambda = \hat{O}$ с точностью до множества нулевой меры и $\dim \mathscr{H}(\lambda) = \text{const}$ для п. в. $\lambda \in \hat{G}$.

Ядром будем называть семейство $\{P(\lambda,\lambda');\lambda,\lambda'\in\Lambda\}$, где $P(\lambda,\lambda')$ - сжимающие операторы из $\mathscr{H}(\lambda')$ в $\mathscr{H}(\lambda)$, причем комплексная функция $\langle\varphi(\lambda)|P(\lambda,\lambda')\psi(\lambda')\rangle_\lambda$ измерима по мере $d\lambda\times d\lambda'$ для любjx $\varphi=\int\oplus\varphi(\lambda)d\lambda,\psi=\int\oplus\psi(\lambda)d\lambda\in\mathscr{H}$ ($\langle\cdot|\cdot\rangle_\lambda$ обозначает скалярное произведение в $\mathscr{H}(\lambda)$). Ядро положительно определено, если

$$\int\limits_\Lambda\int\limits_\Lambda\langle\varphi(\lambda)|P(\lambda,\lambda')\varphi(\lambda')\rangle_\lambda d\lambda d\lambda'\geqslant 0$$

для всех $\varphi\in\mathscr{C}_1=\left\{\varphi:\int\limits_\Lambda\|\varphi(\lambda)\|_\lambda d\lambda<\infty\right\}$. Для таких ядер однозначно с точностью до эквивалентности определяется диагональное значение $P(\lambda,\lambda)$ (см. [141]). Обозначим $1_B(\lambda)=\int\limits_B\lambda(g)dg$, где dg-мера Хаара в G.

Т е о р ема. Соотношение

$$\langle\varphi|M(B)\psi\rangle=\int\limits_\lambda\int\limits_\Lambda\langle\varphi(\lambda)|P(\lambda,\lambda')\varphi(\lambda')\rangle_\lambda\hat{1}_B(\lambda-\lambda')d\lambda d\lambda',$$

где B пробегает компактные подмножества в $G,\varphi,\psi\in\mathscr{H}_1$, устанавливает взаимно однозначное соответствие между ковариантными разложениями едниицы в $\mathscr{H}$ и кллассами эквивалентности положительно определенных ядер $\{P(\lambda,\lambda')\}$, таких что $P(\lambda,\lambda)=\mathrm{I}_\lambda$ (единичный оператор в $\mathscr{H}(\lambda)$).

Эта теорема сводит вопрос об описании множества $\operatorname{Extr}\mathfrak{R}^{G,V}(G)$ к нахождению крайних точек выпуклого множества положительно определенных ядер $\{P(\lambda,\lambda')\}$, удовлетворяющих условию $P(\lambda,\lambda)=\mathrm{I}_\lambda$. В полном объеме эта задача не решена даже для конечного Λ. Можно, однако, выделить подкласс множества $\operatorname{Extr}\mathfrak{R}^{G,V}(G)$, существенный для квантовомеханических приложений.

Для простоты ограничимся далее случаем, когда $\dim\mathscr{H}(\lambda)=\mathrm{const}$, $\lambda\in\Lambda$. Обозначим $\mathfrak{R}_c^{G,v}(G)$ класс ковариантных разложений единицы, ядра которых удовлетворяют соотношению

$$P(\lambda,\lambda')P(\lambda',\lambda'')=P(\lambda,\lambda'');\lambda,\lambda',\lambda''\in\Lambda$$

Если $\Lambda=G$, то этот класс совпадает с $\mathfrak{M}_0^{G,\mathrm{v}}(G)$, с другой стороны, $\mathfrak{M}_c^{G,\mathrm{v}}(G)\subset\operatorname{Extr}\mathfrak{M}^{G,\mathrm{v}}(G)$, причем совпадение имеет место только, если Λ состоит из двух точек. Все элементы $\mathfrak{M}_c^{G,\mathrm{v}}(G)$ получаются друг из друга калибровочными преобразованиями

$$M'(B)=U^*M(B)U$$

где $U=\int\limits_\Lambda\oplus U(\lambda)d\lambda$ - разложимый унитарный оператор в $\mathscr{H}=\int\limits_\Lambda\oplus\mathscr{H}(\lambda)d\lambda$.

Если реализовать $\mathscr{H}$ как $L^2_{\mathscr{K}}(\Lambda,d\lambda)$, где $\mathscr{H}(\lambda)\equiv\mathscr{K},\lambda\in\Lambda$, то в классе $\mathfrak{R}_c^{G,v}(G)$ выделяется разложение единицы M_c, определя емое ядром $P(\lambda,\lambda')\equiv\mathrm{I}_{\mathscr{K}}$ (единичный оператор в $\mathscr{K}^2$), для которого

$$\langle\psi|M_c(B)\varphi\rangle=\int\limits_\Lambda\int\limits_\Lambda\langle\psi(\lambda)|\varphi(\lambda')\rangle\hat{\mathscr{K}^{1_B}}(\lambda-\lambda')d\lambda d\lambda'$$

Всякое $M\in\mathfrak{R}_c^{G,v}(G)$ имеет ядро вида $U(\lambda)^*U(\lambda')$, где $\{U(\lambda)\}$-измеримое семейство унитарных операторов в $\mathscr{K}$.

3.5. Каноническая сопряженность в квантовой механике. Пусть x-одномерный параметр, так что $G=\mathscr{D}$ является ве- щественной прямой $\mathbf{R}$ (случай параметра сдвига),

или единичной окружностью T (случай параметра поворота), и пусть $x \to \to V_\alpha = e^{-ixA}$ - унитарное представление группы G в $\mathscr{H}$. Спектр Λ оператора A содержится в двойственной группе $\hat{G}$, которая совпадает с $\mathbf{R}$ в случае $G = \mathbf{R}$ и с множеством целых чнсел $\mathbf{Z}$ в случае $G = \mathbf{T}$.

Условие ковариантности обобщенной наблюдаемой $\mathbf{M}$ имеет вид

$$V_x^* M(B) V_x = M(B - x); \quad B \in \mathscr{B}(G), x \in G$$

где $B - x = \{y : y + x \in B\}$, причем в случае $G = \mathbf{T}$ имеется в виду сложение по модулю 2π. Вводя операторы

$$U_y = \int\limits_G e^{iyx} M(dx), \quad y \in \hat{G}$$

получаем, что (3.9) равносильно соотношению Вейля (см. п. 1.2.3)

$$U_y V_x = e^{ixy} V_x U_y; \quad x \in G, y \in \hat{G}$$

в котором, однако, операторы U_v, вообще говоря, неунитарны. В этом смысле обобщенная наблюдаемая $\boldsymbol{M}$ является канонически сопряженной к наблюдаемой A.

Для обобщенной канонической пары $(A, \mathbf{M})$ имеет место соотношение неопределенностей [100]

$$\Delta_S^M(y) \cdot \mathbf{D}_S(A) \geqslant 1/4; \quad y \in \hat{G}$$

где $\Delta_S^M(y) = y^{-2} \left\{ |\operatorname{Tr} S U_y|^{-2} - 1 \right\}, \quad y \neq 0$, есть некоторая функциональная мера неопределенности ковариантной обобшенной наблюдаемой M в состоянии S-(см. [43, & IV.7]). Если $G = \mathbf{R}$ и $\mathbf{M}$ имеет конечнуго дисперсию $\mathbf{D}_S(\mathbf{M})$, то $\lim_{y \to 0} \Delta_S^{\mathbf{M}}(y) = \mathbf{D}_S(\mathbf{M})$, так что из (3.11) следует обобщение соотношения неопределенностей Гейзенберга

$$\mathbf{D}_S(\mathbf{M}) \mathbf{D}_S(A) \geqslant 1/4$$

Для параметра поворота ($G = \mathrm{T}$) дисперсия не является адекватной мерой неопределенности, и неравенство (3.11) следует рассматривать как окончательное. Различные формы соотношения неопределенностей для угловых переменных обсуждались в обзорах [19], [17]. Следует отметить, что обобщенная наблюдаемая угла поворота существует всегда, поскольку условня предложения 1 из предыдущего пункта выполняются автоматически ($\hat{G} = \mathbf{Z}$). С другой стороны, условия предложения 2 не могут быть выполнены, если $\dim \mathscr{H} < \infty$ (как для систем с конеqным спином), и в этих случаях обычной наблюдаемой угла поворота не существует.

Нанбольший интерес представляют ковариантные обобщенные наблюдаемые, имеющие минимальную неопределенность.

Те орем а ([100]). Пусть $S = |\psi\rangle\langle\psi|$ - чистое состояние, тогда

$$\min_{M \in \mathbb{M}^{G,\ \mathrm{V}(G)}} \Delta_S^M(y) = y^{-2} \left[\left(\int\limits_{\hat{\sigma}} \|\psi(y')\| \, \|\psi(y' + y)\| \, dy' \right)^{-2} - 1 \right]$$

В частности, для $G := \mathbf{R}$

$$\min_{\mathbf{M} \in \mathbb{N}^{\mathbf{R},\mathbf{V}}(\mathbf{R})} \mathbf{D}_s(\mathbf{M}) = \int\limits_{\mathbf{R}} \left(\frac{d}{dy} \|\psi(y)\| \right)^2 dy$$

где $\psi(y)$ - компоненты вектора ψ в представлении, диагонализующем оператор A. Минимум достигается на ковариантной наблюдаемой $\boldsymbol{M}^*$ класса $\mathfrak{R}_c^{G,v}$, которая задается ядром $P^*(y,y')$ таким, что $P^*(y,y')\,\psi(y') / \|\psi(y')\| = \psi(y)/\|\psi(y)\|; \quad y, \quad y' \in \Lambda$.

Величины (3.12), (3.13) дают внутреннюю меру неопределенности параметра x в состоянии S.

Таким образом, требования ковариантности и минимальной неопределенности (относительно чистых состояний) определяют канонически сопряженную обобщенную наблюдаемую однозначно с точностью до калибровочного преобразования (3.7). Следует отметить, что аналогичная степень произвола остается и в стандартной формулировке квантовой механики, поскольку в случае $\Lambda = \hat{G}$ класс ${\mathfrak{P}_c}^{G,V}(G)$ совпадает с классом ковариантных наблюдаемых $\mathfrak{R}_0^{G,v}(G)$.

П р и м ер. Рассмотрим квантовую систему с положительным гамильтонианом H. Представление $t \to V_t = e^{-iHt}$ группы временных сдвигов не удовлетворяет условиям предложения 2 предыдущего пункта, поскольку $\Lambda \subset \mathrm{R}_+$. Поэтому ковариантной наблюдаемой временного сдвига не существует [1)]. Предположим для простоты, что $\Lambda = \mathbb{R}_+$и что спектр H однороден (т. е. имеет постоянную кратность для п. в. $\lambda \in \Lambda$). Тогда H унитарно эквивалентен оператору умножения на λ в гильбертовом пространстве $\mathscr{C} = L^2_{\mathscr{K}}(\mathbf{R}_+)$квадратично-интегрируемых функций $\psi = [\psi(\lambda)]$ на $\mathbb{R}_+$со значениями в некотором гильбертовом пространстве $\mathscr{K}$. Ковариантные обобщенные наблюдаемые класса $\mathfrak{M}_c^{\mathbf{R},V}(\mathbb{R})$ с точностью до калибровочного преобразования (3.7) эквивалентны наблюдаемой $\mathbf{M}_c$, определяемой соотношением (3.8), т. е.

$$\langle\psi|M_c(B)\varphi\rangle = \int\limits_{R_+}\int\limits_{R_+} \langle\psi(\lambda)|\varphi(\lambda')\rangle\, \mathscr{F}\int\limits_B e^{i(\lambda'-\lambda)\tau}\frac{d\tau}{2\pi}.$$

Разложение единицы $\mathbf{M}_c$ является обобщенной спектральной мерой в смысле [2] максимального симметричного (но не самосо-

1. На трудности с определением наблюдаемой времени в квантовой механике указывал Паули (см. Handbuch der Physik.-1958.-5/1.-C. 60-63). пряженного) оператора

$$T = i\frac{d}{d\lambda}, \quad \mathscr{D}(T) = \{\psi : \psi \text{ абсолют но непрерывна, } \psi(0) = 0,$$
$$\int\limits_{\mathbf{R}_+} \left\| \frac{d}{d\lambda}\psi(\lambda) \right\|^2_{\mathscr{K}} d\lambda < \infty \Bigg\}.$$

Минимальное расширение Наймарка разложения единицы $\mathbf{M}_c$ в пространстве $\widetilde{\mathscr{H}} = L^2_{\mathscr{K}}(\mathbf{R})$ дается формулой, аналогичной (3.14), с заменой $\mathbf{R}_+$на $\mathbf{R}$, и является спектральной мерой самосопряженного оператора $i\frac{d}{d\lambda^3}L^2_{\mathscr{K}}(\mathbf{R})$.

3.6. Локализуемость. Пусть $\mathbf{W}$—-унитарное представление группы, описывающей кинематику данной квантовой системы (универсальной накрывающей группы Галилея в нерелятивистском или группы Пуанкаре в релятивистском случае), в гильбертовом пространстве $\mathscr{C}$ и пусть $\mathbf{U}$ - ограничение $\mathbf{W}$ на универсальную накрывающую G группы евклидовых преобразований $g : x \to Ax + b, x \in \mathbf{R}^3$. Система называется локализуемой по Вайтману, если в $\mathscr{K}$ существует ортогональное разложение единицы $\mathbf{E}$ на σ-алгебре $\mathscr{B}(\mathbf{R}^3)$ борелевских подмножеств координатного пространства $\mathbf{R}^3$, удовлетворяющее условию евклидовой ковариантности

$$U_g^* E(B) U_g = E\left(g^{-1}B\right); g \in G, B \in \mathscr{B}\left(\mathbb{R}^3\right)$$

При этом условии для любой области $B \subset \mathbf{R}^3$ найдется вектор состояния ψ такой, что $\langle\psi|E(B)\psi\rangle = 1$, т. е. вероятность обнаружения системы в области B равна 1. Для локализуемой системы определены совместимые наблюдаемые координат

$$Q_j = \iiint x_j E\left(dx_1 dx_2 dx_3\right); j = 1, 2, 3$$

ковариантные относительно евклидовых преобразований.

Используя то обстоятельство, что (U, E) - система импримитивности, можно доказать, что локализуемыми по Вайтману являются все массивные частицы и релятивистские безмассовые частицы с нулевой спиральностью. Безмассовые частицы с ненулевой спиральностью (фотон, нейтрино) оказываются нелокализуемыми (Ньютон, Вигнер, 1949, Вайтман, 1962). Такой вывод не согласуется с экспериментальной локализуемостью фотона; более того, как показал Хегерфельдт, такое понятие локализуемости приводит к противоречию с требованием причинности в релятивистской динамике (см., например, [55]). Эти трудности снимаются, если в определении локализуемости допускаются произвольные разложения единицы. Неортогональное разложение единицы M, описывающее локализацию фотона, было -указано, в частности, в работах Крауса (в сб. [159]), А. С. Холево [99]. Полная классификация соответствующих обобщенных систем импримитивности, при дополнительном условии кова' риантности относительно преобразований подобия, включающая характеризацию крайних точек, дана Кастрижьяно [71]. Релятивистские безмассовые частицы оказываются п и бл л ж е н но локализуемыми в том смысле, что $\sup_{\|\psi\|=1}\langle\psi|M(B)\psi\rangle = 1$ для любой области $B \subset \mathbf{R}^3$. Наблюдаемые координаты, определенные соотношением (3.15), являются самосопряженными, но неперестановочными операторами и поэтому не имеют совместной спектральной меры.

В ряде работ, обзор которых имеется в статьях Али, Пруговечки [55], развивалась идея стохастической локализуемости в фазовом пространстве. Результаты этих работ также указывают на то, что обобщенная статистическая модель квантовой механики дает возможность, по крайней мере, смягчить известные противоречия между релятивистской инвариантностью и нелокальностью квантовомеханического описания.

12.3 Evolution of an Open System

12.3.1 1. Transformations of Quantum States and Observables

Динамика изолированной квантовой системы, описываемая однопараметрической группой унитарных операторов, обратима во времени. Эволюция открытой системы, подверженной внешним воздействиям, будь то процесс установления равновесия с окружением или взаимодействие с измерительным прибором, обнаруживает черты необратимости. В математическом плане такие необратимые изменения описываются вполне положительными отображениями.

1.1. Вполне положительные отображения.

Пусть $\mathscr{A} \subset \mathfrak{B}(\mathscr{H})$ - некоторая C^*-алгебра операторов, т. е. подпространство $\mathfrak{B}(\mathscr{H})$, замкнутое относительно алгебраических операций, инволюции и перехода к пределу по операторной норме (см., например, [32], [9]). Обозначим $\mathfrak{P}_n$ алгебру комплексных $n \times n$-матриц. Линейное отображение Φ из $\mathscr{A}$ в $\mathscr{P}(\mathscr{K})$ (где $\mathscr{K}$ гильбертово пространство) называется положительным, если из $X \in \mathfrak{A}, X \geqslant 0$ следует $\Phi[X] \geqslant 0$, и вполне положительным, если для любого $n \geqslant 1$ отображение $\Phi_n C^*$-алгебры $\mathscr{A} \otimes \mathfrak{M}_n$ в C^*-алгебру $\mathfrak{B}(\mathscr{K}) \otimes \mathfrak{M}_n$, определяемое формулой $\Phi_n(X \otimes Y) = \Phi_n(X) \otimes Y$, является

положительным. Другими словами, для любой матрицы $[X_{jk}]_{j,k=1,\ldots,n}$ с элементами $X_{jh} \in \mathscr{A}$, положительно определенной в том смысле, что $\sum_{k=1}^{n} \langle \varphi_j | X_{jk} \varphi_k \rangle \geqslant 0$ для любого набора $\{\varphi_j\} \subset \mathscr{H}$, матрица

$[\Phi(X_{jk})]_{j,k=1,\ldots,n}$ также является положительно определенной.

Еще одно эквивалентное определение: для любых конечных на- боров $\{X_i\} \subset \mathscr{A}$ и $\{\psi_j\} \subset \mathscr{H}$

$$\sum_{j,k} \left\langle \psi_j | \Phi \left[x_j^* X_k \right] \psi_k \right\rangle \geqslant 0$$

Для положительного отображения имеет место неравенство Кэдисона-Шварца

$$\Phi[X]^* \Phi[X] \leqslant \|\Phi\| \Phi\left[X^* X\right]$$

для всех X Я таких, что $X^*X = XX^*$. Если Φ вполне положительно, то это неравенство выполняется для всех X я. Пример положительного, но не вполне положительного отображениятранспонирование в $\mathfrak{D}_n$. Если Φ положительно и $\mathfrak{A}$, либо $\Phi(\mathrm{Re})$ коммутативны, то Φ вполне положительно. Таким образом, свойство полной положительности проявляется лишь в некоммутативной ситуацин.

Отображение $\pi : \mathfrak{A} \to \mathfrak{B}(\tilde{\mathscr{K}})$. называется *-гомоморбизмом (представлением), если оно сохраняет алгебраические операции и инволюциіо.

Т е о р ем а (Стайнспринг, 1955). Пусть $\mathscr{A} \subset \mathfrak{B}(\mathscr{H})$ – C^*-алгебра с единицей и $\Phi : \mathfrak{A} \to \mathfrak{B}(\mathscr{K})$-линейное отображение. Φ вполне положительно тогда и только тогда, когда оно допускает представление

$$\Phi[\lambda] = V^* \pi[X] V$$

где V-ограниченное линейное отображение из $\mathscr{K}$ в некоторое гильбертово пространство $\breve{\mathscr{K}}, \pi$ - -гомоморфизм $\mathfrak{A}$ В $\mathfrak{F}(\widetilde{\mathscr{K}})$.

Существует единственное с точностью до унитарной эквивалентности минимальное представление (1.3), характеризующееся свойством: по дпространство $\{\pi[\curvearrowright] V\psi : X \in \mathscr{A}, \psi \in \mathcal{K}\}$ плотно в $\tilde{\mathcal{K}}$.

Доказательство прямого утверждения представляет собой обобщение конструкции Гельфанда-Наймарка-Сигала (ГНС), которая соответствует случаю положительного линейного функционала на $\mathscr{A}(\dim \mathscr{K} = 1)$ [32], [9]. На алгебраическом тензорном произведении $\mathfrak{A} \otimes \mathscr{K}$ определяется (псевдо-) скалярное произведение, такое что

$$\langle X \otimes \varphi | Y \otimes \psi \rangle = \langle \varphi | \Phi\left[X^* Y\right] \psi \rangle_{\mathscr{K}}; \quad X, Y \in \mathscr{A}; \varphi, \psi \in \mathscr{K}.$$

Неотрицательность скалярного квадрата следует из (1.1). Пусть $\widetilde{\mathscr{K}}$ гильбертово пространство, получающееся в результате факторизации и пополнения $\mathscr{A} \otimes \mathscr{G}$ по этому скалярному произведению. Соотношения

$$\pi[X](Y \otimes \psi) = XY \otimes \psi$$
$$V_\varphi = I \otimes \varphi$$

определяют переходом в $\tilde{\mathscr{K}}$ объекты V, л, удовлетворяющие соотношению (1.3).

З а м е ч а н и е. Если $\mathscr{X}$ - метризуемый компакт и $\mathbf{M}$ - разложение единицы в $\mathscr{K}$ на σ-алгебре борелевских подмножеств $\mathscr{B}(\mathscr{X})$, то отображение

$$f \to \int_{\mathscr{X}} f(x) M(dx); \quad f \in C(\mathscr{Q})$$

C^*-алгебры $C(\mathscr{X})$ непрерывных комплексных функций на $\mathscr{Z}$ в $\mathscr{Y}(\mathscr{K})$ является (вполне) положительным. Теорема Стайнспринга в этом случае дает расширение Наймарка для $\mathbf{M}$, поскольку *-гомоморфизм $C(\mathscr{X})$ задается ортогональным разложением единицы.

Всякая алгебра фон Неймана $\mathscr{B}$ является C^*-алгеброй с единицей. Положительное отображение Φ алгебры $\mathscr{B}$ называется нормальныц, если из $X_\alpha \uparrow X$ в $\mathscr{B}$ следует $\Phi[X_\alpha] \uparrow \Phi[X]$.

С лед ств и е ([117]). Всякое нормальное вполне положительное отображение $\Phi : \mathfrak{B}(\mathscr{H}) \to \mathscr{P}(\mathscr{C})$ имеет вид

$$\Phi[\ddot{\Lambda}] = \sum_{n=1}^{\infty} V_n^* \bar{\Lambda}_n$$

тде ряд $\sum\limits_{n=1}^{\infty} V_n^* V_n$ сходится сильно в $\mathfrak{B}(\mathscr{H})$.

Доказат ельство. Если Φ нормально, то представление π в формуле (1.3) также можно считать нормальным. Известно, qто всякое нормальное представление алгебры $\mathfrak{B}(\mathscr{H})$ в пространстве $\tilde{\mathscr{K}}$ кратно единичному, т. е. $\tilde{\mathscr{K}} = \mathscr{H} \otimes \mathscr{H}_0$ и $\pi[\lambda] = X \otimes \mathrm{I}_0$, где $\mathscr{C}_0$-некоторое гильбертово пространство, I_0-единичный оператор в $\mathscr{C}_0$ (см., например, [78, гл. 9]). Пусть $\{e_j\}$-ортонормированный базис в $\mathscr{C}_0$, тог да $V\psi = \sum\limits_{n=1}^{\infty} V_n \psi \otimes e_n$, а соотношение (1.3) переходит в (1.4).

Обзор свойств вполне положительных отображений имеется в статье Штермера в сборнике [85]. Андо и Чой [57] рассмотрели н е ли н е й н ы е вполне положительные отображения и установили для них обобщение теоремы Стайнспринга.

1.2 Операции, динамические отображения.

Алгебра $\mathscr{B}(\mathscr{C})$ как банахово пространство является сопряженным к пространству ядерных операторов $\mathfrak{T}(\mathscr{C})$ (см. П. 1.1.1). Если Ψ - линейное отображение в $\mathfrak{T}(\mathscr{G})$, положительное в том смысле, что $\Psi[T] \geqslant 0$, если $T \geqslant 0$, то Ψ ограничено (см., например, [78, гл. 2]) и поэтому имеет сопряженное отображение $\Phi = \Psi^* : \mathscr{B}(\mathscr{H}) \to \to \mathscr{P}(\mathscr{G})$, которое является линейным положительным нормальным отображением; более того, всякое Φ с такими свойствами является сопряженным к некоторому Ψ. Если Ψ положительно и, кроме того, $\operatorname{Tr}\Psi[T] \leqslant \operatorname{Tr} T$ для всех $T \in \mathfrak{T}(\mathscr{C}), T \geqslant 0$, то Ψ на- зывается операцией (в пространстве состояний). Это равноснльно тому, что $\Phi[\mathrm{I}] \leqslant \mathrm{I}$. Отображение Φ также называется операцией (в алгебре наблюдаемых).

В квантовой статистике операции описывают изменения состояний (наблюдаемых) открытой системы в результате эволюции или макроскопического воздействия, включая отбор по какому-либо признаку (например, по результату измерения) в соответствующем статистическом ансамбле. Если S-оператор плотности исходного состояния, то число $\operatorname{Tr}\Psi[S]$ интерпретируется как доля отобранных представителей ансамбля, а $\Psi[S]/\operatorname{Tr}\Psi[S]$ как оператор плотности, описывающей новое состояние отобранного ансамбля. Термин «операция» был введен в известной работе Хаага и Кастлера (1964), посвященной обоснованию квантовой теории поля. Базирующийся на понятии операции аксиоматический подход к квантовой механике был развит Дэвисом и Льюисом, Людвигом и другими авторами (см., например, [78], [125], [116], [85]).

В динамической теории особенно важны операции, переводящие состояние в состояние. Это равносильно тому, что $\operatorname{Tr}\Psi[T] = \operatorname{Tr} T$ для всех $T \in \mathfrak{T}(\mathscr{C})$ или же $\Phi[\mathrm{I}] = \mathrm{I}$, где $\Phi = \Psi^*$. Если, кроме того, Φ - вполне положительно, то Ψ (или Φ) называется динамическим

отображением [1)]. Из теоремы Вигнера (п. 1.2.1) следует, что обратимые динамические отображения описываются формулами

$$\Psi[T] = UTU^*, \quad \Phi[X] = U^*XU$$

где U - унитарный оператор в $\mathscr{C}$ (если U антиунитарный, то Φ не может быть линейным отображением). В общем случае динамические отображения описывают необратимые эволюции и являются некоммутативным аналогом марковских отображений в теории вероятностей. Мерой необратимости может служить относительная энтропия квантовых состояний

$$H(S_2|S_1) = \operatorname{Tr} S_1 (\ln S_1 - \ln S_2)$$

О свойствах относительной энтропии см. Линдблад [122], Верль. [166], Петц [139]). Важнейшим является о бо бш е н н а я H - те орем а: для любого динамического отображения Ψ:

$$H(\Psi[S_2]|\Psi[S_1]) \geqslant H(S_2|S_1)$$

Согласно следствию из п. 1.1, динамическое отображение допускает представление

$$\Psi[T] = \sum_{n=0}^{\infty} V_n T V_n^*, \Phi[X] = \sum_{n=0}^{\infty} V_n^* \tilde{\lambda} V_n$$

где $\sum\limits_{n=0}^{\infty} V_n^* V_n = \mathrm{I}$. Отсюда нетрудно получить

1. На свойство полной положительности эволюции открытой системы. было указано, в частности в работах [117], [39].

С ле д с т в и е ([123]). Отображение $\Psi : \mathfrak{T}(\mathscr{H}) \to \mathfrak{T}(\mathscr{H})$ является динамическим тогда и только тогда, когда существуют гильбертово пространство $\mathscr{H}_0$, состояние S_0 в $\mathscr{H}_0$ и унитарный оператор U в $\widetilde{\mathscr{B}} = \mathscr{H} \otimes \mathscr{H}\mathscr{C}_0$, такие что

$$\Psi[S] = \operatorname{Tr}_{\mathscr{H}_0} U (S_{\otimes} S_0) U^*$$

где $\operatorname{Tr}\mathscr{G}_0$ - частичный след в $\mathscr{H}_0$.

Таким образом, динамическое отображение расширяется до обратимой эволюции составной системы, включающей исходную открытую систему и «окружение», причем возможность такого расширения обусловлена свойством полной положительности.

1.3 Условные ожидания.

Так называются отображения $\mathscr{E} : \mathscr{B}(\mathscr{C}) \to \mathscr{D}(\mathscr{C})$, являющиеся идемпотентами ($\mathscr{E}^2 = \mathscr{E}$) с единичной нормой. $\mathscr{E}$ отображает $\mathscr{B}(\mathscr{H})$ на C^*-подалгебру $\mathscr{A} = \{X : X \in \mathscr{B}(\mathscr{H}), \mathscr{E}[X] = X\}$. Если $\mathscr{E}$ нормально, то $\mathscr{A}$-алгебра фон Неймана. Условное ожидание согласовано с состоянием S, если $\operatorname{Tr} S\mathscr{E}[X] = \operatorname{Tr} SX; X \in \mathscr{B}(\mathscr{H})$. Томияма показал, что условное ожидание является положительным отображением и обладает свойством

$$\mathscr{E}(XYZ) = X\mathscr{E}(Y)Z; \quad Y \in \mathscr{B}(\mathscr{H}); \quad X, Z \in \mathscr{A},$$

которое включалось в первоначальное определение, данное Умегаки [158]. На самом деле всякое условное ожидание вполне положительно.

Общий критерий существования нормального условного ожидания в алгебрах фон Неймана дал Такесаки [157]. В случае $\mathscr{B}(\mathscr{C})$ этот критерий имеет следующую формулировку. Пусть S - невырожденный оператор плотности, тогда с ним связана модулярная групп а автоморфизмов $\mathscr{B}(\mathscr{H})$

$$\alpha_t[X] = S^{it} X S^{-it}; \quad X \in \mathscr{B}(\mathscr{H}), \quad t \in \mathbf{R}.$$

Условное ожидание $\mathscr{E}$ на подалгебру $\mathscr{A} \subset \mathscr{P}(\mathscr{H})$, согласованное с состоянием S, существует тогда и только тогда, когда $\mathscr{A}$ инвариантна относительно α_t. В частности, это выполняется, если $[S, X] = 0$ для всех $X \in (?)$

Пример нормального условного ожидания (усреднение по подсистеме составной системы) был дан в п. 1.3.1. Приведем другой важный пример. Пусть $\{E_n\}$ - ортогональное разложение единицы в $\mathscr{H}$. Тогда

$$\mathscr{E}[X] = \sum_{n=1}^{\infty} E_n X E_n$$

является нормальным условным ожиданием на подалгебру $\mathfrak{A}$ операторов вида (1.5), согласованным с любым состоянием, оператор плотности которого принадлежит $\mathscr{A}$. Алгебру $\mathfrak{A}$ можно описать также соотношением $\mathscr{V} = \{E_n; n = 1, 2, \ldots\}'$, где $\mathfrak{M}'$ обозначает ко м м у т а н т подмножества $\mathfrak{R} \subset \mathfrak{F}(\mathscr{H})$, т. е. совокупность всех ограниченных операторов, коммутирующих с операторами из $\mathfrak{M}$.

Обзор результатов об условных ожиданиях в алгебрах фон Неймана имеется в статьях Чеккини в сб. [141] и Петца в сб. [143]. В них же излагается некоторое обобщение понятия условного ожидания, принадлежащее Аккарди и Чеккини.

12.3.2 2. Quantum Dynamical Semigroups

2.1. Определение и примеры.

Динамнческая полугруппа является некоммутативным обобщением полугруппы переходных - операторов в теории марковских случайных процессов. Возможны два эквивалентных способа задания динамической полу. группы-в пространстве состояний и в алгебре наблюдаемых системы. Квантовой дижамической полугруппой в пространстве состояний называется семейство динамических отображений $\{\Psi_t; t \in \mathrm{R}_+\}$банахова пространства ядерных операторов $\mathfrak{T}(\mathscr{H})$, такое что

1. $\Psi_t \cdot \Psi_s = \Psi_{t+s}; t, s \in \mathbf{R}_+$;
2. $\Psi_0 = \mathrm{Id}$ (тождественное отображение);
3. $\{\Psi_t\}$ сильно непрерывна, т. е. $\lim_{t\to 0} \|\Psi_t[T] - T\|_1 = 0$ для ліобого $T \in \mathfrak{E}(\mathscr{H})$.

Из общей теории полугрупп в банаховом пространстве (см., например, [9, гл. 3]) вытекает, что существует плотно определенный инфинитезимальный оператор

$$\mathscr{K}[T] = \lim_{t\to 0} \frac{\Psi_t[T] - T}{t}$$

Если Ψ_t непрерывна по норже, т. е. $\lim_{t\to 0} \|\Psi_t - \mathrm{Id}\| = 0$, то $\mathscr{K}$ - всюду определенное, ограниченное отображение $\mathfrak{T}(\mathscr{H})$. Если S_0 начальное состояние, то функция $S_t = \Psi_t[S_0]$ удовлетворяет квантовому марковскому управляющему уравнению [1)]

$$\frac{dS_t}{dt} = \mathscr{K}[S_t]$$

которое является некоммутативным аналогом уравнения Колмогорова-Чепмена. В физических приложениях динамические полугруппы и возникают как решения марковских управляющих уравнений.

Динамическая полугруппа в алгебре наблюдаемых - это полугруппа динамических отображений $\{\Phi_t; t \in \mathbf{R}_+\}$алгебры $\mathfrak{B}(\mathscr{H})$,

такая что $\Phi_0 = \mathrm{Id}$ и $w^* - \lim_{t\to 0} \Phi_t[X] = X$ для любого $X \in \mathfrak{B}(\mathscr{H})$.

1. Английский термин - master equation.

Мы будем в основном рассматривать полугруппы, непрерывные по норме, т. е. такие, что $\lim_{t\to 0} \|\Phi_t - \mathrm{Id}\| = 0$.

П р и ме р ([116]). Пусть $^{t\to 0}G$ - сепарабельная локально компактная группа, $g \to V_g$ - непрерывное унитарное представление G в $\mathscr{G}$ и $\{\mu_t; t \in \mathbf{R}_+\}$ −непрерывная сверточная полугруппа вероятностных мер на G (см., например, [13]). Соотношения

$$\Psi_t[S] = \int\limits_G V_g S V_g^* \mu_t(dg); \Phi_t[X] = \int\limits_G V_g^* X V_g \mu_t(dg)$$

задают квантовые динамические полугруппы, соответственно, в $\mathfrak{E}(\mathscr{H})$ и в $\mathfrak{B}(\mathscr{H})$.

В частности, пусть A-эрмитов оператор в $\mathscr{H}$, тогда выражение

$$\Psi_t[S] = \frac{1}{\sqrt{2\pi t}} \int\limits_{-\infty}^{\infty} e^{-\frac{x^2}{2t}} e^{-iAx} S e^{iAx}$$

соответствующее гауссовской сверточной полугруппе на $\mathbf{R}$, определяет динамическую полугруппу с инфинитезимальным оператором

$$\mathscr{K}[S] = ASA - A^2 \circ S.$$

Если U-унитарный оператор, $\lambda > 0$, то

$$\Psi_t[S] = \sum_{n=0}^{\infty} \frac{(\lambda t)^n}{n!} e^{-\lambda t} U^n S U^{*n}$$

является динамической полугруппой, отвечающей пуассоновской сверточной полугруппе на $\mathbf{Z}$, с инфинитезимальным оператором

$$\mathscr{K}[S] = \lambda [USU^* - S]$$

Понятие динамической полугруппы было предложено Коссаковским [116] (см. также Дэвис [78]), однако без условия полной положительности, которое позднее было введено Линдбладом [123]. Многие физические примеры укладываются в общую схему квазисвободных динамических полугрупп, которые являются квантовым аналогом гауссовских марковских полугрупп. В случае ККС такие полугруппы характеризуются условием, что они переводят гауссовские состояния в гауссовские (см. п. 1.2.4). В статистической механике они описывают необратимую динамику открытых Бозе- или Ферми-систем с квадратичным взаимодействием (см. обзоры [27], [56]).

2.2. Инфинитезимальный оператор.

Требование полной положительности налагает нетривиальные ограничения на инфинитезимальный оператор полугруппы. Описание инфинитезимального оператора непрерывной по норме квантовой динамической полугруппы было получено Линдбладом и, независимо в случае $\dim \mathscr{C} < \infty$, Горини, Коссаковским и Сударшаном.

Т еорема ([123]). Для того чтобы ограниченное отображение $\mathscr{K}$ пространства $\mathfrak{T}(\mathscr{H})$ было инфинитезимальным оператором непрерывной по норме квантовой динамической полугруппы, необходимо и достаточно, чтобы

$$\mathscr{K}[S] = -i[H, S] + \sum_{j=1}^{\infty} \left(L_j S L_j^* - L_j^* L_j \circ S \right)$$

где $H, L_j \in \mathfrak{B}(\mathscr{H}), H = H^*$ и ряд $\sum\limits_{j=1}^{\infty} L_j^* L_j$ сходится сильно.

Первое слагаемое в (2.4) отвечает обратимой эволюции с гамильтонианом H, а второе задает диссипативные члены. Оператор $\sum\limits_{j=1}^{\infty} L_j^* L_j$ связан со скоростью диссипации. Переходя к формулировке в алгебре наблюдаемых, имеем для инфинитезимального оператора $\mathscr{L} = \mathscr{K}^*$ полугруппы $\Phi_t = \Psi_t^*$

$$\mathscr{L}[X] = i[H, X] + \sum_{j=1}^{\infty} \left(L_j^* \dot{\Lambda} L_j - L_j^* L_j \circ X \right)$$

В основе доказательства теоремы лежат следующие два факта [123], [84].

Предложени е. Пусть $\mathscr{L}$ - ограниченное отображение $\mathfrak{B}(\mathscr{H})$ в себя, такое что $\mathscr{L}[\mathrm{I}] = 0$. Следующие утверждения эквивалентны:

1. $\exp t\mathscr{L}$ вполне положительно для всех $t \in \mathbf{R}_+$;

2. $\mathscr{L}$ вполне диссипативно, т. е. $\mathscr{L}[X^*] = \mathscr{L}[X]^*$ и

$$\sum_{j,k} \left\langle \psi_j \mid \left(\mathscr{L}\left[X_j^* X_k\right] - X_j^{**} \mathscr{L}[X_k] - \mathscr{L}[X_j]^* X_k \right) \psi_k \right\rangle \geqslant 0$$

для любых конечных наборов $\{\psi_j\} \subset \mathscr{H}, \{X_j\} \subset \mathscr{B}(\mathscr{H})$;

3. $\mathscr{L}[X^*] = \mathscr{L}[X]^*$ и $\mathscr{L}$ условно вполне положительно т. е. из $\sum\limits_j X_j \psi_j = 0$ следует

$$\sum_{j,k} \left\langle \psi_j | \mathscr{L}\left[X_j^* \ddot{X}_k\right] \psi_k \right\rangle \geqslant 0$$

Это утверждение родственно теореме Шенберга в теории условно положительно определенных функций (см., например, [138], а также п. 4.2.4).

Те орем а. Пусть $\mathscr{L}$ - ограниченное отображение $\mathscr{B}(\mathscr{H})$ в себя, такое что $\mathscr{L}[\mathrm{I}] = 0$. Для того чтобы $\mathscr{L}$ было вполне диссипативным, необходимо и достаточно, чтобы

$$\mathscr{L}[X] = \Phi[X] + K^* X + XK$$

где Ф-вполне положительное отображение, $\mathscr{Y}(\mathscr{H})$.

Соотношение (2.5) получается тогда из формулы (1.3) для нормального вполне положительного отображения.

Доказательство формулы (2.6) может быть связано с когомологиями алгебры $\mathscr{B}(\mathscr{H})$. Конструкция типа ГНС сопоставляет вполне диссипативному отображению $\mathscr{L}$ линейное отображение B алгебры $\mathscr{B}(\mathscr{G})$ в пространство ограниченных операторов из $\mathscr{H}$ в $\mathscr{K}$ (другое гильбертово пространство), так что

$$\mathscr{L}[X^*Y] - X^*\mathscr{L}[Y] - \mathscr{L}[X]^*Y = B[X]^*B[Y]$$

Более того, отображение B оказывается к о и к лом некоторого представления (*-гомоморфизма) π алгебры $\mathscr{B}(\mathscr{H})$ в $\mathfrak{B}(\mathscr{K})$, т. е. удовлетворяет уравнению

$$B[XY] = \pi[X]B[Y] + B[X]Y; X, Y \in \mathscr{B}(\mathscr{H}).$$

Основную трудность представляет доказательство того, что всякий коцикл тривиален, т. е. имеет вид $B[X] = \pi[X]R - RX$, где R-ограниченный оператор из $\mathscr{H}$ в $\mathscr{K}$. Кристенсен и Эванс [76] обобщили этот подход и получили аналог представления (2.6) для произвольной C^*-алгебры операторов.

2.3. Свойство консервативности.

Проблема характеризации инфинитезимального оператора динамической полугруппы без требования непрерывности по норме трудна и остается открытой. Нетривиальной является и задача построения динамической полугруппы по формальному выражению типа (2.5), где H, L_j - неограниченные операторы. Дэвис [79] указал довольно общие условия, при которых с формальным выражением (2.4) ассоциируется сильно непрерывная полугруппа вполне положительных отображений $\{\Phi_t; t \in \mathbf{R}_+\}$, такая что

$$\Phi_t[\mathrm{I}] \leqslant \mathrm{I}$$

и являюшаяся аналогом феллеровского минимального решения в классической теории марковских процессов. Если минимальная полугруппа консервативна в том смысле, что $\Phi_t[\mathrm{I}] = \mathrm{I}$, то она является единственной динамической полугруппой, инфинитезимальный оператор которой является замыканием оператора (2.5). Неконсервативность, как и в классической теории, связана с возможностью «ухода на бесконечность» за конечное время.

Прим е р 1 ([79]). Пусть $\mathscr{H} = l^2$ - гильбертово пространство последовательностей $\{\psi_n; n \geqslant 0\}$ и «операторы рожденияуничтожения» a^*, a определены соотношениями $(a^*\psi)_n = \sqrt{n}\psi_{n-1}, \quad (a\psi)_n = \sqrt{n+1}\psi_{n+1}$. Рассмотрим управляющее уравнение

$$\frac{dS_t}{dt} = LS_tL^* - L^*L_0S_t$$

где $L = a^{*2}, L^* = a^2$, а S_t - диагональный оператор плотности в l^2. Диагональные элементы $p_n(t); n = 0, 1, \ldots$, оператора S_t удовлетворяют уравнению чистого рождения

$$\frac{dp_n(t)}{dt} = -(n+2)(n+1)p_n(t) \pm n(n-1)p_{n-2}(t)$$

минимальное решение которого неконсервативно, $\sum\limits_{n=0}^{\infty} p_n(t) < 1$ при $t > 0$.

Дэвис дал достаточные условия консервативности, пригодные для класса моделей квантовой диффузии. Оригинальные общие условия консервативности, основанные на аналогиях с классической теорией марковских процессов, предложил А. М. Чеботарев в [49], [35]. Рассмотрим для простоты случай формального инфинитезимального оператора

$$\mathscr{L}[X] = L^*XL + K^*X + XK$$

где L, L^*, K, K^* - операторы, имеющие плотную общую инвариантную, область определения $\mathscr{D}$. Предполагается, что $\mathscr{D}$ - существенная область определения для операторов K, K^*, которые являются инфинитезимальными операторами сильно непрерывных сжимающих полугрупп в $\mathscr{H}$, и что $K = -\frac{1}{2}L^*L + iH$, где H - самосопряженный оператор. Условия консерва- тивности имеют вид

$$[L, L^*] \geqslant -cI, i\,[L^*L, H] \geqslant -cL^*L,$$

где $c > 0$ и неравенства понимаются как неравенства для соответствующих форм, определенных на $\mathscr{D}$. Представление о диапазоне применимости этих условий дают два примера.

Пример 2. Пусть $\mathscr{H} = L^2(\mathbf{R}), Q$-оператор умножения на $x; P = i^{-1}\frac{d}{dx}$, $a(x)$ - дважды непрерывно дифференцируемая функция. Рассмотрим формальное выражение

$$\mathscr{L}[\tilde{X}] = Pa(Q)Xa(Q)P - Pa(Q)^2P \circ X$$

Если X-оператор уможения на дважды непрерывно дифференцируемую функцию $f(x)$, то $\mathscr{L}[X]$ есть оператор умно жения на $\frac{1}{2}\frac{d}{dx}\left(a(x)^2\frac{df}{dx}\right)$, т. е. совпадает с инфинитезимальным оператором симметричной диффузии на коммутативной подалгебре $L^\infty(\mathbf{R}) \subset \mathfrak{B}\,(L^2(\mathbf{R}))$.

Условия А. М. Чеботарева выполняются, если $\sup_x a(x)a''(x) < \infty$.

П риме р 3. В обозначениях предыдущего примера рассмотрим выражение

$$\mathscr{L}[X] = \int_{-\infty}^{\infty} m(d\xi)c(Q,\xi)^*V_\xi^*X^*V_\xi c(Q,\xi) -$$

$$- \int_{-\infty}^{\infty} m(d\xi)|c(Q,\xi)|^{2\circ}\tilde{K},$$

где $V_x = \exp(-ixP), m$ - вероятностная мера на $\mathbf{R}, c$-комплексная измеримая функция, такая что $x(x) \equiv \int m(d\xi)|c(x,\ \xi)\,|^2 < \infty$ для всех x. На коммутативной подалгебре $L^\infty(\mathbf{R})(2.8)$ совпадает с инфинитезимальным оператором скачкообразного марковского процесса в R с интенсивностью скачков $x(x)$. Достаточные условия консервативности выполняются, если

$$\sup_x \int m(x|d\xi)\,[\varkappa_1(x+\xi) - \varkappa_i(x)] < \infty,$$

где $m(x|d\xi) = m(d\xi)|c(x,\xi)|^2/x(x)$ - условные вероятности скачков.

Полученные в [49] условия консервативности позволяют рас. смотреть также суммы выражений типа (2.7), (2.8) и гамильтоновых членов вида $i[H, X]$ с неограниченным H.

2.4. Ковариантные эволюции.

Пусть $g \to V_g$ - представление в $\mathscr{C}$ группы G, описывающей симметрии окружения открытой квантовой системы. Динамическая полугруппа $\{\Psi_t; t \in \mathbb{R}_+\}$называется ковариантной, если

$$\Psi_t\left[V_gSV_g^*\right] = V_g\Psi_t[S]V_g^*$$

для всех $S \in \mathcal{S}(\mathscr{G}), g \in G, t \in \mathbb{R}_+$. Структура ковариантных вполне положительных отображений рассмотрена в [149]. В конечномерном случае получена достаточно полная

классификация инфинитезимальных операторов динамических полугрупп, ковариантных относительно групп простр анственных симметрий [93], [1].

П р и м е р. Рассмотрим эволюцию (2.1) открытой системы со спином $1/2(\dim \mathscr{H} = 2$; см. п. 1.1.6), ковариантную относительно действия группы SO(2), соответствующей аксиально симметричному окружению. Представление имеет вид $\varphi \to e^{iq\sigma_3}$, где $\varphi \in [0, 2\pi)$. Общий вид инфинитезимального оператора ковариантной динамической полугруппы

$$\mathscr{L}[S] = -i[H, S] + \sum_{j=-1}^{1} c_j \left(L_j S L_j^* - L_j^* L_j \mathrm{O} S \right)$$

где $c_j \geqslant 0, \quad H = \frac{1}{2}\omega_0\sigma_3, L_{-1} = \frac{1}{\sqrt{2}}(\sigma_1 - i\sigma_2), \quad L_0 = \sigma_3, \quad L_1 = \frac{1}{\sqrt{2}}(\sigma_1 + i\sigma_2)$. Полагая $S_t = S(\mathrm{a}_t)$, для вектора a_t имеем. уравнение Блоха

$$\frac{d\mathrm{a}_t}{dt} = \begin{bmatrix} -T_\perp^{-1} & \omega_0 & 0 \\ -\omega_0 & -T_\perp^{-1} & 0 \\ 0 & 0 & T_\parallel^{-1} \end{bmatrix} \mathrm{a}_{t.} + \begin{bmatrix} 0 \\ 0 \\ c_\infty/T_\parallel \end{bmatrix}$$

где $T_\perp^{-1} = 2c_0 + (c_1 + c_{-1}), T_\parallel^{-1} = 2(c_1 + c_{-1}), \quad c_\infty = 2T_\parallel (c_1 - c_{-1})$. Уравнение (2.10) описывает релаксацию спина в аксиальносимметричном магнитном поле. Параметр $T_\parallel (T_\perp)$ имеет смысл времени продольной (поперечной) релаксации. При $t \to +\infty$ $\mathbf{a}_t \to \begin{bmatrix} 0 \\ 0 \\ c_\infty \end{bmatrix}$, так что S_t стремится к предельному состоянию

$$S_\infty = \frac{1}{2}(\mathrm{I} + c_\infty \sigma_3)$$

Инфинитезимальный оператор (2.9) вполне диссипативен, что налагает нетривиальные ограничения на физические параметры эволюции. Именно, $2T_\perp^{-1} - T_\parallel^{-1} = 2c_0 \geqslant 0$, откуда $2T_\parallel \geqslant \geqslant T_\perp$[93].

$\bar{B}$ серии работ, обзор которых имеется в [83], описаны инфинитезимальные операторы инвариантных динамических полугрупп (не обязательно непрерывных по норме), действующих тождественно на алгебре инвариантных элементов.

2.5. Эргодические свойства.

Если Ф-динамическое отображение, то семейство $\left\{\Phi^k; k = 0, 1, \ldots\right\}$ можно рассматривать как динамическую полугруппу с дискретным временем. Асимптотические свойства таких полугрупп при $k \to \infty$ являются нетривиальным обобщением эргодической теории для классических цепей Маркова. Свойство полной положительности используется при этом лишь постольку, поскольку оно влечет неравенство Кэдисона-Шварца (1.2), а эргодические теоремы для средних верны для положительных отображений.

В большинстве работ в той или иной форме присутствует предположение, что Ф имеет точное нормальное инвариантное состояние, т. е. состояние с невырожденным оператором плотности S_∞, такое, что $\mathrm{Tr}\, S_\infty \Phi[X] = \mathrm{Tr}\, S_\infty X$ для всех $X \in \mathscr{F}(\mathscr{H})$. Имеет место эргодическая теорема для средних

$$w^* - \lim_{k\to\infty} \frac{1}{k} \sum_{j=0}^{k} \Phi^k[\bar{X}] = \mathscr{E}_\infty[X]$$

где $\mathscr{E}_\infty$ - условное ожидание на подалгебру $\mathscr{N}_\infty$ инвариантных элементов Ф. В разной степени общности этот результат был получен Я. Г. Синаем, Е. А. Морозовой и Н. Н.

Ченцовым, Кюммерером и другими авторами (см. обзор [27]). Соотношение (2.11) можно рассматривать как обобщение закона больших чисел. Много внимания было уделено распространению теорем типа (2.11) на неограниченные операторы и изучению некомму- тативноо. аналога сходймости почти наверное в алгебрах фон Неймана. Подробный обзор этих результатов дан В. В. Аншелевичем и M. Ш. Гольдштейном в [34], Петцем в [141], Яйте [111]. Отображение Φ неприводимо (Дэвис, Эванс), если не существует проектора $P \neq 0$, I, такого что $\Phi[P] = P$. Последнее равенство равносильно тому, что подалгебра операторов внда $PXP; P \in \mathscr{B}(\mathscr{H})$ инвариантна относительно Φ. Неприводимость эквивалентна адинственности инвариантного состоянйя S_∞ и одномерности подалгебры $\varkappa_\infty$. При этом в формуле (2.11)$\mathscr{E}_\infty[X] = (\operatorname{Tr} S_\infty X) \cdot \mathrm{I}$. Для неприводимости отображения Φ, записанного в виде (1.4), необходимо и достаточно, чтобы $\{V_n; n = 1, 2, \ldots \ldots\}'' = \mathfrak{B}(\mathscr{H})$, где $\mathfrak{A}'' = (\mathfrak{A}')'$. Для неприводимого отображения имеет место аналог теоремы Перрона-Фробениуса, отвечающй разложению замкнутого класса состояний цепи Маркова на подклассы (Эванс, Хег-Крон, Альбеверио; см. обзор [27]). Случай $\dim \mathscr{H} < \infty$ детально рассмотрен также в книге Т. А. Сарымсакова [31].

Пусть теперь $\{\Phi_t; t \in \mathbf{R}_+\}$-квантовая динамическая полугруппа, имеющая точное нормальное инвариантное состояние S_∞. Для нее также имеет место эргодическая теорема для средних (см. обзоры [27], [94]). Неприводимые полугруппы изучалн Дэвис, Эванс, Шпон, Фриджерио (см. [78], [152]). Необходимое и достаточное условие неприводимости динамической полугруппы с инфинитезимальным оператором (2.5) состоит в том, что

$$\left\{H, L_j, L_j^*; j = 1, 2, \ldots\right\}' = \mathfrak{B}(\mathscr{H})$$

Для неприводимых квантовых динамических полугрупп с непрерывным временем имеет место существенное усиление эргодической теоремы (см. [94])

$$w^* - \lim_{t \to +\infty} \Phi_t[X] = (\operatorname{Tr} S_\infty X) \cdot \mathrm{I}$$

Этот факт не переносится на динамические полугруппы в произвольных алгебрах фон Неймана. Обобщения на этот случай других асимптотических свойств, спектральной теории и теоремы Перрона-Фробениуса подробно рассмотрены в обзоре Гроха [94].

Основные физические примеры эргодических динамических полугрупп относятся к классу квазисвободных полугрупп, для которых эргодичность устанавливается непосредственно (см. обзор [27]).

2.6. Расширения динамических полугрупп.

С точки зрения статистической механики закономерен вопрос- насколько по-

нятие динамической полугруппы согласуется с более фундамен-

тальным законом обратимой эволюции для изолированной системы. В физических приложениях управляющее уравнение (2.1) получается при рассмотрении взаимодействия квантовой системы с окружением в марковском приближении (пределы слабого или сингулярного взаимодействия). Строгое обоснова- ние такого приближения требует достаточно громоздких оценок даже для простых моделей. Имеется ряд обзоров [152], [56], [93], [27], [52], в которых эта проблема квантовой статистической механики получила всестороннее освещение, и лучшее, что здесь. можно предложить - это обратиться к одному из этих обзоров.

В принципиальном плане представляет интерес также постановка обратной задачи о расширении динамической полугруппы до группы автоморфизмов, т. е. представление марковской динамики через обратимую динамику открытой системы,

взанмодействующей с окружением. Возможность такого расширения обусловлена, главным образом, свойством полной положительности (Дэвис; Эванс, Льюис; см. [84]).

Т е о р е м а. Пусть $\{\Psi_t; t \in \mathbf{R}_+\}$- непрерывная по норме динамическая полугруппа в пространстве состояний $\mathfrak{S}(\mathscr{H})$. Найдутся гильбертово пространство $\mathscr{H}_0$, состояние S_0 в $\mathscr{H}_0$ и сильно непрерывная группа унитарных операторов $\{U_t; t \in \mathbf{R}\}$ в $\mathscr{H} \otimes \mathscr{H}_0$. такие что

для всех $t \in \mathbf{R}_+$.

$$\Psi_t[S] = \operatorname{Tr}_{\mathscr{H}_0} U_t (S \otimes S_0) U_t^*; S \in S(\mathscr{H})$$

В п. 5.2.2 будет приведена явная конструкция расширения, допускающая прозрачное динамико-статистическое истолкование. Следует отметить, что одна и та же динамическая полугруппа может иметь много неэквивалентных расширений (даже если требовать минимальность расширения). Дополнительный свет на структуру возможных расширений проливает понятие квантового случайного процесса. Согласно определению Аккарди, Фриджерио и Льюиса (1980), квантовый случайный процесс задается тройкой $(\mathrm{Re}, (j_t), \varphi)$, где $\mathfrak{A}$ – C^*-алгебра, $(j_t)_{t\in\mathbf{R}}$ - семейство *-гомоморфизмов некоторой фиксированной C^*-алгебры в в $\mathfrak{A}, \varphi$ - состояние на $\mathfrak{A}$. При определенных условиях регулярности квантовый случайный процесс однозначно с точностью до эквивалентности восстанавливается по корреляционным ядрам

$$w_1^t, \ldots, t_n (X_1, \ldots, X_n; Y_1, \ldots, Y_n) =$$
$$= \varphi \left(j_{t_1} (X_1)^* \ldots j_{t_n} (X_n)^* j_{t_n} (Y_n) \ldots j_{t_1} (Y_1)_) \right)$$

(некоммутативный аналог теоремы А. Н. Колмогорова о продолжении системы конечномерных распределений) (см. сборник [20]). В классическом случае $\mathscr{A}$ и $\mathfrak{B}$ коммутатнвные алгебры измеримых ограниченных функций, соответственно, на пространстве элементарных исходов Ω и на фазовом пространстве системы $E, (j_t)$ определяется семейством случайных величин на Ω со значениями в E, а φ - функционал математического ожидания, соответствующий вероятностной мере на Ω.

С квантовым случайным процессом связываются семейства подалгебр «прошлого», «настоящего» н «будущего»

$$\mathfrak{A}_{t]} = \bigvee_{s\leqslant t} j_s(\mathfrak{B}), \quad \mathfrak{A}_t = j_t(\mathfrak{B}), \quad \mathfrak{A}_{[t} = \bigvee_{s\geqslant t} j_s(\mathfrak{B})$$

Процесс называется жарковскик, если существует согласованное с φ семейство условных ожиданий $(\mathscr{E}_{t]})_{t\in\mathbf{R}}$ из $\mathfrak{A}$ на $\mathfrak{A}_{t]}$, такое что

$$\mathscr{E}_{t]} \left(\mathfrak{A}_{[t} \right) \subseteq \mathscr{A}_t$$

ковариантным марковския, если дополнительно существует группа *-автоморфизмо в $(\alpha_t)_{t\in R}$ алгебры $\mathscr{A}$, такая что $\alpha_t \left(\mathrm{Re}_{s]} \right) = \mathfrak{R}_{t+s]}; t, s \in \mathbb{R}$, и $\alpha_t \cdot \mathscr{E}_{s]} \cdot \alpha_{-t} = \mathscr{E}_{t+s]}$, и стационарныцм марковским, если φ инвариантно относительно (α_t). Для ковариантного марковского процесса соотношение

$$\Phi_t[X] = j_t^{-1} \mathscr{E}_{t]} \dot{j}_t[X]$$

при выполнении некоторых условнй непрерывности определяет динамическую полугруппу в Я. Обратно, всякая непрерывная по норме квантовая динамическая полугруппа $\{\Phi_t\}$ расширяется до. ковариантного марковского процесса, удовлетворяющего соотношению (2.12). Если же динамическая полугруппа

удовлетворяет условню детального равновесия, то она расширяется до стационарного марковского квантового случайного процесса (Горини, Фриджерио). Условие детального равновесия относи· тельно состояния S для полугруппы $\{\Phi_t\}$ в $\mathscr{B}(\mathscr{Z})$ означает, что существует другая динамическая полугруппа $\left\{\Phi_t^+\right\}$в $\mathscr{B}(\mathscr{H})$, такая что

$$\operatorname{Tr} S\Phi_t + [X]Y = \operatorname{Tr} SX\Phi_t[Y]; \quad X, Y \in \mathscr{B}(\mathscr{H})$$

с инфинитезимальным оператором $\mathscr{L}^+$, удовлетворяющим соотношению

$$\mathscr{L}[X] - \mathscr{L} + [X] = 2i[H, X]$$

где $H \in \mathscr{P}_h(\mathscr{H})$ (состояние S с необходимостью оказывается стационарным для Φ_t и Φ_t^+). До сих пор отсутствует полное описание динамических полугрупп, допускающих стационарные марковские расширения.

Фриджерио и Маассен [87] указали широкий класс полугрупп, не удовлетворяющих условию детального равновесия, но допускающих расширение с помощью «квантового пуассоновского процесса». Систематическое исследование стационарных марковских расширений предпринял Кюммерер [119]. Он установил прямую связь между эргодическими свойствами динамического отображения (неприводимость, слабое, сильное перемешивание) и его минимального стационарного марковского расширения. Кюммерер и Маассен [120] показали, что квантовая динамическая полугруппа в конечномерном гильбертовом пространстве допускает стационарное марковское расширение с помощью классического случайного процесса тогда и только тогда, когда ее

. инфинитезимальный оператор имеет вид

$$\mathscr{L}[\mathrm{X}] = i[H, X] + \sum_{s=1}^{k} \left(A_s X A_s - A_s^2 \circ X\right) + \\ + \sum_{r=1}^{l} \lambda_r \left(U_r^* X U_r - X\right)$$

тде A_s - эрмитовы, U_r - унитарные операторы, $\lambda_r > 0$. Оператор (2.13) является суммой выражений $(2.2), (2.3)$, соответствующих гауссовским и пуассоновским полугруппам, а расширение получается с помощью случайного блуждания на группе автоморфизмов алгебры $\mathfrak{M}_n$.

Неоднозначность расширения динамической полугруппы до случайного процесса связана с тем, что знание полугруппы $\{\Phi_t\}$ позволяет восстановить лишь хронологически-упорядоченные корреляционные ядра

$$w_{t_1,\ldots,t_n}(X_1, \ldots, X_n; Y_1, \ldots, Y_n) = \\ = \varphi_0\left(\Phi_{t_1}\left[X_1^* \Phi_{t_2 - t_1}\left[\ldots \Phi_{t_n - t_{n-1}}\left[X_n^* Y_n\right]\ldots\right] Y_1\right]\right),$$

-для которых $0 < t_1 < \ldots < t_n$ (здесь $\varphi_0 = \varphi|\mathscr{A}_0$ - начальное состояние). В классической теории вероятностей корреляционные ядра зависят от времен $t_1, \ldots, t_n$ симметричным образом; известная конструкция Колмогорова-Даниэля однозначно сопоставляет полугруппе переходных вероятностей марковский процесс, являющийся ее минимальным расширением до группы временных сдвигов в пространстве траекторий. Определение квантового случайного процесса, основанное только на хронологически-упорядоченных ядрах, было предложено Линдбладом [124], некоммутативные обобщения конструкции КолмогороваДаниэля рассматривались Винсент-Смитом [161], В. П. Белавкиным [3], Соважо [146].

Алицки и Мессер установили существование и единственность решения класса н елине й ных кинетических уравнений, в частности, квантового уравнения Больцмана:

$$\frac{dSt}{dt} = \mathrm{Tr}_{(2)}\, W\,(S_t \otimes S_t)\, W^* - (\mathrm{Tr}\, S_t)\cdot S_t$$

где W - унитарный «оператор парных столкновений» в $\mathscr{C}\otimes\mathscr{H}$, $\mathrm{Tr}_{(2)}$ - частичный след по второму множителю в $\mathscr{H}\otimes\mathscr{H}$. Отвечая на вопрос, поставленный Стритером в [143], Фриджерио и - Аратари построили расширение «нелинейной квантовой динами'ческой полугруппы», определенной уравнением (2.14) по уни"тарной эволюции в квантовой системе, состоящей из бесконечно'го числа частиц с парными взаимодействиями (квантовое обобщение «карикатуры Мак-Кина» классического уравнения Боль- цмана). В. П. Белавкин [4] дал конструкцию квантового ветвящегося процесса, в котором одночастичная динамика описывается полугруппой нелинейных вполне положительных отображений общего вида.

12.4 Consistent and Continuous Measurement Processes

12.4.1 1. Statistics of Successive Measurements

1.1. Понятие инструмента.

Рассмотрим последовательное измерение двух величин X, Y, принимающих значения, соответственно, в множествах $\mathscr{X}$ и $\mathscr{Y}$, которое осуществляется над системой в состоянии S. Совместная вероятность того, что исход первого измерения x попадает в множество A, а исход второго y попадает в B (где $A\subset\mathscr{X}, B\subset\mathscr{Y}$) есть

$$\mu_s(A;B) = \mu_s(A)\mu_s(B|A)$$

где $\mu_{\mathcal{S}}(A) = \mu_{\mathcal{B}}(A;\dagger)$ - вероятность того, что $x\in A$, а $\mu_{\mathcal{S}}(B|A)$ - соответствуюшая условная вероятность. Обозначим S_A состояние системы после первого измерения (оно зависит также от S, но не зависит от B). Тогда, согласно (2.1.4),

$$\mu_S(B|A) = \mathrm{Tr}\, S_A M(B)$$

где $\boldsymbol{M}$ - разложение единицы, отвечающее величине Y. Из (1.1), (1.2) видно, что функция множеств

$$\mathscr{M}(A)[S] = \mu_S(A)S_A$$

должна быть σ-аддитивна по A. Это мотивирует следующее определение (Дэвис и Льюис, 1970).

Пусть $\mathscr{X}$ - множество с σ-алгеброй измеримых подмножеств $\mathscr{B}(\mathscr{Q})$. Инструментом (в пространстве состояний) со значениями в $\mathscr{X}$ называется функция множеств $\mathscr{M}$, заданная на $\mathscr{B}(\mathscr{L})$ и удовлетворяющая условиям:

1. $\mathscr{M}(B)$ - операция для любого $B\in\mathscr{B}(\mathscr{X})$;
2. $\mathscr{M}(\mathscr{X})$ - динамическое отображение, т. е. $\mathrm{Tr}\,\mathscr{M}(\mathscr{X})[T] = \mathrm{Tr}\, T$ для всех $T\in\mathfrak{T}(\mathscr{C})$;
3. если $\{B_j\}\subset\mathscr{B}(\mathscr{X})$ - конечное или счетное разбиение множества $B\in\mathscr{B}(\mathscr{C})$ на попарно непересекающиеся подмножест-; ва, то

$$\mathscr{M}(B)[T] = \sum_j \mathscr{M}(B_j)[T]; T \in \mathfrak{T}(\mathscr{H})$$

где ряд сходится по норме $\mathfrak{T}(\mathscr{H})$.

Постулируется, что если S - оператор плотности, описываю: щий состояние системы перед измерением, то вероятность собы: тия, что исход измерения попадает в множество $B \in \mathscr{B}(\mathscr{X})$, равна

$$\mu_{\boldsymbol{s}}(B) = \operatorname{Tr} \mathscr{A}(B)[S]$$

а состояние доли статистического ансамбля, в которой зарегистрировано это событие, дается оператором плотности

$$S_B = \mathscr{M}(B)[S] / \operatorname{Tr} \mathscr{M}(B)[S]$$

(при условии, что $\mu_8(B) > 0$). В частности, изменение состояния всего статистического ансамбля задается динамическим отображением $S \to \mathscr{M}(\mathscr{X})[S]$.

Переходя к сопряженным отображениям $\mathscr{P}(B) = \mathscr{M}(B)^*$, получаем формулировку в алгебре наблюдаемых: инструмент это функция множеств $\mathscr{P}$ на $\mathscr{B}(\mathscr{D})$, такая что

1. $\mathscr{P}(B)$ - положительное нормальное отображение $\mathscr{B}(\mathscr{H})$ в себя для любого $B \in \mathscr{B}(\mathscr{Q})$;
2. $\mathscr{P}(\mathscr{X})[\mathrm{I}] = \mathrm{I}$;
3. если $\{B_i\} \subset \mathscr{B}(\mathscr{X})$ - разбиение множества B, то

$$\mathscr{P}(B)[X] = \sum_j \mathcal{P}(B_j)[X]; X \in \mathscr{B}(\mathscr{H})$$

где ряд сходится *-слабо.

Каждому инструменту отвечает обобщенная наблюдаемая

$$M(B) = \mathscr{P}(B)[\mathrm{I}]; \quad B \in \mathscr{B}(\mathscr{X})$$

такая, что

$$\mu_B(B) = \operatorname{Tr} SM(B)$$

Озава [135] показал, что для любого инструмента $\mathscr{M}$ и любого состояния S существует семейство апостериорных состояний $\{S_x; x \in \mathscr{Q}\}$, т. е. операторов плотности S_x, таких что:

1. функция $x \to \operatorname{Tr} S_x Y \mu_s$-измерима для любого $Y \in \mathscr{F}(\mathscr{C})$;
2. $\operatorname{Tr} \mathscr{M}(B)[S]Y = \int\limits_B (\operatorname{Tr} S_x Y)\, \mu_s(dx)$.

Оператор плотности S_x описывает состояние доли статистического ансамбля, в которой исход измерения равен x, а величина $\operatorname{Tr} S_x Y = \mathbf{E}_s(Y|x)$ есть апостериорное среднее наблюдаемой Y при условни, что исход предыдущего измерения равен x.

Инструмент $\mathscr{M}$ (или $\mathscr{P}$) называется вполне положительным, если отображения $\mathscr{P}(B); B \in \mathscr{B}(\mathscr{X})$, вполне положительны.

П р и м е р 1. Пусть $A = \sum_i x_i E_i$ - вещественная наблюдаемая с чисто точечным спектром. Соотношение

$$\mathscr{M}(B)[S] = \sum_{i:x_i \in B} E_i S E_i$$

определяет вполне положительный инструмент со значениями в $\mathbf{R}$, соответствующий проекционному постулату фон Неймана, который описывает предельно точное измерение наблюдаемой A.

Распределение вероятностей в состоянии S есть

$$\mu_S(B) = \sum_{i:x_i \mathrm{G}^B} \operatorname{Tr} S E_i$$

а апостериорные состояния даются формулой

$$S_i = E_i S E_i / \operatorname{Tr} S E_i$$

Прим е р 2. Пусть A - вещественная наблюдаемая и $p(x)$ - плотность распределения вероятностей на $\mathbf{R}$, такая что

$$\int_{-\infty}^{\infty} x p(x) dx = 0, \quad \int_{-\infty}^{\infty} x^2 p(x) dx = \sigma^2 < \infty$$

Вполне положительный инструмент

$$\mathscr{M}(B)[S] = \int_B \sqrt{p(xI - A)} S \sqrt{p(xI - A)} dx$$

описывает неточное измерение наблюдаемой A со случайной ошибкой, распределенной с плотностью $p(x)$. В самом деле

$$\mu_S(B) = \int_B \operatorname{Tr} S p(x\mathrm{I} - A) dx =$$
$$= \int_B \int_B p(x - y) \mu_S^A(dy) dx,$$

где ${\mu_s}^A$ - распределение вероятностей наблюдаемой A в состоянии S. Апостериорные состояния суть

$$S_x = \frac{\sqrt{p(x\mathrm{I} - A)} S \sqrt{p(x\mathrm{I} - A)}}{\operatorname{Tr} S p(x\mathrm{I} - A)}$$

Чем меньше σ^2, т. е. чем ближе $p(x)$ к δ-функции, тем точнее измерение наблюдаемой A. Для наблюдаемой A с чисто точечным спектром случай $\sigma^2 = 0$ соответствует примеру 1 ; для наблюдаемой с непрерывным спектром возникают принципиальные трудности, не позволяющие непосредственно обобщить проекционный постулат на этот случай (см. далее п. 1.3).

1.2 Представление вполне положительного инструмента.

Многие реальные процессы укладываются в следующую схему косвенного измерения: рассматриваемая система взаимодействует с «пробной» системой, после чего над пробной системой производится прямое измерение некоторой квантовой наблюдаемой. Пусть $\mathscr{C}_0$ - гильбертово пространство пробной системы, S_0 - оператор плотности, описывающий ее исходное состояние, U - унитарный оператор в $\mathscr{C} \otimes \mathscr{H}_0$, задающий взаимодействие и E_0 - ортогональное разложение единицы в $\mathscr{C}_0$, соответствующее измеряемой величине. Распределение вероятностей такого измерения дается формулой

$$\mu_{\mathcal{S}}(B) = \operatorname{Tr} U\,(S \otimes S_0)\,U^*\,(\mathrm{I} \otimes E_0(B))\,;\, B \in \mathscr{B}(\mathscr{X})$$

где S - оператор плотности системы перед измерением. Оно может быть записано в виде (1.3), где

$$\mathscr{M}(B)[S] = \operatorname{Tr}_{\mathscr{C}_0} U\,(S \otimes S_0)\,U^*\,(\mathrm{I}_{\otimes} E_0(B))$$

- вполне положительный инструмент в пространстве состояний системы $\mathscr{H}$ (здесь $\operatorname{Tr}\mathscr{H}_0$ - частичный след по $\mathscr{H}0$). Верно и обратное.

Т е оре м а (Озава, [134]). Пусть $\mathscr{M}$ - вполне положительный инструмент со значениями в $\mathscr{X}$. Найдется гильбертово пространство $\mathscr{C}_0$, оператор плотности S_0 в $\mathscr{C}_0$, унитарный оператор $U_{\text{в}}\,\mathscr{C} \otimes \mathscr{C}_0$ и ортогональное разложение единицы $\mathbf{E}_0$ в $\mathscr{C}$, такие что для любого оператора плотности S в $\mathscr{H}$ имеет место формула (1.10).

В основе этой теоремы лежит следующая комбинация теоремы Наймарка и теоремы Стайнспринга: если $\mathscr{P}$ - вполне положительный инструмент (в алгебре наблюдаемых), то существует гильбертово пространство $\mathscr{K}$, изометрический оператор V из $\mathscr{H}$ в $\mathscr{K}$, ортогональное разложение единицы E в $\mathscr{K}$ и нормальный *-гомоморфизм π из $\mathscr{B}(\mathscr{H})$ в $\mathfrak{F}(\mathscr{K})$, такие что $[E(B), \pi[X]] = 0$ для всех $B \in \mathscr{B}(\mathscr{C}), X \in \mathscr{B}(\mathscr{C})$ и

$$\mathscr{P}(B)[X] = V^* E(B)\pi[X]V$$

Пространство $\mathscr{K}$ превращается в $\mathscr{H} \otimes \mathscr{H}_0$ с помощью рассуждений, которые были использованы при доказательстве формулы (3.1.4).

Из (1.11) выводится аналог представления (3.1.4) для вполне положительного инструмента

$$\mathscr{P}(B)[X] = \int\limits_B \sum_{n=1}^{\infty} V_n(x)^* X V_n(x)\mu(dx)$$

где $\mu - \sigma$-конечная мера на $\mathscr{R}$, а $V_n(x) - \mu$-измеримые функции на $\mathscr{X}$ со значениями в $\mathscr{O}(\mathscr{H})$, такие что

$$\int\limits_{\mathscr{Q}}^{\infty} \sum_{k=1}^{\infty} V_n(x)^* V_n(x)\mu(dx) = \mathrm{I}$$

Соответствующий инструмент в пространстве состояний имеет вид

$$\mathscr{K}(B)[S] = \int\limits_B \sum_{n=1}^{\infty} V_n(x) S V_n(x)^* \mu(dx)$$

При этом распределение вероятностей в состоянии S дается формулой

$$\mu_S(B) = \int\limits_B \sum_{n=1}^{\infty} \operatorname{Tr} SV_n(x)^* V_n(x) \mu(dx)$$

$$S_x = \sum_{n=1}^{\infty} V_n(x) S V_n(x)^* | \sum_{n=1}^{\infty} \operatorname{Tr} SV_n(x)^* V_n(x)$$

1.3 Три уровня описания квантовых измерений.

Теорема Озава имеет принципиальное значение, поскольку демонстрирует согласованность понятия (вполне положительного) инструмента со стандартным формализмом квантовой механики. Описание измерения в обобщенной статистической модели квантовой механики может быть осуществлено с различной степенью подробности. Имеется три основных уровня описания, каждому из которых отвечает определенный математический объект в гильбертовом пространстве системы:

1. Задана только статистика исходов измерения. Как показано в п. 2.1.2, это эквивалентно заданию обобщенной наблюдаемой, т. е. некоторого разложения единицы в $\mathscr{H}$.

2. Кроме статистики, задан закон преобразования состояний в зависимости от исхода измерения. На этом уровне адекватное описание измерения дается понятием инструмента. Каждому инструменту по формуле (1.5) отвечает обобщенная наблюдаемая, однако это соответствие не взаимно однозначно, поскольку инструмент дает более подробное описание измерения, нежели наблюдаемая.

3. Задано динамическое описание взаимодействия системы с пробной системой. Этот уровень является еще более подробным: каждому инструменту по формуле (1.10) может соответствовать. множество различных процедур косвенного измерения. Детальность схемы косвенного измерения зависит от того, где в измерительном приборе проводится черта между «пробной системой» и «детектором», осушествляющим прямое измерение.

С точки зрения физических приложений представляет большой интерес вопрос о реализуемости той или иной теоретической схемы квантового измерения. Высказывалась мысль (см., например, статью «Проблема измерения» в сборнике [11]), что хотя квантовая механика правильно отражает некоторые черты микромира, далеко не все, что содержится в ее математической модели, может иметь свой прототип в реальности. Известны обшие ограничения типа правил суперотбора (см., например, [23]), которые постулируют измеримость только наблюдаемых, совместимых с некоторой выделенной величиной типа заряда. В связи со схемой косвенного измерения возникают следующие вопросы:

1. Соответствует ли данному унитарному оператору U реальное квантовомеханическое взаимодействие?

2. Соответствует ли данной наблюдаемой A реально измеримая физнческая величина?

Подробное обсуждение таких вопросов выходит за рамки настоящего обзора, но некоторые комментарии здесь все же необходимы. В работах Ваневского [165] и Мельника [129] показано, что всякий унитарный оператор может быть получен из шрёдингеровской эволюции с некоторым потенциалом, зависящим от времени. Таким

образом, первый вопрос сводится к реализуемости потенциалов в квантовой механике. С другой стороны, в п. 1.5 будет показано, что второй вопрос сводится к первому для взаимодействий специальног) вида. Практически, конечно, эти вопросы могут быть совсем не просты и требуют отдельного рассмотрения в каждой конкретной задаче измерения (см. в этой связи поучительное обсуждение «приемника Долинара» в [37, гл. VI] и в [18]).

1.4. Воспроизводимость. Пусть S-оператор плотности, $\mathscr{M}_1, \ldots, \mathscr{M}_n$ - последовательность инструментов со значениями в измеримых пространствах $\mathscr{X}_1, \ldots, \mathscr{X}_n$. Из постулатов (1.3), (1.4) следует, что величина

$$\mu_S^{\mathscr{M}_1,\ldots,\mathscr{M}_n}(B_1 \times \ldots \times B_n) = \\ = \operatorname{Tr} \mathscr{M}_n(B_n)[\ldots \mathscr{M}_1(B_1)[S]\ldots]$$

где $B_j \in \mathscr{B}(\mathscr{X})$ есть вероятность того, что в последовательности измерений, задаваемых инструментами $\mathscr{M}_1, \ldots, \mathscr{M}_n$, над системой, первоначально находившейся в состоянии S, будут получены исходы $x_j \in B_j; j = 1, \ldots, n$. Если $\mathscr{X}_1, \ldots, \mathscr{X}_n$ - стандартные измеримые пространства, то функция множеств (1.12), заданная на параллелепипедах $B_1 \times \ldots \times B_n$, однозначно продолжается до вероятностной меры на б-алгебре $\mathscr{B}(\mathscr{R}\mathscr{R}_1) \times \ldots \ldots \times \mathscr{B}(\mathscr{X}_n)$ (см. [78,4.2]). Соотношение (1.15) можно записать также в виде

$$\mu_S^{\mathscr{M}_1}, \ldots, \mathscr{M}_n(B_1 \times \ldots \times B_n) = \\ = \operatorname{Tr} S\mathscr{P}_1(B_1)[\ldots \mathscr{P}_n(B_n)[1]\ldots]$$

В случае инструментов, сооответствующих проекционному постулату (1.6), соотношение (1.15) переходит в формулу Вигнера (см. статью «Проблема измерения» в сборнике [11]).

Рассмотрим повторное измерение, описываемое инструментом $\mathscr{M}$. Инструмент $\mathscr{M}$ называется воспроизводимьм, если

$$\mathscr{M}(B_1)[\mathscr{M}(B_2)[S]] = \mathscr{M}(B_1 \cap B_2)[\mathrm{S}]; B_1, B_2 \in \mathscr{B}(\mathscr{X})$$

для любого оператора плотности S. Это свойство является математическим выражением гипотезы воспроизводи мо с ти, гласящей, что «если физическая величина дважды измеряется на системе $\mathscr{P}$, причем измерения следуют непосредственно одно за другим, то в обоих случаях получается одно и.то же значение» (см. [26, гл. IV, п. 3]).

Рассмотрим инструмент со счетным множеством исходов $\mathscr{Z} = \{x_1, x_2, \ldots\}$ и положим $\mathscr{M}_i = \mathscr{M}(\{x_i\})$.

П р едложение ([134], [78]). Всякий инструмент вида (1.6) обладает свойствами:

1. $\mathscr{M}_i[\mathscr{M}_j[S]] = \delta_{ij}\mathscr{M}_i[S]$ (воспроизводимость); ния);
2. если $\operatorname{Tr} \mathscr{M}_i[S] = 1$, то $\mathscr{M}_i[S] = S$ (минимальность возмуще-
3. если $X \geqslant 0$ и $\mathscr{M}_i^*[X] = 0$ для $i = 1, 2, \ldots$, то $X = 0$ (невырожденность). (1.6).

Обратно, всякий инструмент с этими свойствами имеет вид

Таким образом, проекционный постулат (1.6) можно рассматривать как следствие ряда физически содержательных свойств соответствующего инструмента, включающих воспроизводимость. Как уже отмечалось, в случае непрерывного спектра возникают принципиальные трудности, которые в наиболее ясной форме выражаются следующей теоремой

Т е о ре м а (Озава [134]). Пусть $\mathscr{X}$ - стандартное измеримое пространство. Всякий инструмент со значениями в $\mathscr{X}$, обладающий свойством воспроизводимости (1.17), с необходимостью является дискретным, т. е. существует счетное подмножество $\mathscr{E}_0 \subset \mathscr{X}$, такое что $\mathscr{M}(\mathscr{X}\setminus\mathscr{X}_0)[S] = 0$ для всех S.

Доказ ательство. Рассмотрим точное состояние, задаваемое невырожденным оператором плотности S. Согласно п. 1.1, существует семейство апостериорных состояний $\{S_x\}$. Пусть $\{B_n\}$ - счетная подалгебра, порождающая $\mathscr{B}(\mathscr{X})$. Обозначая $M(B) = \mathscr{M}(B) * [\mathrm{I}]$ й используя воспроизводимость, имеем

$$\int_B \operatorname{Tr} S_x M(B_n)\,\mu_S(dx) = \operatorname{Tr}\mathscr{M}(B)[S]M(B_n) =$$

$$= \operatorname{Tr}\mathscr{N}(B\cap B_n)[S] = \int_B 1_{B_n}(x)\mu_S(dx),$$

откуда $\operatorname{Tr} S_x M(B_n) = 1_{B_n}(x)$ для μ_S-почти всех $x \in \mathscr{X}$. Поэтому найдется подмножество $\mathscr{X}_0 \subset \mathscr{X}$, такое что $\mathscr{M}(\mathscr{X}\setminus\mathscr{X}_0)[S] = 0$ и

$$\operatorname{Tr} S_x M(B) = 1_B(x); x \in \mathscr{X}_0, B \in \mathscr{B}(\mathscr{X})$$

Но тогда $\operatorname{Tr} S_x M(\{x\}) = 1, x \in \mathscr{X}_0$, т. е. $M(\{x\}) \neq 0$ и $\mu_S(\{x\}) \neq 0$, откуда следует, что $\mathscr{Q}_0$ счетно.

В примере 1 апостериорные состояния (1.7) таковы, что в этих состояниях (дискретная) наблюдаемая A с вероятностью 1 имеет определенное значение x_j. Причина трудностей с непрерывным спектром связана с тем, что (алгебраическое) состояние, в котором непрерывная наблюдаемая A имеет определенное значение, не может быть нормальным (т. е. задаваться каким-либо оператором плотности).

1.5. Измерения непрерывных наблюдаемых. В работах Шриниваза [153] и Озавы [136] указана возможность описания воспроизводимых измерений непрерывных наблюдаемых, использующая состояния и инструменты, не удовлетворяющие ус- ловию нормальности. Пусть $A = \int_{-\infty}^{\infty} xE_A(dx)$ - вещественная наблюдаемая и пусть η-какое-либо инвариантное среднее [1)] на пространстве $C(\mathrm{R})$ ограниченных непрерывных функций на R. Следуя [153], рассмотрим отображение ${\mathscr{E}_\eta}^A$ алгебры $\mathscr{B}(\mathscr{H})$ в себя, определяемое формулой

$$\operatorname{Tr} S{\mathscr{E}_\eta}^A[X] = \eta_y\left(\operatorname{Tr} Se^{iyA}Xe^{-iyA}\right)$$

где индекс y означает, что усреднение происходит по переменной y, и функцию множеств

$$\mathscr{S}_A(B)[X] = E_A(B){\mathscr{E}_\eta}^A[X]; \quad B \in \mathscr{B}(\mathbf{R})$$

Отображение ${\mathscr{E}_\eta}^A$ является условным ожиданием на коммутативную подалгебру $\{E_A(B); B \in \mathscr{B}(\mathbf{R})\}' = \mathscr{P}_A$, порожденную; наблюдаемой A. Если A имеет чисто точечный спектр, то ${\mathscr{E}_\eta}^A$ есть нормальное условное ожидание, задаваемое формулой (3.1.5), а соотношение (1.18) совпадает с проекционным посту. латом (1.6). В общем случае отображение ${\mathscr{E}_\eta}^A$ не нормальное, а функция множеств (1.18) обладает всеми свойствами воспроизводимого инструмента, кроме нормальности.

Вероятности последовательного измерения наблюдаемых $A_1, \ldots, A_n$ даются обобщением формулы (1.16)

$$\mu_S^{A_1,\ldots,A_n}(B_1\times\ldots\times B_n) =$$
$$= \operatorname{Tr} S\mathscr{P}_{A_1}(B_1)[\ldots\mathscr{P}_{A_n}(B_n)[\mathrm{I}]\ldots].$$

Если $A_1, \ldots, A_n$ совместимы, то $\mathscr{E}_\eta^{A_j}[E_{A_k}(B)] = E_{A_k}(B)$, откуда

$$\mu_S^{A_1,\ldots,A_n}(B_1 \times \ldots \times B_n) = \operatorname{Tr} S E_{A_1}(B_1) \ldots E_{A_n}(B_n)$$

т. е. распределение вероятностей последовательных точных измерений совместимых наблюдаемых совпадает с распределением точного совместного измерения этих наблюдаемых (см. п. 1.1.5) - результат, который подтверждает правомерность «обобщенного проекционного постулата» (1.18).

С другой стороны, если A_j несовместимы, то из-за не нормальности отображений $\mathscr{E}_\eta^{A_j}$, функция множеств (1.18) может оказаться лишь конечно аддитивной на (R). Для того чтобы восстановить σ-аддитивность, необходимо рассматривать распределение на компактификации вещественной прямой $\overline{\mathbf{R}} = \mathbf{R} \cup \{-\infty\} \cup \{\infty\}$. Например, после точного измерения наблюдаемой координаты Q система переходит в не нормальное состояние, в котором импульс P с положительными вероятностями принимает значения $\pm\infty$[153].

1. См. Ф. Гринлиф. Инвариантные средние на топологических группах и их приложения.- М.: Мир, 1973.

Озава [136] построил процесс косвенного измерения, отвечающий обобщенному проекционному постулату (1.18) и разъяснил роль инвариантного среднего η. Рассмотрим наблюдаемые Q, P во вспомогательном гильбертовом пространстве $\mathscr{H}_0 = L^2(\mathbf{R})$, которое будет описывать «пробную систему». Пользуясь теоремой Банаха о продолжении, можно показать, что для любого η на алгебре $\mathfrak{B}(\mathscr{C}_0)$ сушествует (не нормальное) состояние E_n, такое, что

$$E_\eta(f(Q)) = f(Q), E_\eta(f(P)) = \eta(f)$$

для любой $f \in C(\mathbb{R})$. Пусть $U_t = \exp(-itH_{\text{lnt}})$ - унитарная эволюция в $\mathscr{H} \otimes \mathscr{H}_0$, где

$$H_{\text{lnt}} = \lambda(A \otimes P)$$

причем λ может быть выбрано произвольно большим, чтобы пренебречь свободной динамикой системы и прибора. В [136] показано, что для любого (нормального) состояния S и любого $X \in \mathscr{B}(\mathscr{H})$

$$\operatorname{Tr} S \mathscr{P}_A(B)[X] = (E_S \otimes E_\eta)\left(U_{1/\lambda}^*(X \otimes E_Q(B))\, U_{1/\lambda}\right); \quad B \in \mathscr{B}(\mathbf{R})$$

Таким образом, пробная система, находящаяся в состоянии E_η с точно определенной координатой, в течение времени $1/\lambda$ взаимодействует с наблюдаемой системой согласно (1.21), после чего производится точное измерение координаты пробной системы.

Такая схема является обобщением процедуры косвенного измерения, рассмотренной фон Нейманом в случае чисто точечного спектра ([26, гл. VI, п. 3]). В принципиальном плане она сводит измерение произвольной квантовой наблюдаемой к измерению координаты пробной системы, при условии реализуемости гамильтониана взаимодействия (1.21).

12.4.2 2. Continuous Measurement Processes

2.1. Неразрушающие измерения.

Рассмотрим изолированную квантовую систему, эволюция которой описывается группой унитарных операторов $\{U_t; t \in \mathbf{R}\}$ в гильбертовом пространстве $\mathscr{H}$. Пусть $\{A_{jt}; j = 1, \ldots, m; t \in T\}$, где $T \subset \mathbf{R}$ - семейство вещественных наблюдаемых. Обозначим

$$A_j(t) = U_t^* A_{jt} U_t; \quad t \in T$$

и предположим, что для любых моментов времени $t_1 < \ldots < t_n$ и любых $j_1, \ldots, j_n$ наблюдаемые $A_{j_1}(t_1), \ldots, A_{j_n}(t_n)$ со в м стимы. Согласно формуле (1.20), последовательное точное измерение наблюдаемых $A_{j_1}(t_1), \ldots, A_{f_n}(t_n)\,(j_k = 1, \ldots, m)$ имеет распределение вероятностей

$$\mu_S\left(B_1 \times \ldots \times \bar{D}_n\right) = \operatorname{Tr} S E_{(t_1)}(B_1) \ldots E_{(t_n)}(B_n)$$

где $B_k \in \mathscr{R}(\mathbf{R}^m)$ и $E_{(t_k)}$-совместная спектральная мера наблю* даемых $A_j(t_k); j = 1, \ldots, m$.

Семейство вероятностных мер (2.2) при всевозможных $n = 1, 2, \ldots; t_1, \ldots, t_n$ является согласованным. Используя теорему А. Н. Колмогорова о продолжении, можно доказать, что существует единственное ортогональное разложение единицы $\mathbf{E}$ на $\mathscr{B}\left(\mathbb{R}^T\right)$, где $\mathscr{B}\left(\mathbf{R}^T\right)$ – σ-алгебра цилиндрических множеств на пространстве траекторий $\mathbf{R}^T$ такое, что

$$E\left(x(\cdot) : x(t_1) \in B_1, \ldots, x(t_n) \in B_n\right) = E_{(t_1)}(B_1) \ldots E_{(t_n)}(B_n)$$

Оно описывает статистику непрерывного (во времени) точного измерения семейства совместимых наблюдаемых (2.1), в том смысле, что вероятность подмножества B в пространстве траекторнй есть

$$\mu_S(x(\cdot) \in B) = \operatorname{Tr} S E(B)$$

В физике подобные измерения получили название неразрушающих и привлекли внимание, в связи с задачей обнаружения слабой силы (гравитационной волны), действующей на пробную систему [69], [140].

П р и м ер. Квантовомеханический осциллятор массы m и с частотой ω, возбуждаемый скалярной силой $\varphi(t)$, описывается уравнениями

$$\dot{Q}(t) = m^{-1} P(t), \quad \dot{P}(t) = -m\omega^2 Q(t) + \varphi(t)\mathrm{I},$$

где $Q(0) = Q$, $P(0) = P$-канонические наблюдаемые, т. е. $[P, Q] = i$. Положим $A_{1t} = Q\cos\omega t - (P/m\omega)\sin\omega t$, так ч то

$$A_1(t) = Q(t)\cos\omega t - (P(t)/m\omega)\sin\omega t.$$

Из уравнений (2.3)

$$\dot{A}_1(t) = -(\varphi(t)/m\omega)\sin\omega t\mathrm{I}$$

поэтому наблюдаемые $A_1(t)$ совместимы при разных t и возможно непрерывное неразрушающее измерение семейства $\{A_1(t)\}$. Сила $\varphi(t)$ может быть определена по любой траектории из соотношения (2.4).

Аналогично, для $A_{2t} = P\cos\omega t + m\omega Q\sin\omega t$ получаем семейство совместимых наблюдаемых

$$A_2(t) = P(t)\cos\omega t + m\omega Q(t)\sin\omega t$$

для которого $\dot{A}_2(t) = \varphi(t)\cos\omega t$ I. Заметим, что $A_1(t)$ и $A_2(t)$ несовместимы, поскольку $[A_2(t), A_1(t)] = i\mathrm{I}$. Действуя в духе п. 2.1.3, рассмотрим семейство совместимых наблодаемых

$$\tilde{A}_1(t) = A_1(t) \otimes \mathrm{I}_0 - \mathrm{I} \otimes Q_0; \quad \widetilde{A}_2(t) = A_2(t) \otimes \mathrm{I}_0 + \mathrm{I} \otimes P_0$$

в пространстве $\mathscr{H} \otimes \mathscr{H}_0$ (см. [103]). Сила $\varphi(t)$ определяется тогда из соотношения

$$\varphi(t) = \cos \omega t \dot{\tilde{A}}_2(t) - m\omega \sin \omega t \dot{\tilde{A}}_1(t).$$

2.2. «Квантовый парадокс Зенона». Попытки рассмотрения непрерывных измерений н е с о ме ст и мых наблюдаемых, опирающиеся на проекционный постулат, приводят к парадоксальным выводам, в основе которых лежит следующий математический факт. Пусть H - самосопряженный оператор из $\mathscr{B}(\mathscr{H}), E$ - проектор, тогда

$$\lim_{n\to\infty} (E \exp(itH/n)E)^n = E \exp(itEHE)$$

Это следует из того, что $\| \exp(itH/n) - \mathrm{I} - itH/n\| = o(1/n)$ и $E^2 = E$. Обобщение этого результата на случай неограниченного H является непростой задачей; некоторые условия были получены Фридманом [86]. Его результаты включают случай, когда $\mathscr{H} = L^2(\mathbf{R}^n), \quad H = -\Delta/2m$ - гамильтониан свободной частицы в $\mathbf{R}^n$, а $E = 1_{\mathscr{D}}(\cdot)$ - индикатор ограниченной области $\mathscr{D} \subset \mathbb{R}^n$ с гладкой границей.

Рассмотрим свободную частицу, эволюционирующую на временном интервале $[0, t]$, и предположим, что в каждый момент времени $tk/n, k = 0, 1, \ldots, n$, производится точное измерение наблюдаемой E, описываемое проекционным постулатом (1.6). Если исход измерения равен 1, то это означает, что частица находится в области $\mathscr{D}$. Вероятность того, что во всех $n + 1$ измерениях получен исход 1, есть

$$\mu_B(1, \ldots, 1) = \mathrm{Tr}(E \exp(itH/n)E)^n S (E \exp(itH/n)E)^n$$

и при $n \to \infty$ в силу (2.6) стремится к

$$\mathrm{Tr}\, E \exp(itEHE) S_0 \exp(-itEHE)E = \mathrm{Tr}\, S_0 E$$

где S_0 - начальное состояние. Если в начальный момент частица находится в области $\mathscr{D}$, то вероятность (2.7) равна 1 независимо от эволюции, т. е. при непрерывном точном измерении местоположения частица никогда не покидает область $\mathscr{D}$ (см. также Дэвис [78, п. 7.4]). Необычные физические следствия соотношения (2.6) были подробно рассмотрены в работе Мисры и Сударшана [130], где для них было предложено общее название «квантовый парадокс Зенона».

Причина парадокса состоит в том, что измерение, описываемое проекционным постулатом, переводя состояние системы в состояние, отвечающее точно определенному значению наблюдаемой, производит конечное изменение, на фоне которого эффект эволюции за время t/n является пренебрежимо малым при $n \to \infty$. Чтобы избежать этого и получить нетривиальный предельный процесс непрерывного измерения, включающий эволюцию, Баркиелли, Ланц и Проспери [59], [60], предложили рассматривать последовательность неточных измерений, точность которых убывает пропорционально числу измерений n. Первоначально описание предельного процесса в частных случаях связывалось с фейнмановским интегралом по траекториям (ср. в этой связи также Менский [25]), однако общая картина прямо основывается на идеях, изложенных в §1, в частности на понятии инструмента. В работах А. С. Холево [47], [102] было указано на параллель такого подхода с классическими предельными теоремами в схеме серий, причем предельный процесс непрерывного измерения оказывается некоммутативным аналогом процесса с независимыми приращениями. Подобно классическому случаю, все такие процессы описываются некоторой формулой типа Леви-Хинчина [102], [35]. Квантовые случайные процессы в смысле Дэвиса [78] с

этой точки зрения соответствуют сложному пуассоновскому процессу. Дальше кратко излагаются результаты этих работ.

2.3. Предельная теорема для сверток инструментов. Для простоты ограничимся измерениями со значениями в $\mathbf{R}$ (сушественно лишь, что пространство значений является абелевой локально компактной группой; см. [102], [35]). Пусть $\mathfrak{N}_1, \ldots, \mathfrak{N}_n$ - инструменты (в алгебре наблюдаемых) со значениями в $\mathbb{R}$. Существует единственный инструмент $\mathcal{P}$ со значениями в $\mathbf{R}^n$, таКоЙ что

$$\mathscr{P}\left(B_1 \times \ldots \times B_n\right)[X] = \mathscr{P}_1\left(B_1\right)[\ldots \mathscr{P}_n\left(B_n\right)[X]\ldots]\,; B_j \in \mathscr{B}(\mathbf{R})$$

Свертка инструментов $\mathscr{P}_1, \ldots, \mathscr{N}_n$ определяется соотношением $\mathscr{N}_1 * \ldots * \mathscr{N}_n(B)[X] = \mathscr{P}\left((x^1, \ldots, x_n) : x_1 + \ldots + x_n \in B\right); B \in \mathscr{B}(\mathbf{R})$

и, согласно формуле (1.13), описывает статистику суммы исходов n последовательнх изме рений, отвечающих инструментам $\mathscr{P}_1, \ldots, \mathscr{N}_n$. Инструмент $\mathscr{N}$ со значениями в $\mathbf{R}$ называется безгранично-делимыцж, если для любого $n = 1, 2, \ldots$ найдется инструмент $\mathscr{N}_{(n)}$ такой, что $\mathscr{S} = \mathscr{N}_{(n)} * \ldots * \mathscr{N}_{(n)} \equiv \mathscr{S}_{(n)}^{*n}$. Проблема непрерывного измерения оказывается тесно связанной с пределами n-кратных сверток вида $\mathscr{P}_{(n)}^{*n}$ при $n \to \infty$ и структурой безгранично-делимых инструментов. Решение этих вопросов опирается на некоторое обобщение метода характеристичесих функций в теории вероятностей.

Обозначим $\mathfrak{F}_\sigma$ банахову алгебру w^*-непрерывных линейных отображений $\mathfrak{B}(\mathscr{H})$ в себя с произведением $\Phi \cdot \Psi[X] = \Phi[\Psi[X]]$. Единицей в этой алгебре является тождественное отображение, обозначаемое Id. В алгебре $\mathscr{F}_\sigma$ вводится топология τ, определяемая семейством полунорм

$$\|\Phi\|_S = \sup_{\|X\|<1} |\operatorname{Tr} S\Phi[X]|, \quad S \in \subseteq (\mathscr{C})$$

Характеристическая функция инструмента определяется соотношением

$$\Phi(\lambda)[\ddot{\Lambda}] = \int\limits_{\mathbf{R}} e^{i\lambda x}\mathscr{P}(d\lambda)[\tilde{X}]$$

где интеграл сходится в топологии τ. Функция $\Phi(\lambda)$ со значениями в $\mathfrak{F}_\sigma$ является характеристической функцией вполне положительного инструмента тогда и только тогда, когда

1. $\Phi(0)[I] = I$;
2. $\Phi(\lambda)\tau$-непрерывна в точке $\lambda = 0$;
3. $\Phi(\lambda)$ положительно определенна в следуюшем смысле: для любых конечных наборов $\{\psi_j\} \subset \mathscr{H}, \{\lambda_j\} \subset \mathbb{R}, \{X_j\} \subset \mathscr{B}(\mathscr{B})$

$$\sum_{j,k} \left\langle \psi_j | \Phi\left(\lambda_k - \lambda_j\right)\left[\lambda_j^* X_k^*\right]\psi_k \right\rangle \geqslant 0$$

(аналог теоремы Бохнера-Хинчина, сводящийся к ней в случае $\dim \mathscr{H} = 1$).

Характеристическая функция свертки $\mathscr{P}_1 \ldots\ldots \mathscr{P}_n$ есть поточечное произведение соответствующих характеристических функций $\Phi_1(\lambda) \cdot \ldots \Phi_n(\lambda)$, поэтому n-кратная свертка $\mathscr{P}_{(n)}^{*n}$ имеет характеристическую функцию $\Phi_{(n)}(\lambda)^n$, где $\Phi_{(n)}(\lambda)$ - характеристическая фунция инструмента $\mathscr{P}_{(n)}$. Распределение вероятностей $\mu_s^{(n)}$ суммы n повторных измерений, описываемых инструментом $\mathscr{P}_{(n)}$, определяется формулой

$$\int\limits_{\mathbf{R}} e^{i\lambda x_\mu^{(n)}}(dx) = \operatorname{Tr} S\Phi_{(n)}(\lambda)^n[1]$$

Следующее утверждение является аналогом центральной предельной теоремы в схеме серий.

П ред лож ение. Пусть $\{\mathcal{P}_{(n)}\}$ - последовательность вполне положительных инструментов и пусть существует τ - непрерывный предел

$$\tau - \lim_{n\to\infty} n\left(\Phi_{(n)}(\lambda) - \mathrm{Id}\right) = \mathscr{L}(\lambda)$$

Тогда свертки ${\mathscr{P}_{(n)}}^{*n}$ слабо сходятся к безгранично делимому инструменту $\mathscr{P}$ с характеристической функцией $\exp \mathscr{L}(\lambda)$[11] в том смысле, что

$$\tau - \lim_{n\to\infty} \int\limits_{\mathbf{R}} f(x)\mathscr{P}_{(n)}(dx) = \int\limits_{\mathbf{R}} f(x)\mathscr{N}^P(dx)$$

для всех непрерывных ограниченных функций $f(x)$.

Заметим, что аналог классического условия асимптотической пренебрегаемости

$$\lim_{n\to\infty} \left\|\Phi_{(n)}(\lambda) - \mathrm{Id}\right\| = 0$$

1. Имеется в виду экспонента в банаховой алгебре σ. в общем случае не влечет (2.9). Вопрос об описании возможных пределов $\tau - \lim_{n\to\infty} \Phi_{(n)}(\lambda)$ при одном этом условии остается открытым.

П р и м е р. Пусть A, H - (ограниченные) вещественные наблюдаемые, $p(x)$ - плотность распределения вероятностей на $\mathbf{R}$, удовлетворяющая условиям (1.8). Рассмотрим вполне положительный инструмент

$$\mathscr{P}_{(n)}(B)[X] = e^{itH/n}\sqrt{n} \int\limits_B \sqrt{p\left(\sqrt{n}x\mathrm{I} - \frac{1}{\sqrt{n}}A\right)}\times$$
$$\times x\sqrt{p\left(\sqrt{n}\times \mathrm{I} - \frac{1}{\sqrt{n}}A\right)}dx e^{-itH/n}$$

Свертка $\mathscr{P}_{(n)}^{*n}$ имеет следующую статистическую интерпретацию. Рассмотрим квантовую систему, динамика которой на интервале $[0,t]$ описывается гамильтонианом H. В моменты времени $t_j = jt/n; j = 0,1,\ldots,n-1$, производится приближенное измерение наблюдаемой A с дисперсией $n\sigma^2 = n\int x^2 p(x)dx$, а затем берется среднее $\frac{1}{n}\sum\limits_{j=0}^{n-1} \alpha\left(t_j^{(n)}\right)$ полученных результатов $\alpha\left(t_j^{(n)}\right)$ (которое имеет дисперсию σ^2). Предел при $n\to\infty$ соответствует среднему $\frac{1}{t}\int\limits_0^t \alpha(\tau)d\tau$ результатов $\alpha(\tau)$ некоторого «непрерывного измерения» наблюдаемой A. Вычисления показывают, что для достаточно гладкой плотности $p(x)$ предел (2.9) равен

$$\mathscr{L}(\lambda)[X] = it[H,X]+$$
$$+\frac{1}{4}J\left(AXA - A^2\circ X\right) + i\lambda A\circ X - \frac{1}{2}\sigma^2\lambda 2X$$

где $J = \int p'(x)^2 p(x)^{-1}dx$ - информационное количество Фишера для семейства плотностей $\{p(x+\theta)\}$ с параметром сдвига $\theta\in\mathbb{R}$, так что $\sigma^2 J \geqslant 1$.

2.4. Сверточные полугруппы инструментов. Следующий результат типа теоремы Шенберга (см., например, [96], [138]) перебрасывает мост между скалярными условно положительно определенными функциями и вполне диссипативными отображениямн (п. 3.2.2). В F_σ.

Предложение. Пусть $\mathscr{L}(\lambda)$ - функция со значениями Следующие условня эквивалентны:

1. $\exp t\mathscr{L}(\lambda)$ положительно определенна для всех $t \geqslant 0$;
2. функция $\mathscr{L}(\lambda)$ эрмитова, т. е. $\mathscr{L}(-\lambda)[X^*] = \mathscr{L}(\lambda)[X]^*$ и условно положительно определенная, т. е. для любых конечных наборов $\{\psi_j\} \subset \mathscr{H}, \{\lambda_j\} \subset \mathbb{R}, \{X_j\} \subset \mathscr{B}(\mathscr{C})$ таких, что $\sum\limits_j X_j\psi_j = 0$ выполняется

$$\sum_{j,k} \left\langle \psi_j | \mathscr{L}\left(\lambda_k - \lambda_j\right)\left[\lambda_j^* X_k\right]\psi_k \right\rangle \geqslant 0$$

Для того чтобы функция $\mathscr{L}(\lambda)$ представлялась в виде предела (2.9), необходимо и достаточно, чтобы она удовлетворяла одному из условий этого предложения, была τ-непрерывна и $\mathscr{L}(0)[1] = 0$. Такие функции будем называть квазихарактеристическими.

Семейство инструментов $\{\mathscr{S}_t; t \in \mathbf{R}_+\}$образует свертоиную полугруппу, если $\mathscr{P}_t * \mathscr{P}_s = \mathscr{P}_{t+s}; t, s \in \mathbb{R}_+$. Очевидно, что все инструменты $\mathscr{P}_t$ безгранично делимы. Пусть $\Phi_t(\lambda)$ - характеристическая функция инструмента $\mathscr{P}_t$. Соотношение

$$\Phi_t(\lambda) = \exp t\mathscr{L}(\lambda); t \in \mathbb{R}_+$$

устанавливает взаимно однозначное соответствие между квазихарактеристическими функциями $\mathscr{L}(\lambda)$ и сверточными полугруппами вполне положительных инструментов, удовлетворяющими условию непрерывности

$$\lim_{t\to 0} \|\mathscr{P}_t(U_0) - \mathrm{Id}\| = 0$$

для любой окрестности нуля U_0.

Следующий результат можно рассматривать как обобщение представления Леви-Хинчина для логарифма характеристической функции безгранично делимого распределения.

Т е о р е м а. Для того чтобы функция $\mathscr{L}(\lambda)$ со значениямн в $F_\triangleleft$ была квазнхарактеристической, необходимо и достаточно, чтобы она допускала представление

$$\mathscr{L}(\lambda) = \mathscr{L}_0 + \mathscr{L}_1(\lambda) + \mathscr{L}_2(\lambda),$$

где $\mathscr{L}_0$ - вполне диссипативное отображение вида (3.2.5), $\mathscr{L}_1(\lambda)[\lambda^*] = \sigma^2\left[(L^*XL - L^*L_0X) + i\lambda\left(L^*X + XL\right) - \frac{1}{2}\lambda_2 X\right]$, (2.15) причем $\sigma^2 \geqslant 0, L \in \mathscr{B}(\mathscr{H})$; т. е. функция типа (2.11);

$$\mathscr{L}_2(\lambda)[X] = \sum_{r,s=1}^{\infty} \int\limits_{\mathbf{R}\setminus 0} \left(V_s^* X V_r e^{i\lambda x} - V_s^* V_{r^\circ} X\right) \mu_{rs}(dx) +$$
$$+ \sum_{s=1}^{\infty} V_s^* X \int\limits_{\mathbf{R}\setminus 0} \left(e^{i\lambda\lambda x} - 1\right) \mu_{0s}(dx) +$$
$$+ \sum_{r=1}^{\infty} X V_r \int\limits_{\mathbf{R}\setminus 0} \left(e^{i\lambda x} - 1\right) \mu_{r0}(dx) +$$
$$+ \left[\int\limits_{R} \left(e^{i\lambda\lambda x} - 1 - \frac{i\lambda x}{1+x^2}\right) \mu_{00}(dx) + i\alpha\lambda\right] \pi$$

где $\alpha \in \mathbb{R}, V_s \in \mathscr{B}(\mathscr{H})$, а $[\mu_r, s]_{r,s=1,2,\ldots}$-положительно определенная матрица комплексных мер на $\mathbf{R}\setminus 0$, такая, что ряд

$$\sum_{r,s=1}^{\infty} \mu_{rs}(\mathbf{R}\setminus 0) V_s^* V_r \text{ сходится } w^*\text{-слабо, и}$$

$$\int\limits_{R\setminus 0} \frac{x^2}{1+x^2} \mu_{00}(dx) < \infty.$$

Доказательство формулы (2.14) использует разновидность конструкции ГНС, которая сопоставляет условно положительно определенной функции $\mathscr{L}(\lambda)$ пару коммутирующих кощиклов алгебры $\mathscr{B}(\mathscr{H})$ и группы $\mathbf{R}$, а также сведения о структуре этих коциклов [96], [84], [76] (доказательство проходит для любой алгебры фон Неймана и абелевой локально-компактной группы). Перенесение вероятностного метода, основанного на понятии сопровождающего закона, представляется в некоммутативной снтуации затруднительным.

Вероятностный смысл каждого из слагаемых в формуле (2.12) выясняется в связи с процессами непрерывного измерения.

2.5. Инструментальные процессы. Пусть - пространство всех вещественных функций на $\mathbf{R}, \mathscr{B}_{a,b}$ – σ-алгебра, порождаемая приращениями $y(s) - y(t); a \leqslant t < s \leqslant b$. Ннструментальным процессом с независимьми приращениями (и. -процессом) называется семейство $\{\mathscr{P}_{a,b}; a, b \in \mathbf{R}, a \leqslant b\}$, где $\mathscr{P}_{a,b}$ - инструмент (в алгебре наблюдаемых) со значениями в $(\mathscr{Y}, \mathscr{B}_{a,b})$, причем

$$\mathscr{P}_{a,b}(E) \cdot \mathscr{P}_{b,c}(F) = \mathscr{P}_{a,c}(E \cap F)$$

если $a \leqslant b \leqslant c$ и $E \in \mathscr{B}_{a,b}, F \in \mathscr{B}_{b,c}$. Если все инструменты $\mathscr{P}_{a,b}$ вполне положительны, то и.-процесс называется вполне положительным. Для любого оператора плотности S и временного промежутка $[a, b]$ и.-процесс определяет распределение вероятностей

$$\mu_s(E) = \operatorname{Tr} S \mathscr{P}_{a,b}(E)[I]; E \in \mathscr{B}_{a,b}$$

на пространстве траекторий $y(t); t \in [a, b]$. С физической точки зрения, исходом непрерывного измерения является производная $\dot{y}(t)$, однако оказывается, что распределение (2.18) сосредоточено на недифференцируемых функциях. Это определение, данное в [102], является модификацией определения Дэвиса [78], использовавшего лишь пространство скачкообразных функций и более общего

определения Баркиелли, Ланца, Проспери [59], основанного на пространстве обобщенных функций. В случае $\dim \mathscr{H} = 1$ и.-процессы - это обычные вещественные процессы с независимыми приращениями. Всякий и.-процесс однозначно определяется набором своих конечномерных распределений, ко- торые в силу (2.17) имеют следующую структуру

$$\begin{gathered}\mathscr{P}_{\tau_0,\tau_p}\left(y(\cdot) : y\left(\tau_1\right) - y\left(\tau_0\right) \in B_1, \ldots, y\left(\tau_p\right) - y\left(\tau_{p-1}\right) \in B_p\right) = \\ = \mathscr{P}_{\tau_0,\tau_1}\left(y(\cdot) : y\left(\tau_1\right) - y\left(\tau_0\right) \in B_1\right) \ldots \\ \ldots \cdot \mathscr{P}_{\tau_{p-1}}, \tau_p\left(y(\cdot) : y\left(\tau_p\right) - y\left(\tau_{p-1}\right) \in B_p\right),\end{gathered}$$

где $\tau_0 \leqslant \tau_1 \leqslant \ldots \leqslant \tau_p; B_1, \ldots, B_p \in \mathscr{B}(\mathbf{R})$.

И.-процесс называется однородным, если для любых a, b, $\tau \in \mathbf{R}$ выполняется

$$\mathscr{P}_{a+\tau,b+\tau}\left(T_\tau(E)\right) = \mathscr{P}_{a,b}(E), \quad E \in \mathscr{B}_{a,b},$$

где $\left(T_\tau y\right)(t) = y(t+\tau)$. Соотношение

$$\mathscr{N}_t(B) = \mathscr{N}_{a,a+t}(y(\cdot) : y(a+t) - y(a) \in B); \quad B \in \mathscr{B}(\mathbf{R})$$

определяет тогда сверточную полугруппу инструментов, через которую конечномерные распределения выражаются по формуле

$$\begin{gathered}\mathscr{P}_{\tau_\bullet,\tau_p}\left(y(\cdot) : y\left(\tau_1\right) - y\left(\tau_0\right) \in B_1, \ldots, y\left(\tau_p\right) - y\left(\tau_{p-1}\right) \in B_p\right) = \\ = \mathscr{P}_{\tau_1-\tau_0}\left(B_1\right) \cdot \ldots \cdot \mathscr{P}_{\tau_p-\tau_{p-1}}\left(B_p\right).\end{gathered}$$

Если и.-процесс непрерывен в том смысле, что

$$\lim_{t\to 0} \left\| \mathscr{P}_{a,a+t}(y(\cdot) : |y(a+t) - y(a)| \geqslant \varepsilon) - \mathrm{Id} \right\| = 0$$

для любого $\varepsilon > 0$, то соответствующая сверточная полугруппа непрерывна в смысле (2.13), и, следовательно, ее характеристи: ческие функцин имеют вид (2.12), где $\mathscr{L}(\lambda)$ - некоторая квази: характеристическая функция. Обратно пусть $\mathscr{L}(\lambda)$ - квазихарактеристическая функция, $\{\mathscr{P}_t\}$ - соответствующая сверточная полугруппа, тогда соотношение (2.20) определяет конечномерные распределения, продолжающиеся до однородного, непрерывного, вполне положительного и.-процесса $\{\mathscr{P}_{a,b}\}$. Более того, модифицируя технику продолжения теории случайных процессов [11], можно доказать, что и.-процесс $\{\mathscr{P}_{a,b}\}$ сосредоточен на подпространстве $\mathscr{D} \subset \mathscr{Y}$, состоящем из функций без разрывов второго рода. Функция $\mathscr{L}(\lambda)$ называется генератором н.-процесса $\{\mathscr{N}_{a,b}\}$.

Слагаемое $\mathscr{L}_0$ в формуле (2.14) описывает эволюцию (в общем случае необратимую) рассматриваемой квантовой системы, происходящую независимо от процесса измерения. В класснческом случае ($\dim \mathscr{H} = 1$) это слагаемое вообще отсутствует. Второе слагаемое $\mathscr{L}_1(\lambda)$ описывает процесс непрерывного приближенного измерения наблюдаемой $A = \sigma^2\left(L + L^*\right)$. Соответствующий и.-процесс сосредоточен на непрерывных траекториях и отвечает классическому вннеровскому процессу. Многомерное обобщение - сумма слагаемых вида (2.11) с разными операторами $L_1, \ldots, L_m$ - задает процесс непрерывного приближенного

1. См. И. И. Гихман, А. В. Скороход. Теория случайных процессов.- М.: Наука, 1973.- 2. измерения нескольких (вообще говоря, несовместимых) наблюдаемых [60]. Наконец, слагаемое $\mathscr{L}_2(\lambda)$ описывает скачкообразную компоненту процесса измерения.

Пр и м е р (ср. [78, гл. 5]). Пусть $B \to \mathscr{P}(B)$; $B \in \mathscr{B}(\mathbf{R}\backslash 0)$ - функция множеств, удовлетворяющая определению (вполне положительного) инструмента (см. п. 1.1), за исключением условия нормировки 2). Таким образом, $C = \mathscr{P}(\mathbf{R}\backslash 0)[\mathrm{I}]$ - некоторый положительный оператор. Соотношение

$$\mathscr{L}(\lambda)[X] = \int\limits_{\mathbf{R}\backslash 0} e^{i\lambda x\mathscr{P}}(dx)[X] - C \circ X + i[H, X]$$

определяет квазихарактеристическую функцию, представляющую собой первое слагаемое в формуле (2.16). Однородный н.-процесс $\{\mathcal{P}_{a,b}\}$ с генератором (2.22) имеет кусочно-постоянные траектории; пусть, например, $F \subset \mathscr{D}$ - подмножество траекторий, имеющих ровно m скачков на отрезке $[a, b]$, причем j-й скачок происходит на интервале $\Delta_j \subset [a, b]$ и имеет величину $h_j \in B_j$, где $B_j \in \mathscr{B}(\mathbf{R}\backslash 0)$. Если интервалы $\Delta_1, \ldots, \Delta_m$ следуют друг за другом без пересечений, то

$$\mathcal{P}_{a,b}(F) = \int\limits_{\Delta_1} \ldots \int\limits_{\Delta_m} e^{(t_1-a)\mathscr{L}_0 \cdot \mathscr{P}}(B_1) \cdot \ldots \mathscr{P}(B_m) \times$$
$$\times\, e^{(b-t_m)\mathscr{L}_0} dt_1 \ldots dt_m,$$

где $\mathscr{L}_0[X] = -C \cdot X + i[H, X]$. Особенно просто устроен аналог пуассоновского процесса с генератором

$$\mathscr{L}(\lambda)[X] = \mu\left(e^{i\lambda h} U^* X U - X\right) + i[H, X]$$

где U - изометрический оператор. Это считающий процесс [154], для которого скачки траектории фиксированной величины h происходят в случайные моменты времени, имеющие экспоненциальное распределение с параметром $\mu > 0$. В момент скачка состояние преобразуется по формуле $S \to USU^*$, а между скачками эволюционирует согласно закону

$$S \to e^{-\mu t} e^{-iHt} S e^{i\#t}.$$

Рассмотрим вкратце вотрос о сходимости повторных измерений к процессу непрерывного измерения. Пусть временная ось $\mathbf{R}$ разбита на промежутки $\left[t_i^{(n)}, t_{l+1}^{(n)}\right]$ длины $1/n$, и каждому моменту времени отвечает измерение, описываемое вполне положительным инструментом $\mathscr{P}_{(n)}$ с характеристической функцией $\Phi_{(n)}(\lambda)$. Серия таких повторных измерений естественным образом определяет и.-процесс $\{\mathscr{P}_{a,b}\}$, траекториями которого являются кусочно-постоянные функции (см. [102]). Обозначим

$$\mu_{S,X}^{(n)}(B) = \operatorname{Tr} S \mathscr{P}_{a,b}^{(n)}(E)[X]; \quad E \in \mathscr{B}_{a,b}$$

где $X \geqslant 0$.

Т е о р е м а. Пусть существует τ-непрерывный предел

$$\tau - \lim_{n\to\infty} n\left(\Phi_{(n)}(\lambda) - \mathrm{Id}\right) = \mathscr{L}(\lambda)$$

причем $\sup_n \sup_{|\lambda|\leqslant 1} n\|\Phi_{(n)}(\lambda) - \mathrm{Id}\| < \infty$. Тогда последовательность мер $\left\{\mu_{S,x}^{(n)}\right\}^n$ сходится в топологии Скорохода к мерам

$$\mu_{S,X}(E) = \operatorname{Tr} S \mathscr{P}_{a,b}(E)\left[X^-\right]$$

где $\{\mathcal{P}_{a,b}\}$-однородный вполне положительный и.-процесс с генератором $\mathscr{L}(\lambda)$.

В частности, последовательность повторных приближенных измерений наблюдаемой A из примера п. 2.3 сходится к процессу непрерывного измерения с генератором (2.11).

В случае $\dim \mathscr{H} = 1$ этот результат переходит в теорему А. В. Скорохода о сходимости сумм незавнсимых случайных величин к процессу с независимыми приращениями.

Знание генератора и.-процесса позволяет в принципе определить основные вероятностные характеристики распределения (2.18) в пространстве траекторий, в частности, произвольные смешанные моменты [60]. На этом основаны квантово-статистические приложения рассматриваемой теории. В работе [103] проведено сравнение оценок неизвестной силы, действующей на открытую квантовую систему, построенных на основе различных процессов непрерывного измерения. Статистика сцитающих процессов рассматривалась в работах [154], [18].

12.5 Processes in the Fock Space

12.5.1 1. Quantum Stochastic Calculus

1.1. Extensions in the Fock Space

Пусть $\mathfrak{b}$-гильбертово пространство. Симметричное пространство Фока, ассоциированное с $\mathfrak{h}$, -определяется как

$$\Gamma(\mathfrak{h}) = \sum_{n=0}^{\infty} \oplus \Gamma_n(\mathfrak{h})$$

где $\Gamma_0(\mathfrak{h}) = \mathbf{C}, \Gamma_n(\mathfrak{h}) = \mathfrak{h}^{sn}$ - симметризованная n-я тензорная степень пространства h) (см. п. 1.3.1). $\Gamma_n(\mathfrak{h})$ называется n-частичным подпространством, $\Gamma_0(\mathfrak{h})$ - вакуумным подпространством. В квантовой физике $\Gamma(\mathfrak{h})$ описывает систему из переменного (неограниченного) числа частиц (бозонов [6], [7]).

В интересуюшем нас случае, когда $\mathfrak{h} = L^2(\mathbf{R}_+)$, пространство Фока $\Gamma(\mathfrak{b})$ состоит из бесконечных последовательностей

$$\psi = [f_0, f_1(t), \ldots, f_n(t_1, \ldots, t_n), \ldots]$$

где $f_0 \mathrm{EC}, f_n(t_1, \ldots, t_n)$-комплексная симметричная квадратично-интегрируемая функция от $t_1, \ldots, t_n \in \mathbf{R}_+$, причем

$$\langle \psi | \psi \rangle \equiv \sum_{n=0}^{\infty} \frac{1}{n!} \int_0^{\infty} \ldots \int_0^{\infty} |f_n(t_1, \ldots, t_n)|^2 \, dt_1 \ldots dt_n < \infty.$$

Удобная модификация этого представления была предложена Маассеном в [142]. Пусть $\tau = \{t_1, \ldots, t_n\}$-цепь в $\mathbf{R}_+$, т. е. подмножество $\mathbf{R}_+$конечной мощности $|\tau| = n$, упорядоченное так, что $t_1 < \ldots < t_n$. Обозначая $\mathfrak{P}$ множество всех цепей, $\mathfrak{P}_n$ - множество цепей мощности n, имеем $\mathfrak{P} = \bigcup_{n=0}^{\infty} \mathfrak{P}_n$, где $\mathfrak{P}_0 = \{\varnothing\}$. Определим на $\mathfrak{p}\sigma$-конечную меру $\mu(d\tau)$, которая совпадает с мерой $dt_1 \ldots dt_n$ на $\mathfrak{P}_n, n > 0$, и $\mu(\varnothing) = 1$. Для $\psi \in \Gamma$ () положим $\psi(\tau) = f_n(t_1, \ldots, t_n)$, если $|\tau| = n > 0$ и $\psi(\varnothing) = f_0$. Симметричная функция f_n однозначно определяется своим ограничением на $\mathfrak{P}_n$, причем $\frac{1}{n!} \int_0^{\infty} \ldots \int_0^{\infty} |f_n(t_1, \ldots, t_n)|^2 \, dt_1 \ldots dt_n = \int_{\mathfrak{P}_n} |\psi(\tau)|^2 \mu(d\tau)$, так что

$$\langle \psi | \psi \rangle = \sum_{n=0}^{\infty} \int_{\mathfrak{P}_n} |\psi(\tau)|^2 \mu(d\tau) = \int_{\mathfrak{P}} |\psi(\tau)|^2 \mu(d\tau).$$

Для любого $t \geqslant 0$ определим операторы $A(t), A^+(t), \Lambda(t)$ соотношениями

$$(A(t)\psi)(\tau) = \int\limits_0^t \psi(\tau \cup \{s\})ds$$

$$\left(A^+(t)\psi\right)(\tau) = \sum_{s\in\tau} 1_{[0,t]}(s)\psi(\tau\backslash\{s\})$$

$$(\Lambda(t)\psi)(\tau) = \sum_{s\in\tau} 1_{[0,t]}(s)\psi(\tau)$$

Оператор $A(t)$ переводит $\Gamma_n \equiv \Gamma_n\left(L^2\left(\mathbf{R}_+\right)\right)$в $\Gamma_{n-1}, A^+(t)$ переводит Γ_n в Γ_{n+1}, и $\Lambda(t)$ переводит Γ_n в Γ_n. В квантовой физике $A(t)$ является оператором уничтожения (бозона на временном отрезке $[0,t]), A^+(t)$ - оператором рождения, $\Lambda(t)$ - оператором числа частиц (бозонов). Общей инвариантной областью определения является подпространство Γ_∞, состоящее из векта- ров $\psi \in \Gamma(\mathfrak{h})$ таких, что

$$\int\limits_{\mathfrak{P}} \lambda^{|\tau|}|\psi(\tau)|^2\mu(d\tau) < \infty$$

для всех $\lambda > 0$. Операторы $A(t), A^+(t)$ однозначно продолжаются до замкнутых взаимно сопряженных операторов (для которых сохраняются прежние обозначения). Операторы $\Lambda(t)$, а также

$$Q(t) = A(t) + A^+(t), P(t) = i\left(A^+(t) - A(t)\right)$$

являются существенно самосопряженными на Γ_∞ (см., например, [6], [29]).

Из определений (1.2) вытекают следующие коммутационные соотношения на Γ_∞

$$[A(t), A(s)] = 0, \quad \left[A^+(t), A^+(s)\right] = 0$$
$$\left[A(t), A^+(s)\right] = (t \wedge s)\mathrm{I}$$
$$[\Lambda(t), \Lambda(s)] = 0$$
$$[\Lambda(t), A(s)] = -A(t \wedge s), \quad \left[\Lambda(t), A^+(s)\right] = A^+(t \wedge s)$$

где $t \wedge s = \min(t, s)$. Отсюда следует, что

$$[Q(t), Q(s)] = 0, \quad [P(t), P(s)] = 0$$
$$[Q(t), P(s)] = 2i(t \wedge s)\mathrm{I}$$

$$[\Lambda(t), Q(s)] = -iP(t \wedge s), \quad [\Lambda(t), P(s)] = iQ(t \wedge s)$$

Пусть $f \in L^2\left(\mathbf{R}_+\right)$. Экспоненциальныц вектором называется вектор $\psi_f \in \Gamma(\mathfrak{h})$ такой, что $\psi_f(\varnothing) = 1, \psi_f(\tau) = \prod_{t\in\tau} f(t)$. Скаля рное произведение двух экспоненциальных векторов

$$\langle\psi_f|\psi_g\rangle = \exp\int\limits_0^\infty \overline{f(t)}g(t)dt$$

Из (1.2) следует, что $A(t)\psi_f = \left(\int\limits_0^t f(s)ds\right)\cdot\psi_f$.

Вектор ψ_0, соответствующий $f \equiv 0$, называется вакуумным вектором. Для него

$$A(t)\psi_0 = 0, \Lambda(t)\psi_0 = 0$$

Линейную оболочку семейства экспоненциальных векторов обозначим Γ_e. Она плотна в $\Gamma(\mathfrak{h})$ (см., например, [96]).

1.2 Стохастический интеграл.

Одно из основных свойств пространства Фока - Функтори а льное св ой ство

$$\Gamma(\mathfrak{h}_1 \oplus \mathfrak{h}_2) = \Gamma(\mathfrak{h}_1) \otimes \Gamma(\mathfrak{h}_2),$$

в частности, для любого $t \in \mathbf{R}_+$

$$\Gamma\left(L^2(\mathbf{R}_+)\right) = \Gamma\left(L^2(0,t)\right) \otimes \Gamma\left(L^2(t,\infty)\right)$$

При этом экспоненциальные векторы, включая вакуумный, также факторизуются

$$\psi_f = \psi_f^{(0,t)} \otimes \psi_f^{(t,\infty)}$$

Поскольку $L^2(\mathbf{R}_+)$можно рассматривать как непрерывную прямую сумму (прямой интеграл) одномерных гильбертовых пространств, пространство $\Gamma(L^2(R_+))$является, в определенном смысле, непрерывным тензорным произведением. Эта структура лежит в основе связи между пространством Фока, безграничной делимостью и процессами с независимыми приращениями (см., например, [96], [138]).

Далее $\mathfrak{G} = \mathscr{H} \otimes \Gamma(L^2(\mathbf{R}_+))$, где $\mathscr{H}$-некоторое «начальное» пространство. Элементы 5 можно рассматривать как функции $\downarrow(\tau), \tau \in \mathrm{Re}$, со значениями в $\mathscr{H}$. Будет удобно не различать в написании операторы, действующие в $\mathscr{H}$, или в $\Gamma(L^2(\mathbf{R}_+))$, и их поднятия в \$; например, $A(t)$ обозначает как оператор в $\Gamma(L^2(\mathbf{R}_+))$, так и оператор $I \otimes A(t)$ в ратор в $\mathscr{H}$). Обозначим $\mathscr{H} \otimes \Gamma_e$ алгебраическое тензорное произведение $\mathscr{H}$ и Γ_e. Семейство (вообще говоря, неограниченных) операторов $\{M(t); t \in \mathbf{R}_+\}$, определенных на $\mathscr{C} \otimes \Gamma_e$, будет называться процессом в 5.

Соотношения (1.8), (1.9) задают естественную фильтрацию в пространстве $\mathfrak{g}$. Процесс $\{M(t); t \in \mathbf{R}_+\}$в $\mathfrak{g}$ называется согласованжбц (с данной фильтрацией), если для любого $t \in \mathbf{R}_+$

$$M(t) = M_{t]} \otimes I_{[t}$$

где $M_{t]}$-оператор, действующий в $\mathscr{C} \otimes \Gamma(L^2(0,t))$, а $\mathrm{I}_{[t}$ - единичный оператор в $\Gamma(L^2(t,\infty))$. Благодаря (1.8), (1.9), определено отображение условного ожидания $\mathscr{E}_{t]}$ в алгебру операторов вида (1.10), согласованное с вакуумным состоянием $|\psi_0\rangle\langle\psi_0| \cdot$ Согласованный процесс называется жартингалож, если $\mathscr{E}_{t]}[M(s)] = M(t)$ при $s > t$. Основные процессы $\{A(t)\}$, $\{A^+(t)\}, \{\Lambda(t)\}$ я вляются мартингалами.

Партасарати и Хадсон [108], [20] построили стохастический интеграл от согласованных процессов по основным мартингалам $A(t), A^+(t), \Lambda(t)$. Дальше излагается модификация этой конструкции (см. статью А. С. Холево в [145]). Процесс $\{M(t); t \in [0,T]\}$ называется простыск, если существует разбиение $0 = t_0 < t_1 < \ldots < t_N = T$, такое что $M(t) = M(t_{j-1})$ для $t \in [t_{j-1},\ t_j)$. Для четверки простых согласованных процессов $\{M_\alpha(t)\}$, $\alpha = 0,1,2,3$, стохастический интеграл определяется соотно ;шением

$$I(T) \equiv \int_0^T \left(M_0 d\Lambda + M_1 dA + M_2 dA^+ + M_3 dt\right) =$$

$$= \sum_{j=1}^N \{M_0(t_{j-1})[\Lambda(t_j) - \Lambda(t_{j-1})] +$$

$$+ M_1(t_{j-1})[A(t_j) - A(t_{j-1})] + M_2(t_{j-1})\left[A^+(t_j) - A^+(t_{j-1})\right] +$$

$$+ M_3(t_{j-1})(t_j - t_{j-1})\}$$

Из неравенств Журне (см. [128, п. V.1.4]) вытекает оценка

$$\sup_{0<t\leqslant T}\left\|I(t)\psi\otimes\bar{\psi}_f\right\|_-^2\leqslant C(\|f\|)\cdot\left\{\int_0^T|f(t)|^2\times\right.$$

$$\times\left\|M_0(t)\psi\otimes\psi_f\right\|^2dt+\int_0^T\left[\left\|M_1(t)\psi\otimes\psi_f\right\|^2+\right.$$

$$\left.\left.+\left\|M_2(t)\psi\otimes\psi_f\right\|^2\right]dt+\left[\int_0^T\left\|M_3(t)\psi\otimes\psi_f\right\|dt\right]^2\right\},$$

тде $\psi\in\mathscr{H}, f\in L^2(\mathbf{R}_+)$. Назовем $\{M_\alpha(t)\}$ допустимой четверкой, если для любого $\varepsilon>0$ найдется четверка $\left\{\tilde{M}_\alpha(t)\right\}$ простых согласованных процессов, такая что

$$\operatorname*{ess\,sup}_{0\leqslant t\leqslant T}\left\|\left[M_0(t)-\tilde{M}_0(t)\right]\psi\otimes\psi_f\right\|<\varepsilon$$

$$\int_0^T\left\|\left[M_{1,2}(t)-\tilde{M}_{1,2}(t)\right]\psi\otimes\psi_f\right\|^2dt<\varepsilon$$

$$\int_0^T\left\|\left[M_3(t)-\tilde{M}_3(t)\right]\psi\otimes\psi_f\right\|dt<\varepsilon$$

и сильно допустимой четверкой, если для любого $\varepsilon>0$ найдется четверка $\left\{\widetilde{M}_\alpha\right\}$ простых согласованных процессов со значениями в $\mathfrak{B}(()$, такая что

$$\operatorname*{ess\,sup}_{0<t\leqslant T}\left\|M_0(t)-\tilde{M}_0(t)\right\|<\varepsilon,$$

$$\int_0^T\left\|M_{1,2}(t)-\tilde{M}_{1,2}(t)\right\|^2dt<\varepsilon,$$

$$\int_0^T\left\|M_3(t)-\tilde{M}_3(t)\right\|dt<\varepsilon.$$

Из неравенства (1.12) вытекает, что для любой допустимо четверки стохастический интеграл

$$I(T)=\int_0^T\left(M_0d\Lambda+M_1dA+M_2dA^+M_3dt\right)$$

определен на $\mathscr{C}\otimes\Gamma_e$ как сильный предел стохастических интегралов вида (1.11) от простых процесов $\left\{\tilde{M}_\alpha\right\}$ и является согласованным процессом. Если $M_3\equiv0$, то $I(t)$ является мартингалом; доказано, что достаточно произвольный ограниченный мартингал в пространстве Фока является стохастическим интегралом (Партасарати и Синха). Пример неограниченного мартингала, не представимого в виде стохастического интеграла по основным процессам, содержится в работе Журне [113].

Из определений (1.2) основных мартингалов вытекает явная формула (В. П. Белавкин [35])

$$(I(t)\psi)(\tau) = \int_0^t \left[M_3(s)\psi + M_1(s)\psi^{(s)}\right](\tau)ds +$$
$$+ \sum_{\substack{s\in\tau \\ s\leqslant t}} \left[M_2(s)\psi + M_0(s)\psi^{(s)}\right](\tau\backslash\{s\}),$$

где $\psi^{(s)}(\tau) = \psi(\tau\bigcup\{s\})$, которая может служить для альтернативного определения стохастического интеграла, имеющего смысл для более широких классов процессов (включая несогласованные процессы).

Стохастический интеграл по процессам в антисимметричном пространстве Фока рассматривался Барнетом, Стритером, Уайлдом [62], [141], Хадсоном и Эпплбаумом [107].

1.3 Квантовая формула Ито.

Соотношение (1.14) принято записывать в дифференциальной форме

$$dI = M_0 d\Lambda + M_1 dA + M_2 dA^+ + M_3 dt$$

Пусть $J(t)$ - другой стохастический интеграл, так что $dJ = N_0 d\Lambda + N_1 dA + N_2 dA^+ + N_3 dt$.

Т е о р ем а. Если четверки $\{M_\alpha\}, \{N_\alpha\}$ сильно допустимы, то произведение $I(t)J(t)$ является стохастическим интегралом, причем

$$d(IJ) = I(dJ) + (dI)J + (dI)(dJ)$$

где произведение вычисляется по следующим формальным правилам: значения любого согласованного процесса в момент t коммутируют со стохастическими дифференциалами основных процессов $d\Lambda(t), dA(t), dA^+(t), dt$, а в слагаемом $(dI)(dJ)$ произведения стохастических дифференциалов основных процессов находятся согласно таблице умножения

	dA^+	$d\Lambda$	dA	dt
dA	dt	dA	0	0
$d\Lambda$	dA^+	$d\Lambda$	0	0
dA^+	0	0	0	0
dt	0	0	0	0

Алгебра стохастических дифференциалов (1.15) с таблицей умножения (1.16) изоморфна некоторой алгебре 3×3-матриц. Особенно удобна реализация, предложенная В. П. Белавкиным в [35]: соответствие

$$dI = M_0 d\Lambda + M_1 dA + M_2 dA^+ + M_3 dt \leftrightarrow$$
$$\mathbf{M} = \begin{bmatrix} 0 & M_1 & M_3 \\ 0 & M_0 & M_2 \\ 0 & 0 & 0 \end{bmatrix}$$

оказывается инволютивным алгебраическим изоморфизмом, переводящим инволюцию $(dI)^* = M_0{}^* d\Lambda + M_2{}^* dA + M_1{}^* dA^+ + M_3^* dt$ в инволюцию

$$\begin{bmatrix} 0 & M_1 & M_3 \\ 0 & M_0 & M_2 \\ 0 & 0 & 0 \end{bmatrix}^\star = \begin{bmatrix} 0 & M_2^* & M_3^* \\ 0 & M_0^* & M_1^* \\ 0 & 0 & 0 \end{bmatrix}$$

П р и м е р. Рассмотрим стохастические интегралы

$$B(t) = \int_0^t J(s)dA(s), B^+(t) = \int_0^t J(s)dA^+(s)$$

где $J(t) = (-1)^{\Lambda(t)}$ - сильн допустимый процесс. Из формулы (1.24) следующего пункта вытекает, что $J(t)$ удовлетворяет уравнению

$$dJ = -2Jd\Lambda$$

Пользуясь таблицей (1.16), находим

$$d(BJ + JB) = -2(BJ + JB)d\Lambda$$

Поскольку $B(0) = 0$, то из теоремы следующего пункта вытекает, что $B(t)J(t) + J(t)B(t) \equiv 0$. Снова пользуясь таблицей (1.16), находим $d\left(BB^+ + B^+B\right) = dt$, откуда

$$B(t)B^+(t) + B^+(t)B(t) = t,$$

т. е. операторы $B(t), B^+(t)$ удовлетворяют каноническому антикоммутационному соотношению для фермионных операторов рождения-уничтожения. Этот факт лежит в основе изоморфизма между симметричным (бозонным) и антисимметричным (фермионным) пространствами Фока, установленного Хадсоном и Партасарати [109].

Квантовый стохастический интеграл и формула Ито имеют естественное обобщение на случай многих степеней свободы, когда основные процессы $A_j(t), A_k{}^+(t), \Lambda_{jk}(t)$ многомерны и действуют в пространстве Фока $\Gamma\left(L_{\mathscr{K}}{}^2(\mathbf{R}_+)\right)$, где $\mathscr{K}$ - гильбертово пространство, размерность которого равна числу степеней свободы (Хадсон, М. П. Эванс [143], В. П. Белавкин [35]), а также в нефоковских пространствах, связанных с гауссовскими состояниями канонических коммутационных соотношений (Хадсон, Линдсей [142]).

1.4. Квантовые стохастические дифференциальные уравнения. Рассмотрим линейное однородное квантовое стохастическое дифференциальное уравнение

$$dV = \left[L_0d\Lambda + L_1dA + L_2dA^+ + L_3dt\right]V, t \geqslant 0$$

с начальным условием $V(0) = \mathrm{I}$, которое является краткой записью интегрального уравнения

$$V(t) = I + \int_0^t \left[L_0(s)d\Lambda(s) + L_1(s)dA(s) + L_2(s)dA^+(s) + \right.$$
$$\left. + L_3(s)ds\right]V(s).$$

Модифицируя рассуждение Хадсона и Партасарати [108], основанные на методе последовательных приближений, можно доказать следующую теорему.

Т е ор ем а. Если $\{L_\alpha\}$ - сильно допустимая четверка, то решение $\{V(t); t \in \mathbf{R}_+\}$уравнения (1.18) существует, единственно и является сильно непрерывным согласованным процессом.

Обозначим $\mathscr{P}_t$ оператор временного сдвига в : $\mathscr{P}_t\psi(\tau) = \psi(\tau_t)$, где $\tau_t = \{t_1 + t, \ldots, t_n + t\}$, если $\tau = \{t_1, \ldots, t_n\}$. Решение $V(t)$ удовлетворяет уравнению ко ц и к л а

$$V(t + u) = \left(\mathscr{S}_u^*V(t)\mathscr{S}_u\right)V(u); t, u \in \mathbf{R}_+$$

Особый интерес представляет случай, когда $V(t), t \in \mathbf{R}_+$, являются унитарными операторами. Для этого необходимо и достаточно, чтобы уравнение (1.18) имело вид

$$dV = \Big[(W-I)d\Lambda + LdA^+ - L^*WdA - \left(iH + \frac{1}{2}L^*L\right)dt\Big]V,$$

где W-унитарный, а H-самосопряженный операторы из $\mathscr{B}(\mathscr{C})$.

Весьма важной является задача обобщения теоремы существования и единственности решения уравнения (1.18) на случай неограниченных коэффициентов $L_\alpha(t)$. Некоторые результаты в этом направлении имеются в работах Хадсона и Партасарати [108], Журне [113], Фриджерио, Фаньолы, А. М. Чеботарева [75]. В работе [113] частично решена задача описания силь- но непрерывных унитарных решений уравнения (1.19). Этот вопрос тесно связан с проблемой консервативности, обсуждавшейся в п. 3.2.3.

Уравнения типа (1.18) связаны с линейными стохастическими дифференциальными уравнениями в гильбертовом пространстве (см., в частности, А. В. Скороход [33]), и можно надеяться, что эти два направления взаимно обогатят друг друга. Решения уравнения (1.20) являются некоммутативным аналогом мультипликативного процесса с независимыми стационарными приращениями в группе унитарных операторов. Общая теория таких процессов развита Аккарди, фон Вальденфельсом и Шурманом [54]. Последний показал [144], [147], что всякий такой процесс, удовлетворяющий условию равномерной непрерывности, является решением уравнения типа (1.20). Используя аналогию с квантовыми процессами, А. С. Холево указал стохастическое дифференциальное уравнение, которому удовлетворяет произвольный классический мультипликативный процесс с независимыми стационарными приращениями в группе Ли (мультипликативный аналог разложения Ито) [104].

Наглядное представление решений уравнения (1.18) дают хронологически упорядоченные экспоненты, родственные мультипликативному стохастическому интегралу в классической теории случайных процессов (по поводу последнего см. Эмери [82]). Пусть $\left\{\widetilde{M}_\alpha(t)\right\}$ - четверка простых согласованных процессов на $[0,T]$ со значениями в $\mathscr{B}(\mathscr{C})$. Положим

$$V_j = \exp\Big[\tilde{M}_0(t_{j-1})(\Lambda(t_j) - \Lambda(t_{j-1})) + \\ + \tilde{M}_1(t_{j-1})(A(t_j) - A(t_{j-1})) + \tilde{M}_2(t_{j-1})\left(A^+(t_j) - A^{+^-}(t_{j-1})\right) + \\ + \tilde{M}_3(t_{j-1})(t_j - t_{j-1})\Big]$$

и обозначим

$$\leftarrow \overleftarrow{\exp} \int_0^T \left(\tilde{M}_0 d\Lambda + \tilde{M}_1 dA + \tilde{M}_2 dA^+ + \tilde{M}_3 dt\right) = \\ = V_N \cdot \ldots \cdot V_1.$$

Оператор (1.21) определен на $\mathscr{H} \otimes \Gamma_e$. В работе А. С. Холево (см. [145]) доказано, что если $\{M_\alpha\}$-сильно допустимая четверка согласованных процессов со значениями в $\mathscr{B}(\mathscr{H})$ и $\left\{\tilde{M}_\alpha^{(N)}\right\}$ - последовательность четверок простых процессов, аппроксимирующая $\{M_\alpha\}$ в смысле (1.13), то существует сильный предел на $\mathscr{C} \otimes \Gamma_e$ выражений вида (1.21), который называется хронологически упорядоченной экспонентой. При этом семейство хронологически упорядоченных экспонент

$$V(t) = \leftarrow \exp_0^T \left(M_0 d\Lambda + M_1 dA + M_2 dA^+ + M_3 dt \right), \quad t \in \mathrm{R}_+$$

является сильно непрерывным на $\mathscr{C} \otimes \Gamma_e$, согласованным процессом, который удовлетворяет стохастическому дифференциальному уравнению (1.18), где $\{L_\alpha\}$ и $\{M_\alpha\}$ связаны соотношениями

$$L_0 = a(M_0), L_1 = M_1 b(M_0), L_2 = b(M_0) M_2$$
$$L_3 = M_3 + M_1 c(M_0) M_2$$

Здесь a, b, c-целые функции

$$a(z) = e^z - 1, \quad b(z) = \frac{e^z - 1}{z}, \quad c(z) = \frac{e^z - 1 - z}{z^2}, \quad z \neq 0$$

Используя изоморфизм (1.17), эти соотношения можно объединить в одно матричное равенство

$$\mathbf{L} = e^{\boldsymbol{M}} - \mathrm{I}$$

Если коэффициенты $M_\alpha(t)$ коммутируют между собой при всевозможных значениях временных аргументов, то хронологически упорядоченная экспонента превращается в обычную

$$V(t) = \exp \int_0^t \left(M_0 d\Lambda + M_1 dA + M_2 dA^+ + M_3 dt \right)$$

и дает, таким образом, явное решение уравнения (1.18).

П р и м е р. Решение уравнения

$$dJ_z = z J_z d\Lambda; \quad J_z(0) = \mathrm{I}$$

при $z \neq -1$ записывается в виде

$$J_z(t) = (z+1)^{\Lambda(t)}, t \in \mathrm{R}_+$$

Если $z = -1$, то решение уравнения (1.24) имеет вид

$$J_{-1}(t) = \delta_{0,\Lambda(t)}$$

где $\delta_{i,j}$-символ Кронекера. Поскольку $J_{-1}(t)$ обращается в нуль, оно не может быть записано в виде экспоненты.

Хронологически упорядоченные экспоненты

$$V(t) = \underset{\exp}{\leftarrow} \int_0^t \left(L dA^+ - L^* dA - iH dt \right)$$

рассматривались фон Вандельфельсом, а также Хадсоном и Партасарати в [141], [20]. Эти экспоненты я вляются унитарными операторами, удовлетворяющими уравнению

$$dV = \left[L dA^+ - L^* dA - \left(iH + \frac{1}{2} L^* L \right) dt \right] V; V(0) = \mathrm{I}$$

П риме р. Пусть $\dim \mathscr{H} = 1$ и $f \in L^2(\mathbf{R}_+)$. Экспонента

$$V_f(t) = \exp \int_0^t \left(f(s) dA^+(s) - \overline{f(s)} dA(s) \right)$$

является унитарным решением уравнения

$$dV_f(t) = \left[f(t) dA^+(t) - \overline{f(t)} dA(t) - \frac{1}{2} |f(t)|^2 dt \right] V_f(t)$$

в $\Gamma\left(L^2\left(\mathbf{R}_+\right)\right)$. Из этого уравнения и квантовой формулы Ито вытекает, что процессы $V_f(t)V_g(\dot{t})$ и $V_{f+\dot{g}}(t) \exp i \operatorname{Im} \int_0^t f(s) \times \quad \times \overline{g(s)} ds$, где g-другая функция из $L^2\left(\mathbf{R}_\mathrm{t}\right)$, удовлетворяют одному и тому же уравнению; кроме того, они совпадают при $t = 0$ и, следовательно, тождественно равны, Т. е.

$$V_f(t) V_g(\boldsymbol{t}) = V_{f+g}(t) \exp \left[i \operatorname{Im} \int_0^t f(s) \overline{\mathrm{g}(s)} ds \right]$$

Рассмотрим $L^2\left(\mathbf{R}_+\right)$как вещественное линейное пространство Z с кососимметричной формой

$$\Delta(f, g) = 2 \operatorname{Im} \int_0^\infty f(s) \overline{g(s)} ds$$

Из (1.28) тогда следует, что операторы $W(f) = V_f(\infty)$ образуют (неприводимое) представление канонического коммутационного соотношения Вейля (1.2.12) в симметричном (бозонном) про. странстве Фока $\Gamma\left(L^2\left(\mathbf{R}_+\right)\right)$, а формулы (1.4), (1.5) дают ннфннтезимальную форму канонического коммутационного соотношения. При этом экспоненциальные векторы играют ту же роль, что и когерентные состояния в случае конечного числа степеней свободы, а отображение дуальности (см. п. 2.1) соответствует переходу к представлению Шрёдингера, диагонализирующему операторы $Q(t)$.

Дальнейшие сведения о квантовом стохастическом исчислении можно найти в обзоре Мейера [128], а также в сборниках [142]-[145], охватывающих такие темы, как связи с некоммутативной геометрией (Хадсон, Эпплбаум, Робинсон), применение в теории кратного стохастического интеграла (Маассен, Мейер, Партасарати, Линдсей), некоммутативные случайные блуждания в «игрушенном пространстве Фока» и их сходимость к основным процессам (Партасарати, Линдсей, Аккарди) и другие.

12.5.2 2. Расширения в пространстве Фока

Благодаря структуре непрерывного тензорного пронзведения, пространство Фока является естественным вместилишем различных «безгранично делимых» объектов. В конце 60-х годов Араки и Стритер рассматривали безгранично делимые представления групп и показали, что такие представления вкладываются в пространство Фока. Поскольку представление группы определяется некоторой положительно определенной функцией, то этот результат дает запись безгранично делимой положительно определенной функции через фоковское вакуумное среднее (см. [96], [138]). Отсюда также следует, что всякое безгранично-делимое распределение вероятностей может быть реализовано как распределение некоторой квантовой наблюдаемой относительно вакуумного состояния в пространстве Фока. Таким образом r $_r$ пространство Фока вмещает в себя все процессы с независимыми приращениями, а также процессы

«квантового шума», которые дают универсальную модель окружения открытой квантовой системы. Это обстоятельство лежит в основе конструкций расширення, использующих фоковское пространство.

2.1. Винеровский и пуассоновский процессы в пространстве Фока. Если $\{X(t); t \in \mathbf{R}\}$ - коммутирующее семейство самосопряженных операторов в гильбертовом пространстве $\mathfrak{g}$, то оно ∂a - гомализуемо: существует пространство с мерой $(\Omega, \mathscr{B}(\Omega), \mu)$ и унитарный оператор J из $\mathfrak{g}$ на $L^2(\Omega, \mu)$, такие что

$$\left(JX(t)J^{-1}\varphi\right)(\omega) = X_t(\omega)\varphi(\omega)$$

для $\varphi \in L^2(\Omega, \mu)$, где $X_t(\omega)$ - вещественные измеримые функция. При этом для любого $\psi \in \xi$ и ограниченной борелевской функции $f(x_1, \ldots, x_n)$

$$\langle \psi | f(X(t_1), \ldots, X(t_n))\, \psi \rangle = \int f(X_{t_1}(\omega), \ldots, X_{t_n}(\omega))\, P(d\omega)$$

где $P(d\omega) = |(J\psi)(\omega)|^2 \mu(d\omega)$ - вероятностная мера на Ω. В этом смысле семейство $\{X(t)\}$ в гильбертовом пространстве 5 с выделенным вектором ψ стохастически квивалентно случайному процессу $\{X_t(\omega)\}$ в вероятностном пространстве $(\Omega, \mathscr{B}(\Omega), P)$.

Рассмотрим коммутирующее (в силу (1.5)) семейство самосопряженных операторов $\{Q(t)\}$ в $\Gamma(L^2(\mathbf{R}_+))$. Пусть $\{W_t;\ t \in \mathbf{R}_+\}$- стандартный винеровский процесс, $L^2(W)$ - гильбертово пространство комплексных квадратично интегрируемых функционалов от винеровского процесса. Отображение дуальности (Сигал)

$$J\psi = f_0 + \sum_{n=1}^{\infty} \int_{\mathfrak{P}_n} \ldots \int f_n(t_1, \ldots, t_n)\, dW_{t_1} \ldots dW_{t_n}$$

где в правой части формулы - кратные стохастические интегралы в смысле Ито, является изоморфизмом пространства Фока $\mathfrak{G} = \Gamma(L^2(\mathbf{R}_+))$и $L^2(W)$, причем

$$J\Psi_0 = 1; \quad JQ(t)^{J-1} = W_t$$

Поэтому семейство $\{Q(t)\}$ в $\Gamma(L^2(\mathbf{R}_+))$с вакуумным вектором ψ_0 стохастически эквивалентно винеровскому процессу W_t. Аналогичное утверждение справедливо и для коммутирующего се- мейства $\{P(t)\}$. Заметим, что в силу (1.5) операторы $Q(t)$ и $P(s)$ не коммутируют между собой и поэтому семейство $\{Q(t),\ P(t)\}$ не эквивалентно двумерному винеровскому процессу. Унитарный оператор $U\psi(\tau) = i^{|\tau|}\psi(\tau)$ переводит ψ_0 в ψ_0 и

$$P(t) = UQ(t)U^{-1}.$$

Оператору U в $L^2(W)$ отвечает преобразование Фурье-Винера [1)].

Рассмотрим теперь коммутирующее семейство самосопряженных операторов $\{\Lambda(t)\}$. Пусть $\{N_t; t \in \mathbf{R}_+\}$- пуассоновский процесс интенсивности λ на вероятностном пространстве $(\Omega, \mathscr{B}(\Omega), P_\lambda)$ и $L^2(N) \equiv L^2(\Omega, P_\lambda)$. Отображение

$$J^{(\lambda)}\psi = f_0 + \sum_{n=1}^{\infty} \int_{\mathfrak{P}_n} \ldots \int f_n(t_1, \ldots, t_n)\, dX_{t_1} \ldots dX_{t_n}$$

где $X_t = \lambda^{-1/2}(N_t - \lambda t)$ - компенсированный пуассоновский процесс, является изоморфизмом пространства Фока $\Gamma(L^2(\mathbf{R}_+))$и $L^2(N)$, причем

$$J^{(\lambda)}\psi_0 = 1, \quad J^{(\lambda)}\Pi^{(\lambda)}(t)J^{(\lambda)-1} = N_t$$

где

$$\Pi^{(\lambda)}(t) = \Lambda(t) + \sqrt{\lambda}Q(t) + \lambda t.$$

Таким образом, семейство $\left\{\Pi^{(\lambda)}(t)\right\}$ в $\Gamma\left(L^2\left(\mathbf{R}_+\right)\right)$с вакуумным вектором ψ_0 стохастически эквивалентно пуассоновскому процессу [108].

С точки зрения классической теории вероятностей соотношение (2.1) не может не вызвать удивления - пуассоновский процесс представлен как сумма винеровского процесса с постоянным сносом и процесса $\Lambda(t)$, равного нулю почти наверное (относительно вакуумного состояния). Дело, конечно, в том, что слагаемые не коммутируют и поэтому не могут рассматриваться как классические случайные процессы на одном вероятностном пространстве. Заметим, что подобная связь между пуассоновским и нормальным распределением хорошо известна в: квантовой оптике [21].

В подходящее пространство Фока $\Gamma\left(L^2_{\mathscr{K}}\left(\mathbf{R}_+\right)\right)$, где $L^2_{\mathscr{K}}\left(\mathbf{R}_+\right)$ - пространство квадратично-интегрируемых функций со значениями в некотором гильбертовом пространстве $\mathscr{K}$, может быть. вложен произвольный стохастически непрерывный процесс с независимыми приращениями (Партасарати, см. [128]). Представление такого процесса требует, вообще говоря, бесконечного числа независимых процессов рождения-уничтожения-числа частиц.

Среди процессов с независимыми приращениями только ви-

1. См. Т. Хида. Броуновское движение.- М.: Наука, 1987. :неровский и пуассоновский обладают следующим свойством хаотической представимости: гильбертово пространство квадра.тично интегрируемых функционалов от процесса является прямой суммой подпространств, порождаемых n-кратными стохастическими интегралами (Винер, Ито). Вопрос-какие другие мартингалы обладают этим свойством - привлек внимание спе-циалистов по теории случайных процессов. В частности, Эмери показал, что этим свойством обладает мартингал Аземы

$$X_t = \operatorname{sgn} W_t \sqrt{2\left(t - g_t\right)}$$

,где g_t - последний нуль винеровского процесса W_t перед моментом t. Партасарати [137] рассмотрел квантовое стохастическое дифференциальное уравнение

$$dX_\cdot(t) = (c-1)X(t)d\Lambda(t) + dQ_\cdot(t), \quad X(0) = 0$$

и показал, что при любом $c \in [-1, 1]$ оно имеет решение, являю- щееся коммутирующим семейством самосопряженных операто: ров и стохастически эквивалентное (относительно вакуумного вектора) мартингалу со свойством хаотической представимости. Как заметил Мейер, при $c = 0$ решение $X(t)$ стохастически эквнвалентно мартингалу Аземы. Таким образом, в высшей степени нелинейное преобразование (2.2) винеровского процесса оказывается тесно связанным с линейным стохастическим дифференциальным уравнением для некоммутирующих процессов.

2.2 Стохастические эволюции и расширения динамических полугрупп. Интересный класс безгранично делимых объектов возникает в связи с динамическими полугруппами. Пусть $\mathscr{C}$ - гильбертово пространство, Ф-динамическое отображение в алгебре $\mathfrak{B}(\mathscr{H})$, т. е. нормальное вполне положительное отображение, такое что $\Phi[\mathrm{I}] = \mathrm{I}$. Назовем Φ безгранично делимым, если для любого $n = 1, 2, \ldots \Phi = (\Phi_n)^n$, где Φ_n - динамическое отображение. Если $\{\Phi_t; t \in \mathbf{R}_+\}$- динамическая полугруппа, то все отображения Φ_t безгранично делимы, поскольку $\Phi_t = \left(\Phi_{t/n}\right)^n$. С другой стороны, если $\dim \mathscr{H} < \infty$, то всякое безгранично де-лимое динамическое отображение имеет вид $\Phi = \mathscr{E} \cdot e^{\mathscr{L}}$, где $\mathscr{E}$ -

условное ожидание на некоторую подалгебру $\mathscr{B} \subset \mathfrak{P}(\mathscr{H})$, а $\mathscr{L}$ - вполне диссипативное отображение, оставляющее подалгебру инвариантной [15]. Отображение $\mathscr{E}$ играет роль, аналогичную идемпотентному делителю в теории безгранично делимых положйтельно определенных функций на группах [138]. Если $\mathscr{E} = \mathrm{Id}$, то через Φ можно провести квантовую динамическую полугруппу.

В работе Хадсона и Партасарати [108] было построено вложение непрерывной по норме квантовой динамической полугруппы в пространство Фока, которое может быть истолковано как расширение до марковского квантового случайного процесса в смысле п. 3.2.6 (см. статью Фриджерио в [142]). Для простоты ограничимся описанием конструкции работы [108] для по- лугруппы с инфинитезимальным оператором вида

$$\mathscr{L}[X] = i[H, X] + L^* X L - L^* L_\circ X$$

где $H, L \in \mathcal{B}(\mathscr{H}), H^* = H$.

П р е д лож ен и е. Пусть $\{\Phi_t; t \in \mathbb{R}_+\}$-квантовая динамичес-: кая полугруппа в $\mathscr{B}(\mathscr{H})$ с инфинитезимальным оператором (2.3). тогда

$$\Phi_t[X] = \mathscr{E}_0 \left[V(t)^*(X \otimes I)V(t)\right], X \in \mathscr{B}(\mathscr{H})$$

где $\{V(t); t \in \mathbf{R}_+\}$-семейство унитарных операторов в $\mathscr{G} = \mathscr{H} \otimes \Gamma\left(L^2\left(\mathbf{R}_+\right)\right)$, удовлетворяющее уравнению (1.26), а отображение $\mathscr{E}0 : \mathscr{V}(\mathfrak{G}) \to \mathscr{O}(\mathscr{C})$ - усреднение по вакуумному состоянию, определяемое формулой

$$\mathrm{Tr}\, S\mathscr{E}_0[Y] = \mathrm{Tr}\left(S \otimes |\psi_0\rangle \langle\psi_0|\right) Y$$

для любого оператора плотности S в $\mathscr{H}$ и любого $Y \in \mathscr{Z}(\natural)$.

Док а за тельство. Из уравнения (1.26) и квантовой формулы Ито вытекает квантовое уравнение Ланжевена для; $X(t)$:

$$dX(t) = [L(t)*, X(t)]dA(t) + [X(t), L(t)]dA^+(t) +$$
$$+ \left\{i[H(t), X(t)] + (L(t)^* X(t) L(t) - L(t)^* L(t) \circ X(t))\right\} dt$$

Усредняя по вакуумному состоянию и учитывая первое из соотношений

$$dA(t)\psi_0 = 0, \quad d\Lambda(t)\psi_0 = 0$$

вытекающих из (1.6), получаем, что семейство наблюдаемых $\tilde{\Phi}_t[X] = \mathscr{E}_0\left[V(t)^*(X \otimes \mathrm{I})V(t)\right]$ в алгебре системы $\mathscr{B}(\mathscr{H})$ удов; летворяет уравнению

$$d\widetilde{\Phi}_t[X] = \widetilde{\Phi}_t[\mathscr{L}[X]]dt; \quad \tilde{\Phi}_0[X] = X$$

Отсюда следует, что $\tilde{\Phi}_t[X] = \exp t\mathscr{L}[X] = \Phi_t[X]$.

Пусть теперь $\{\Psi_t; t \in \mathbf{R}_+\}$-соответствуюшая динамическая полугруппа в пространстве состояний. Из представления (2.4) вытекает конструктивное доказательство теоремы о расширении, сформулированной в п. 3.2.6. Обозначим $\mathscr{C}_0 = \Gamma\left(L^2(\mathbf{R})\right)$ пространство Фока, ассоциированное с $L^2(\mathbf{R})$, и пусть $S_0 = |\psi_0\rangle \langle\psi_0|$, где ψ_0 - вакуумный вектор в $L^2(\mathbf{R})$. В пространстве $\mathscr{C} \otimes \mathscr{C}_0$ действует группа унитарных операторов временного. сдвига $\{\mathscr{P}_t; t \in \mathbf{R}\}$, определяемых как в п. 1.4. Поскольку $\mathscr{H}_0 = \Gamma\left(L^2\left(\mathbf{R}_-\right)\right) \otimes \Gamma\left(L^2\left(\mathbf{R}_+\right)\right)$, где $\mathbf{R}_- = (-\infty, 0)$, действие основных процессов $A(t), A^+(t), \Lambda(t); t \in \mathrm{R}_+$;естественно переносится в $\mathscr{C} \otimes \mathscr{H}_{\circ}$. Решение уравнения (1.26) является тогда семейством унитарных операторов $\{V(t); t \in \mathbf{R}_+\}$в $\mathscr{H} \otimes \mathscr{H}_0$, удовлетворяющим соотношению коцикла (1.19). Из этого соотношения вытекает qt0

$$U_t = \begin{cases} \mathscr{S}_t V(t), & t \in \mathrm{R}_+ \\ V(-t)^* \mathscr{S}_t, & t \in \mathrm{R}_- \end{cases}$$

является группой унитарных операторов в $\mathscr{H} \otimes \mathscr{H}_0$. Поскольку $\mathscr{P}_t^* (X \otimes \mathrm{I}) \mathscr{P}_t = X \otimes \mathrm{I}$, из (2.4) следует, что

$$\Psi_t[S] = \mathrm{Tr}_{?\mathscr{H}_0} U_t \, (S \otimes S_0) \, U_t^*, \quad t \in \mathbf{R}_+.$$

Построенное расширение имеет прозрачную физическую интерпретацию. Группа операторов временного сдвига $\{\mathscr{I}_t\}$ описывает динамику квантового шума, который играет роль окружения рассматриваемой системы. Записывая операторы $V(t)$ в виде хронологически упорядоченной экспоненты (1.25), можно видеть, что они задают эволюцию системы с гамильтонианом H, взаимодействующей с окружением посредством сингулярного гамильтониана

$$H_{\mathrm{Int}} \ = i \left(L\dot{A} + (t) - L^* \dot{A}(t) \right).$$

Усреднение унитарной эволюции $\{U_t\}$ по вакуумному состоянию шума и дает динамическую полугруппу в $\mathscr{B}(\mathscr{C})$.

Аналогичное унитарное расширение имеет место для пронзвольной квантовой динамической полугруппы с инфинитезкмальным оператором (3.2.4) - надо только использовать квантовое стохастическое исчисление с бесконечным набором операторов рождения-уничтожения.

С точки зрения статистической механики представляет интерес выяснение точных условий, при которых такая в высшей степени идеалиэированная динамическая система, как квантовый шум, возникает из более реалистичных физических моделей открытых систем (см. в этой связи работу [52], где обсуждаются приближения слабого взаимодействия и малой плотности).

Из формулы (2.4) можно получить представления квантовой динамической полугруппы через решения классических стохастических дифференциальных уравнений в гильбертовом пространстве $\mathscr{H}$ (см. статью А. С. Холево в [35]). Пусть W_t - стандартный винеровский процесс и $\left\{ V_t^{(1)}(W); t \in \mathbf{R}_+ \right\}$- случайный процесс со значениями в $\mathscr{B}(\mathscr{H})$, удовлетворяющий стохастическому дифференциальному уравнению

$$dV_t^{(1)}(W) = \left[L dW_t - \left(iH + \frac{1}{2} L^* L \right) dt \right] V_t^{(1)}(W)$$
$$V_0^{(1)}(W) = 1$$

Тогда

$$\Phi_t[X] = \mathbf{M}_{(1)} V_t^{(1)}(W)^* \lambda V_t^{(1)}(W),$$

где $\mathbf{M}_{(1)}$-математическое ожидание, отвечающее распределению винеровского процесса. С другой стороны, пусть N_t - пуассоновский процесс. с единичной интенсивностью и $\left\{ V_t^{(2)}(N) ; \right.$

Тогда

$$dV_t^{(2)}(N) = \left[(L - \mathrm{I}) dN_t - \left(iH + \frac{1}{2} \left(L^* L - \mathrm{I} \right) \right) dt \right] V_t^{(2)}(N)$$
$$V_0^{(2)}(N) = \mathrm{I}$$

$$\Phi_t[X] = M_{(2)} V_t^{(2)}(N)^* \lambda V_t^{(2)}(N)$$

где $\mathbf{M}_{(2)}$ - математическое ожидание, отвечающее распределению пуассоновского процесса.

Заметим, что решения уравнений $(2.7), (2.9)$ могут быть заэисаны в виде хронологически-упорядоченных экспонент (мультипликативных стохастических интегралов)

$$V_t^{(1)}(W) = \underset{\exp}{\leftarrow} \int_0^t \left\{ L dW_s - \left[iH + \frac{1}{2}(L^* + L) L \right] ds \right\}$$

$$V_t^{(2)}(N) = \underset{\exp}{\leftarrow} \int_0^t \left\{ (\ln L) dN_s - \left[iH + \frac{1}{2}(L^* L - \mathrm{I}) \right] ds \right\}.$$

Ограничимся выводом представления (2.8). Введем семейство изометрических операторов $V_t^{(1)}$ из $\mathscr{H}$ в $\mathfrak{H}_\ell = \mathscr{H}, \otimes \Gamma(L^2(\mathbf{R}_+))$, определя емых соотношением

$$V_t^{(1)} \varphi = V(t)(\varphi \otimes \psi_0); \quad \varphi \in \mathscr{H}\mathscr{C}.$$

Из уравнения (1.26) следует

$$dV_t^{(1)} = \left[L dQ(t) - \left(iH + \frac{1}{2} L^* L \right) dt \right] V_t^{(1)}$$

поскольку в силу (2.5) коэффициент при $dA(t)$ может быть произвольным. Если воспользоваться теперь преобразованнем дуальности, то формула (2.4) перейдет в (2.8), а уравнение (1.26) - в уравнение (2.7). Аналогично, вывод представления (2.10) из формулы (2.4) основан на преобразовании $J^{(\lambda)}$ из п. 2.1 (при $\lambda = 1$) (см. п. 2.4).

2.3. Расширения инструментальных процессов. При рассмотрении процессов непрерывного измерения естественно возникает понятие безграничной делимости инструмента, которое объединяет безграничную делимость распределений вероятностей и динамических отображений. В работе Баркиелли и Лупиери (см. [61], [142]) указано соответствующее расширение в пространстве Фока, которое можно рассматривать как конкретизацию общего результата Озава (п. 4.1.2) для процессов нзмерения, протекающих во времени. Ограничимся здесь двумя наяболее важными примерами.

Приме р 1. Рассмотрим и.-процесс $\left\{ \mathcal{N}_{a,b}^{(1)} \right\}$ с генератором

$$\mathscr{L}^{(1)}(\lambda)[X] = \mathscr{L}[\lambda] + i\lambda (L^* X + X L) - \frac{1}{2} \lambda^2 X,$$

где $L, H = H^*$-ограниченные операторы в гильбертовом пространстве $\mathscr{H}$, а $\mathscr{L}[X]$ дается формулой (2.3). Согласно п. 4.2.3, это есть процесс непрерывного измерения наблюдаемой $A = (L + L^*)$ в системе, эволюционирующей с гамильтонианом H. Из результата Баркиелли и Лупиери следует, что

$$\mathscr{P}_{0,t}^{(1)}(E)[X] = \mathscr{E}_0 \left[V(t)^* \left(X \otimes P_{0,t}^{(1)}(E) \right) V(t) \right]; \quad E \in \mathscr{B}_{0,t}$$

где $\{V(t)\}$-семейство унитарных операторов в гильбертовом пространстве $= \mathscr{H}, \otimes \Gamma(L^2(\mathbf{R}_+))$, удовлетворяющее квантовому стохастическому дифференциальному уравнению (1.26), а $P_{0,t}^{(1)}(E)$; $E \in \mathscr{B}_{0,t}$, спектральная мера семейства совместимых наблюдаемых $Q(s); 0 \leqslant s \leqslant t$, в $\Gamma(L^2(\mathbf{R}_+))$(см. п. 4.2.1) (в силу однородности аналогичное представление имеет место и для $\mathscr{P}_{a,b}^{(1)}$, где $a \leqslant b$).

Пусть $\left\{\mathscr{N}_{a,b}^{(1)}\right\}$-соответствующий и.-процесс в пространстве состояний. Тогда соотношение (2.16) приобретает вид формулы (4.1.10)

$$\mathscr{K}_{0,t}^{(1)}(E)[S] = \mathrm{Tr}_{\Gamma(L^2(\mathrm{R}_+)}\, V(t)\left(S\otimes|\psi_0\rangle\langle\psi_0|\right)\times \\ \times V(t)^*\left(\mathrm{I}\otimes P_{0,t}^{(1)}(E)\right),$$

которая имеет ясную физическую интерпретацию: наблюдаемая система, первоначально находившаяся в состоянии S и эволюционирующая с гамильтонианом H, взаимодействует с квантовым шумом посредством сингулярного гамильтониана (2.6). При этом над квантовым шумом, который играет роль пробной системы, производится непрерывное неразрушающее измерение семейства совместимых наблюдаемых $Q(s); 0\leqslant s\leqslant t$.

Прим ер 2. И.-процесс $\left\{\mathcal{P}_{a,b}^{(2)}\right\}$ с генератором

$$\mathscr{L}^{(2)}(\lambda)[X] = i[H,\ddot{\Lambda}] + \left(L^*XLe^{i\lambda} - L^*L\circ\dddot{\Lambda}\right),$$

где $H, L\in\mathfrak{B}(\mathscr{H})$, является естественным обобщением считающего процесса из п. 4.2.5. Для этого процесса расширение имеет вид

$$\mathscr{S}_{0,t}^{(2)}(E) = \mathscr{E}_0\left[V(t)^*\left(\mathrm{I}\otimes P_{0,t}^{(2)}(E)\right)V(t)\right];\quad E\in\mathscr{B}_{0,t}$$

где $P_{0,t}^{(2)}(E); E\in\mathscr{B}_{0,t}$, спектральная мера семейства совместимых наблюдаемiх $\Lambda(s);\ 0\leqslant s\leqslant t$, в $\Gamma\left(L^2\left(\mathbf{R}_+\right)\right)$. Соответствуюшее представление в пространстве состояний

$$\mathscr{K}_{0,t}^{(2)}(E) = \mathrm{Tr}_{\Gamma(L^2(R_+))}\, V(t)\left(S\otimes|\psi_0\rangle\langle\psi_0|\right)V(t)^*\left(\mathrm{I}\otimes P_{0,t}^{(2)}(E)\right) \quad (2.20)$$

имеет интерпретацию, аналогичную соотошению (2.17).

Несколько слов о методе доказательства соотношения (2.16), (2.19). Обозначим

$$\tilde{\mathscr{P}}_t^{(j)}(B) = \mathscr{E}_0\left[V(t)^*\left(I\otimes P_{0,t}^{(j)}(y(\cdot): y(t)-y(0)\in B)\right)V(t)\right],$$

где $B\in\mathscr{B}(\mathbf{R})$, и введем характеристические функции
Тогда

$$\tilde{\Phi}_t^{(j)}(\lambda) = \int_{\mathbf{R}} e^{i\lambda x}\tilde{\mathcal{P}}_t^{(j)}(dx)$$

$$\tilde{\Phi}_t^{(j)}(\lambda)[K] = \mathscr{E}_0\left[V(t)^*\cdot\left(\lambda^n\otimes e^{i\lambda Y^{(j)}(t)}\right)V(t)\right],$$

где $Y^{(1)}(t) = Q(t)$ и $Y^{(2)}(t) = \Lambda(t)$. Используя Квантовую формулу Ито, можно доказать, что функции (2.21) удовлетворяют уравнениям

$$d\widetilde{\Phi}_t^{(j)}(\lambda) = \mathscr{L}^{(j)}(\lambda)\cdot\widetilde{\Phi}_t^{(j)}(\lambda)dt,$$

r. e.

$$\tilde{\Phi}_t^{(j)}(\lambda) = \exp t\mathscr{L}^{(f)}(\lambda).$$

Отсюда вытекает, что $\left\{\tilde{\mathcal{P}}_t^{(j)}\right\}$ есть сверточная полугруппа, отвечающая и.-процессу $\left\{\mathcal{P}_{a,b}^{(j)}\right\}$. В силу взаимной однозначности соответствия между и.-процессами и сверточными полугруппами (п. 4.2.5) отсюда следуют соотношения (2.16), (2.19).

2.4. Стохастические представления процессов непрерывного измерения. Используя прием, который позволил получить в п. 2.2 стохастические представления квантовой динамической полугруппы, найдем соответствующие стохастические представ, ления для процессов непрерывного измерения [105]. Из этих представлений вытекает явное описаник распределений вероятностей в пространстве траекторий - исходов непрерывного измерения и апостериорных состояний наблюдаемой квантовой системы.

Рассмотрим сначала и.-процесс с генератором (2.15). ак отмечалось в п. 4.2.5, он сосредоточен на непрерывных траекториях. Пусть $\mu_{(1)}$-мера Винера в пространстве непрерывных функций $\mathscr{B}$, отвечающая стандартному винеровскому процессу W_t.

Предложение 1. И.-процесс $\left\{\boldsymbol{N}_{a,b}^{(1)}\right\}$ абсолютно непрерывен по мере, $\mu_{(1)}$ в том смысле, что

$$\mathscr{K}_{0,t}^{(1)}(E)[S]=\int\limits_E V_{(t)}^{1;}(W)SV_t^{(1)}(W)^*d_{\mu_{(1)}}(W);E\in\mathscr{B}_{0,t}\cap\mathscr{C},$$

где $\left\{V_t^{(1)}(W)\right\}$-семейство ограниченных операторов в $\mathscr{C}$, удовлетворяющее стохастическому дифференциальному уравнению (2.7) относительно меры $\mu_{(1)}$.

Доказательство основано на применении преобразования дуальности к представлению (2.17). При этом, как в п. 2.2, поя вляются операторы $V_t^{(1)}(W)$, а спектральная мера $P_{0,t}^{(1)}$ семеАсства $Q(s);0\leqslant s\leqslant t$, так что проектор $P_{0,i}^{(1)}(E)$ переходит в индикатор множества $E\in\mathscr{B}_{0,t}\cap\mathscr{C}$.

Соотношение (2.17) дает конкретное представление вполне положительного инструмента $\boldsymbol{x}_{0,t}^{(1)}$ в виде (4.1.12). Отсюда получается распределение вероятностей в пространстве наблюдаемых траекторий

$$\mu_S(E)=\int\limits_E \operatorname{Tr} SV_t^{(1)}(W)^*V_t^{(1)}(W)d_{\mu_{(1)}}(W);\quad E\in\mathscr{B}_{0,t}\cap\mathscr{C}$$

Оно абсолютно непрерывно по мере Винера $\mu_{(1)}$, причем плотность дается формулой

$$p_t^{(1)}(W)=\operatorname{Tr} SV_t^{(1)}(W)V_t^{(1)}(W)^*$$

и почти наверное положительна. Апостериорное состояние, отвечающее наблюдаемой траектории $W_s;0\leqslant s\leqslant t$, есть

$$S_t^{(1)}(W)=p_t^{(1)}(W)^{-1}V_t^{(1)}(W)SV_t^{(1)}(W)^*$$

Отметим, что если начальное состояние чистое, $S=|\psi\rangle\langle\psi|$, то апостериорные состояния являются чистыми $S_t^{(1)}(W)=\left|\psi_i^{(1)}(W)\right\rangle\left\langle\psi_t^{(1)}(W)\right|$, где

$$\psi_t^{(1)}(W)=V_t^{(1)}(W)\psi/\left\|V_t^{(1)}(W)\psi\right\|$$

Переидем к случаю гчитающего процесса с генератором (2.18). Пусть $\mu_{(2)}$-мера в пространстве $\mathscr{D}$, отвечающая пуассоновскому процессу единичной интенсивности.

П редложен и е 2. И.-процесс $\left\{\mathscr{M}_{a,b}^{(2)}\right\}$ абсолютно непрерывен по мере $\mu_{(2)}$, а именно

$$\mathscr{A}_{0.t}^{(2)}(E)[S]=\int\limits_E V_t^{(2)}(N)SV_t^{(2)}(N)^*d_{\mu_{(2)}}(N);E\in\mathscr{B}_{0,t}\cap\mathscr{D},$$

где $\left\{V_t^{(2)}(N)\right\}$-семейство ог раниченных операторов в $\mathscr{B}$, удовлетворяющее стохастическому дифференциальному уравнению (2.9) относительно меры $\mu_{(2)}$.

Доказательство соотношения (2.25) требует некоторого преобразования представления (2.20). Рассмотрим унитарные операторы Вейля $V_{\mathbf{s}}(t) = \exp[zA^+(t) - zA(t)]$, где $z \in \mathbf{C}$. При $s \leqslant t$ имеет место соотношение

$$V_{\mathrm{x}}(t)^*\Lambda(s)V_{\mathrm{z}}(t) = \Lambda(s) + \bar{z}A(s) + zA^+(s) + |z|^2 s \equiv \Pi(s)$$

которое проверяется с использованием уравнения (1.27) и квантовой формулы Ито. Положим $\bar{z} = 1$, тогда $\Pi(\mathrm{s})$ является пуассоновским процессом единичной интенсивности в пространстве

Фока. Обозначая $\widetilde{U}_t = V_1(t) * V(t)$, перепишем (2.20) в виде

$$\boldsymbol{x}^{(2)}_{0,t}(E) = \mathrm{Tr}_{\Gamma(L^2(R_+))}\, \tilde{U}_t \left(S \otimes |\psi_0\rangle \langle\psi_0|\right) \tilde{U}_t^* \left(\mathrm{I} \otimes \tilde{P}^{(2)}_{0,t}(E)\right),$$

где $\widetilde{P}^{(2)}_{0,t}$-спектральная мера семейства совместимых наблюдаемых $\Pi(s)$; $\quad 0 \leqslant s \leqslant t$. Из квантовой формулы Ито вытекает уравнение для $\tilde{U}_t$:

$$\begin{aligned} d\widetilde{U}_t = \big\{&(L - \mathrm{I})dA^+(t) - (L - \mathrm{I})^* dA(t) - \\ &- \left[iH + \frac{1}{2}\left(L^*L - 2L + \mathrm{I}\right)\right] dt \Big\} \tilde{U}_t \end{aligned}$$

Вводя изометрические операторы $V_t^{(2)}$ из $\mathscr{C}$ в $\mathfrak{F}$ по формуле

$$V_t^{(2)}\varphi = \tilde{U}_t\left(\varphi \otimes \psi_0\right); \quad \varphi \in \mathscr{B}$$

и учитывая соотношения (2.5), получаем уравнение

$$dV_t^{(2)} = \left\{(L - \mathrm{I})d\Pi(t) - \left[iH + \frac{1}{2}\left(L^*L - \mathrm{I}\right)\right] dt\right\} V_t^{(2)}$$

Унитарный оператор $J^{(1)}$ из п. 2.1 переводит пространство Фока $\Gamma\left(L^2\left(\mathbf{R}_+\right)\right)$в $L^2(N)$, где N_t - классический пуассоновский процесс единичной интенсивности, при этом уравнение (2.27) переходит в (2.9), проектор $\widetilde{P}^{(2)}_{0,t}(E)$ - в индикатор множества E, а формула (2.26) - в представление (2.25).

Для распределения вероятностей в пространстве наблюдаемых траекторий и апостериорных состояний получаются формулы, аналогичные (2.23) – (2.25).

2.5. Нелинейные стохастические уравнения апостериорной динамики. Получим стохастические дифференциальные уравнения, которым удовлетворяют наблюдаемые траектории и апостериорные состояния в процессе непрерывного квантового измерения. Рассмотрим сначала процесс измерения наблюдаемой $A = L + L^*$ с. генератором (2.15). Из уравнения (2.7) для семейства $V_t^{(1)}(W)$ и формулы (2.23) вытекает, что плотность $P_t^{(1)}(W)$ распределения вероятностей наблюдаемых траекторий μ_s относительно меры Винера $\mu_{(1)}$ удовлетворяет стохастическому дифференциальному уравнению

$$dp_t^{(1)}(W) = m_t(W)p_t^{(1)}(W)dWW_t$$

где

$$m_t(W) = \mathrm{Tr}\, S_t^{(1)}(W)A$$

- апостериорное среднее наблюдаемой A. Отсюда следует [1)], что наблюдаемый процесс $Y(t)$ является процессом диффузнонного типа, удовлетворяющим стохастическому дифференциальному уравнению

$$dY(t) = m_t(Y)dt + dW_t$$

1. См. Р. Ш. Липцер, А. Н. Ширяев. Статистика случайных процессов.М.: Наука, 1974, 7.2.

Применяя стохастическое исчисление Ито, получаем уравнение для апостернорного состояния (2.24)

$$dS_t^{(1)}(Y) - \mathscr{K}\left[S_t^{(1)}(Y)\right] = \Big[(L - m_t(Y))\, S_t^{(1)}(Y) + \\ + S_t^{(1)}(Y)\,(L - m_t(Y))^*\Big]\,[dY(t) - m_t(Y)dt]$$

где

$$\mathscr{K}[S] = -i[H, S] + LSL^* - L^*L \circ S$$

Это уравнение было получено В. П. Белавкиным из рассмотрения квантового аналога задачи фильтрации случайных процессов [64]. В случае чистых состояний уравнение для вектора апостериорного состояния имеет вид

$$d\psi_t^{(1)}(Y) = [L - m_t(Y)]\,\psi_t^{(1)}(Y)\,[dY(t) - m_t(Y)dt] - \\ - \left[iH + \frac{1}{2}\left(L^*L - 2Lm_t(Y) + m_t(Y)^2\right)\right]\psi_t^{(1)}(Y)dt$$

Нелинейность уравнений $(2.30), (2.31)$ обусловлена нормировкой апостериорных состояний (2.24), в основе же лежит линейное стохастическое уравнение (2.7) типа уравнения Закаи в классической теории фильтрации.

Большой интерес представляет задача вывода и исследования уравнений (2.30), (2.31) в случае, когда L, H - неограниченные операторы. В работе В. П. Белавкина и Сташевского [65] рассмотрено уравнение

$$d\psi_t^{(1)}(Y') = (Q - m_t(Y))\,\psi_t^{(1)}(Y)\,[dY(t) - m_t(Y)dt] - \\ - \left[iP^2/2m + \frac{1}{2}\,(Q - m_t(Y))^2\right]\psi_t^{(1)}(Y)dt$$

которое получается из (2.31) формальной заменой $H = P^2/2m$, $L = Q$, где P, Q - канонические наблюдаемые нерелятивистской частицы массы m. Это соответствует непрерывному приближенному измерению координаты свободной частицы. Найдено явное решение в случае гауссовского начального состояния и показано, что оно является гауссовским с дисперсией, стремящейся к конечному пределу при $t \to +\infty$. Таким образом, уравнение (2.32) снимает известный квантовомеханический парадокс с расплыванием волнового пакета свободной частицы.

Интересно, что сходные нелинейные уравнения, однако с совершенно иной мотивировкой и интерпретацией, возникли практически одновременно в работах ряда авторов, занимающихся поисками альтернативного концептуального обоснования теории квантового измерения. В работе, опубликованной в сборнике [142], Гирарди, Римини и Вебер поставили вопрос о нахождении уравнений, дающих единое описание микро-и макросистем, из которых, в частности, вытекали бы как обратимая квантовая динамика, так и необратимые изменения типа проекционного постулата. Предлагались различные решения этого вопроса; в работах Джизена [91], Гирарди, Пирла и Римини [89] введено уравнение типа (2.31), где, однако, вместо $dY(t)$ - $m_t(Y)dt$ фигурирует стохастический дифференциал некоторого априорно данного винеровского процесса (уравнение в [91]

отличается за счет выбора фазового множителя у $\psi_t^{(1)}\Big)$. Пусть $H = 0, L = \Sigma x_i E_i$ - самосопряженный оператор с чисто точечным спектром. В [91], [89] отмечается, что получающееся уравнение

$$d\psi_t = (L - \langle L\rangle_t)\,\psi_t dW_t - \frac{1}{2}\,(L - \langle L\rangle_t)^2\,\psi_t dt$$

где $\langle L\rangle_t = \langle\psi_t|L\psi_t\rangle$, дает динамическое описание проекционного постулата $\psi \to \psi_i = E_i\psi/\,\|E_i\psi\|$, в том смысле, что при $t \to +\infty$ решение ψ_t стремится к одному из состояний ψ_i. В работе Гатарека и Джизена [88] дано математическое исследование уравнения (2.33) для неог раниче н ного оператора L, а также уравнения типа (2.32). Для доказательства существования слабого решения эти авторы использовали формальный прием преобразования вероятностной меры (теорему Гирсанова), который в схеме непрерывного измерения имеет содержательный смысл перехода от процесса $Y(t)$ к винеровскому процессу W_t, определяемого формулой (2.29).

В случае считающего процесса с генератором (2.18) стохастическое уравнение для плотности в пространстве траекторий имеет вид

$$dp_t^{(2)}(N) = [\lambda_t(N) - 1]\,p_t^{(2)}(N)(dN - dt)$$

где

$$\lambda_t(N) = \mathrm{Tr}\,S_t^{(2)}(N)L^*L$$

- апостериорнай интенсивность скачков. Уравнение для апостерио рного состояния

$$dS_t^{(2)}(Y) - \mathscr{K}\left[S_t^{(2)}(Y)\right]dt =$$
$$= \left[\frac{LS_t^{(2)}(Y)L^*}{\lambda_t(Y)} - \mathrm{I}\right][dY(t) - \lambda_t(Y)dt]$$

В статье В. П. Белавина в сборнике [35] приведено общее нелинейное уравнение квантовой фильтрации, включающее в себя как уравнение (2.30), так и (2.34).

Part IV
Problems

13 General Questions

13.1 Questions to Check Basic General Knowledge

(????)

13.2 Questions to Check Basic Technical Knowledge

(???? write from Fillipov)

13.2.1 Problems about States, Entanglement

Ф-вв-л2.1 Параметры Стокса

Найдите параметры Стокса для поляризационного состояния фотона

$$|\psi\rangle = \frac{\sqrt{2}-i}{2}|H\rangle + \frac{e^{i\pi/6}}{2}|V\rangle$$

Solution

Представляем состояние в виде столбца, находим матричный элемент (??? Почему такие формулы???)

$$|\psi\rangle = \frac{1}{2}\begin{pmatrix} \sqrt{2}-i \\ e^{i\pi/6} \end{pmatrix} \qquad \langle\psi| = \frac{1}{2}\begin{pmatrix} \sqrt{2}+i & e^{-i\pi/6} \end{pmatrix}$$

$$\langle X\rangle = \langle\psi|X|\psi\rangle = \frac{1}{4}\begin{pmatrix} \sqrt{2}+i & e^{-i\pi/6} \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \sqrt{2}-i \\ e^{i\pi/6} \end{pmatrix} = \frac{\sqrt{6}-1}{4}$$

$$\langle Y\rangle = \langle\psi|Y|\psi\rangle = \frac{1}{4}\begin{pmatrix} \sqrt{2}+i & e^{-i\pi/6} \end{pmatrix}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\begin{pmatrix} \sqrt{2}-i \\ e^{i\pi/6} \end{pmatrix} = \frac{\sqrt{2}+\sqrt{3}}{4}$$

$$\langle Z\rangle = \langle\psi|Z|\psi\rangle = \frac{1}{4}\begin{pmatrix} \sqrt{2}+i & e^{-i\pi/6} \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} \sqrt{2}-i \\ e^{i\pi/6} \end{pmatrix} = \frac{1}{2}$$

Ф-вв-л2.2 Измерение

Физическая величина задаётся оператором $F = 2|H\rangle\langle H| + (1-i)|H\rangle\langle V| + (1+i)|V\rangle\langle H|$. Какие результаты можно получить при измерении этой физической величины?

Solution

Пишем состояние в виде матрицы и находим собственные значения:

$$F = \begin{pmatrix} 2 & 1-i \\ 1+i & 0 \end{pmatrix}$$

$$\det\begin{pmatrix} 2-\lambda & 1-i \\ 1+i & -\lambda \end{pmatrix} = \lambda^2 - 2\lambda - 2 = 0$$

$$\lambda_\pm = 1 \pm \sqrt{3}$$

Ф-вв-л2.3 Коллапс

В какие состояния может перейти (коллапсировать) квантовая система при измерении физической величины $F = 2|H\rangle\langle H| + (1-i)|H\rangle\langle V| + (1+i)|V\rangle\langle H|$?

Solution

$$F\,|f_\pm\rangle = \lambda_\pm\,|f_\pm\rangle$$
$$|f_+\rangle = \frac{1}{\sqrt{6+2\sqrt{3}}}\begin{pmatrix} 1+\sqrt{3} \\ 1+i \end{pmatrix}, \quad |f_-\rangle = \frac{1}{\sqrt{6-2\sqrt{3}}}\begin{pmatrix} 1-\sqrt{3} \\ 1+i \end{pmatrix}$$

Ф-вв-л2.4 Перепутанность

При каких значениях действительного параметра φ квантовое состояние двух фотонов

$$|\psi\rangle = \frac{1}{2}\left(|H\rangle\otimes|H\rangle + |H\rangle\otimes|V\rangle + |V\rangle\otimes|H\rangle + e^{i\varphi}|V\rangle\otimes|V\rangle\right)$$

является перепутанным?

Solution

Задача сводится к проверке определения:

$$\frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ 1 \\ e^{i\varphi} \end{pmatrix} \stackrel{?}{=} \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix}$$

Ответ: при всех $\varphi \neq 2\pi n, n \in \mathbb{Z}$

Ф-вв-л3.2 Измерение

Двухкубитная система находится в квантовом состоянии $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, где $\{|0\rangle, |1\rangle\}$ - стандартный базис для каждого кубита. В некоторый момент времени происходит измерение физической величины $X = |0\rangle\langle 1| + |1\rangle\langle 0|$ пад первым кубитом. В какие состояния может перейти (коллапсировать) вся система после измерения?

Solution

(думать нужно, там его рукой написан ответ)

Ф-вв-л3.3 Спектр

Какие значения может принимать при измерении физическая величина $F \otimes G$ если $F = (\mathbf{a}\cdot\sigma)$ и $G = (\mathbf{b}\cdot\sigma), \mathbf{a}, \mathbf{b} \in \mathbb{R}^3$?

Solution

(думать нужно, там его рукой написан ответ)

14 Typical Problems

14.1 Problems about Basic Models (!!)

(!!! добавлю много из Филиппова семинаров!!! очень хорошо по ним тренироваться)

14.1.1 Problems about Qubits

Вопросы по теории

Какое ускорение в решении задачи поиска можно получить в квантовом алгоритме по сравнению с классическим

?
$\sqrt{N}$
(???? А почему??????)

14.1.2 Problems about Qutrits, Exotic Qubits

6. О

(а) Можно ли преобразовать состояние двух кутритов $\sqrt{\frac{7}{12}}|00\rangle + \frac{1}{\sqrt{3}}|11\rangle + \frac{1}{\sqrt{12}}|22\rangle$ в состояние $\frac{1}{\sqrt{2}}|01\rangle + \frac{e^{i\pi/4}}{2}|11\rangle + \frac{i}{\sqrt{8}}|20\rangle + \frac{e^{i\pi/3}}{\sqrt{8}}|22\rangle$ посредством локальных операций и классической коммуникации?

(б) Можно ли преобразовать состояние двух кутритов $\sqrt{\frac{7}{12}}|00\rangle + \frac{1}{\sqrt{3}}|11\rangle + \frac{1}{\sqrt{12}}|22\rangle$ в состояние $\frac{1}{\sqrt{3}}|01\rangle + \frac{e^{i\pi/4}}{\sqrt{6}}|11\rangle + \frac{i}{2}|20\rangle + \frac{e^{i\pi/3}}{2}|22\rangle$ посредством локальных операций и классической коммуникации?

15 Other Problems (????)

(???? тут много еще про это нужно думать.)

15.0.1 Other Problems (????)

(???? тут много еще про это нужно думать.)

1.

Для d-уровневой системы, где d - простое число, экспериментатор равновероятно выбирает взаимно несмещенные базисы $\{|a\alpha\rangle\}_\alpha, a = 1, \ldots, d+1$ (из полного набора таких базисов) и проводит проективные измерения в этих базисах. Выразите матрицу плотности ϱ через вероятности исходов измерений.

2. О

Известно, что чистые кубитные состояния $|\psi_1\rangle = |0\rangle$ и $|\psi_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ генерируются квантовым источником с вероятностями $p_1 = \frac{4}{5}$ и $p_2 = \frac{1}{5}$ соответственно. Какова максимально возможная вероятность успеха в задаче безошибочного различения этих состояний?

3. О

Найдите физически реализуемое приближение для транспонирования d-уровневой квантовой системы. Для этого рассмотрите деполяризующее отображение $\Phi_q[\varrho] = q\varrho + (1-q)\,\mathrm{tr}[\varrho]\frac{I}{d}$ и укажите диапазон для действительного параметра q, при котором отображение Φ_q о T является квантовым каналом.)T - транспонирование в фиксированном ортонормированном базисе).

5. Кубитный инструмент

Рассмотрите кубитный инструмент $\{i \to \mathcal{I}_i\}$ с двумя элементарными исходами ($i = 1, 2$) вида $\mathcal{I}_1[\varrho] = \frac{1}{2}U_1\sqrt{1+p\sigma_z}\varrho\sqrt{1+p\sigma_z}U_1^\dagger, \mathcal{I}_2[\varrho] = \frac{1}{2}U_2\sqrt{1-p\sigma_z}\varrho\sqrt{1-p\sigma_z}U_2^\dagger$, где U_1 и U_2 - унитарные операторы, $-1 < p < 1$. Постройте физическую реализацию этого квантового инструмента.

7.

Классический источник производит биты " 0 " и " 1 " с вероятностями p_0 и p_1 соответственно. Бит " 1 " физически кодируется в оптический импульс интенсивности $I_1 = I$, а биту " 0 " соответствует отсутствие сигнала $(I_0 = 0)$. Информация передается по длинному оптоволокну и детектируется "оп-off" детектором. В результате ослабления оптического импульса в волокне и конечной квантовой эффективности детектора вероятность зарегистрировать исход "оп" при пересылке бита "1" равна $1/2$. Темновых отсчетов у детектора нет. Найячте пропускную способность классического канала связи. Каким должно быть соотношение битов "0" и "1" в словах, используемых для достижения максимальной скорости надежной передачи данных?

8. Дефазировка

В линии квантовой коммуникации происходит дефазировка квантовых состояний и присутствуют потери частиц, что приводит к квантовому каналу

$$\Phi[\varrho] = \left(\begin{array}{c|c} p\,(q\varrho + (1-q)\sigma_x\varrho\sigma_x) & 0 \\ \hline 0 & (1-p)\,\mathrm{tr}[\varrho] \end{array}\right), \quad 0 \leqslant p, q \leqslant 1$$

где ϱ - матрица плотности кубита. Используя однобуквенные кодирования, при которых среднее состояние ансамбля ϱ_A является максимально смешанным,

а) оцените классическую пропускную способность этого канала;

б) найдите комплементарньй канал;

в) оцените классическую пропускную способность линии связи с использованием ресурса перепутанности;

г) оцените квантовую пропускную способность линии связи.

9.

При каком условии на параметр q кубитный деполяризующий канал $\Phi_q[\varrho] = q\varrho + (1-q)\,\mathrm{tr}[\varrho]\frac{I}{2}$ является дважды самосовместимым? Т.е., при каких значениях шумового параметра q возможно приближенное клонирование произвольных кубитных состояний?

10. О кинетическом уравнении Накажимы-Цванщига для кубита

Решите кинетическое уравнение Накажимы-Цванщига для кубита:

$$\frac{d}{dt}\varrho(t) = \int\limits_0^t \left(\gamma\delta\left(t-t'\right) - \gamma^2 \sin\left[\gamma\left(t-t'\right)\right]\right)\left[\sigma_z\varrho\left(t'\right)\sigma_z - \varrho\left(t'\right)\right]dt'$$

15.0.2 Problems about Special Quantum Channels (?????)

4. О канале Ландау-Стритера

Докажите, что канал Ландау-Стритера является унистохастическим.
(не думаю, что про это думать полезно пока минимальный уровень не взят.)

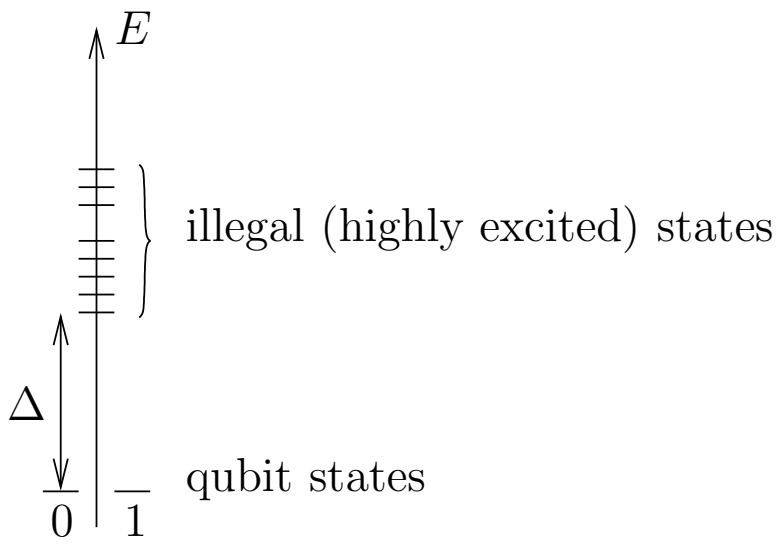


Figure 16.1: Spectrum of a physical qubit system.

Part V
Other Basic Topics

16 Topological phases and quantum computation Kitaev, Laumann

16.1 Introduction: The quest for protected qubits

The basic building block of quantum computation is the qubit, a system with two (nearly) degenerate states that can be used to encode quantum information. Real systems typically have a full spectrum of excitations that are considered illegal from the point of view of a computation, and lead to decoherence if they couple too strongly into the qubit states during some process. See Fig. 16.1. The essential problem then is to preserve the quantum state of the qubit as long as possible to allow time for computations to take place.

Assuming the gap Δ to the illegal states is reasonable, we can quite generally describe the dynamics of the qubit state by an effective Schödinger equation

$$\frac{d}{dt}|\Psi\rangle = -iH_{\text{eff}}|\Psi\rangle \tag{16.1}$$

where H_{eff} is the effective qubit Hamiltonian. In quantum optics, H_{eff} is often known with high precision. This is not so in condensed matter systems such as quantum dots. Even worse, H_{eff} may fluctuate or include interaction with the environment. This causes decoherence of the qubit state.

Ideally, we would like to arrange for H_{eff} to be zero (or $H_{\text{eff}} = \epsilon I$) for some good reason. Usually, we use a symmetry to protect degeneracies in quantum systems. For example, a quantum spin $\frac{1}{2}$ has a two-fold degeneracy protected by the $SU(2)$ symmetry, as do the $2s+1$ degeneracies of higher spins s. Indeed, any *non-Abelian* symmetry would work. Unfortunately, the $SU(2)$ symmetry of a spin is lifted by magnetic fields and it's generally difficult to get rid of stray fields.

Rather than symmetry, in what follows we will look to topology to provide us with physically protected degeneracies in quantum systems. In particular, we will examine a number of

exactly solvable models in one and two dimensions which exhibit topologically phases – that is, gapped phases with a protected ground state degeneracy dependent on the topology of the manifold in which the quantum model is embedded. In Sec. 16.2 we warm up with the study of several quantum chains that exhibit Majorana edge modes and thus a two-fold degeneracy on open chains. The topological phenomena available in two dimensional models are much richer and will be the focus of the remaining three sections. We introduce and solve the toric code on the square lattice in Sec. 16.3, exhibiting its topolological degeneracy and excitation spectrum explicitly. The following section steps back to examine the general phenomenology of quasiparticle statistics braiding in two dimensional models. Finally, in Sec. 16.5 we introduce the honeycomb lattice model which exhibits several kinds of topological phases, including that of the simple toric code and, in the presence of time reversal symmetry breaking, a gapped phase with chiral edge modes protected by the topology of the Fermi surface.

16.2 Topological phenomena in 1D: boundary modes in the Majorana chain

We will consider two examples of 1D models with $\mathbb{Z}_2$ symmetry and topological degeneracy: the *transverse field Ising model* (TFIM) and the *spin-polarized superconductor* (SPSC). Although these models look rather different physically, we will find that they are mathematically equivalent and that they both exhibit a topological phase in which the ground state degeneracy is dependent on the boundary conditions of the chain. That is, the ground state on an open chain is 2-fold degenerate due to the presence of boundary zero modes, whereas the ground state is unique on a closed loop. This topological degeneracy will be stable to small *local* perturbations that respect the $\mathbb{Z}_2$ symmetry. More details on these models may be found in [4].

1. The *transverse field Ising model* is a spin-1/2 model with Hamiltonian:

$$H_S = -J\sum_{j=1}^{N-1}\sigma_j^x\sigma_{j+1}^x - h_z\sum_{j=1}^{N}\sigma_j^z. \tag{16.2}$$

   Here J is the ferromagnetic exchange coupling in the x direction and h_z is a uniform transverse (z) field. This model has a $\mathbb{Z}_2$ symmetry given by a global spin flip in the σ_x basis:

$$P_S = \prod_{j=1}^{N}\sigma_j^z \tag{16.3}$$

2. The *spin-polarized 1-D superconductor* is a fermionic system with Hamiltonian:

$$\begin{aligned} H_F &= \sum_{j=1}^{N-1}\left(-w(a_j^\dagger a_{j+1} + a_{j+1}^\dagger a_j) + \Delta a_j a_{j+1} + \Delta^* a_{j+1}^\dagger a_j^\dagger\right) \\ &\quad -\mu\sum_{j=1}^{N}\left(a_j^\dagger a_j - \frac{1}{2}\right) \end{aligned} \tag{16.4}$$

   where a_j and $a_j^\dagger$ are fermionic annihilation and creation operators, w is the hopping amplitude, Δ is the superconducting gap and μ is the chemical potential. For simplicity, we will assume that $\Delta = \Delta^* = w$, so that

$$H_F = w\sum_{j=1}^{N-1}(a_j - a_j^\dagger)(a_{j+1} + a_{j+1}^\dagger) - \mu\sum_{j=1}^{N}\left(a_j^\dagger a_j - 1/2\right). \tag{16.5}$$

This model has a $\mathbb{Z}_2$ symmetry given by the fermionic parity operator:

$$P_F = (-1)^{\sum_j a_j^\dagger a_j} \tag{16.6}$$

Although the two models are mathematically equivalent, as we will see in Sec. 16.2.2, they are clearly physically different. In particular, for the superconductor, the $\mathbb{Z}_2$ symmetry of fermionic parity cannot be lifted by any local physical operator, as such operators must contain an even number of fermion operators. Unfortunately, for the spin system the degeneracy is lifted by a simple longitudinal magnetic field $h_x \sum_j \sigma_j^x$ and thus the topological phase of the TFIM would be much harder to find in nature.

16.2.1 Nature of topological degeneracy (spin language)

Consider the transverse field Ising model of Eq. (16.2). With no applied field, there are a pair of Ising ground states ($h_z = 0$):

$$|\psi_\rightarrow\rangle \;=\; |\rightarrow\rightarrow\rightarrow\cdots\rightarrow\rangle\,,\; |\psi_\leftarrow\rangle = |\leftarrow\leftarrow\leftarrow\cdots\leftarrow\rangle\,. \tag{16.7}$$

The introduction of a small field h_z allows the spins to flip in the σ^x basis. In particular, tunneling between the two classical ground states arises via a soliton (domain-wall) propagating from one side of the system to the other:

$$|\rightarrow\rightarrow\rightarrow\cdots\rightarrow\rangle \;\longrightarrow\; |\leftarrow:\rightarrow\rightarrow\cdots\rightarrow\rangle \longrightarrow |\leftarrow\leftarrow:\rightarrow\cdots\rightarrow\rangle \tag{16.8}$$

$$\longrightarrow\; |\leftarrow\leftarrow\leftarrow:\cdots\rightarrow\rangle \longrightarrow \cdots \longrightarrow |\leftarrow\leftarrow\leftarrow\cdots\leftarrow\rangle\,. \tag{16.9}$$

As usual, the tunneling amplitude t associated with this transition falls off exponentially in the distance the soliton must propagate

$$t \sim e^{-N/\xi} \tag{16.10}$$

where ξ is the correlation length of the model. The two-fold degeneracy is therefore lifted by the effective Hamiltonian:

$$H_{\text{eff}} = \begin{pmatrix} 0 & -t \\ -t & 0 \end{pmatrix}. \tag{16.11}$$

The splitting is exponentially small in the system size and the two-fold degeneracy is recovered in the thermodynamic limit as expected. Moreover, it is clear why introduction of a longitudinal field h_x will fully split the degeneracy.

16.2.2 Reduction of TFIM to SPSC by the Jordan-Wigner transformation

To show the equivalence of the one dimensional models introduced above, we will use a standard Jordan-Wigner transformation to convert the spins of the Ising model into fermions. It is perhaps not surprising that a fermionic description exists for spin 1/2 systems – we simplify identify the up and down state of each spin with the presence or absence of a fermion. The only difficulty arises in arranging the transformation so that the appropriate (anti)-commutation relations hold in each description. The Jordan-Wigner transformation does this by introducing string-like fermion operators that work out quite nicely in 1-D nearest neighbor models.

To reduce H_S to H_F, we

1. Associate the projection onto the z-axis of the spin with the fermionic occupation number:

$$|\uparrow\rangle \leftrightarrow n = 0, \quad |\downarrow\rangle \leftrightarrow n = 1. \tag{16.12}$$

That is,

$$\sigma_j^z = (-1)^{a_j^\dagger a_j}. \tag{16.13}$$

2. Introduce the string-like annihilation and creation operators

$$\begin{aligned} a_j &= \left(\prod_{k=1}^{j-1} \sigma_k^z\right) \sigma_j^+ \\ a_j^\dagger &= \left(\prod_{k=1}^{j-1} \sigma_k^z\right) \sigma_j^- \end{aligned} \tag{16.14}$$

where σ^+ and σ^- are the usual spin raising and lower operators. At this stage, we can check that the usual fermionic anticommutation relations hold for the $a_j, a_j^\dagger$:

$$\left\{a_i, a_j^\dagger\right\} = \delta_{ij} \tag{16.15}$$

3. Observe that

$$\sigma_j^x \sigma_{j+1}^x = -(a_j - a_j^\dagger)(a_{j+1} + a_{j+1}^\dagger), \tag{16.16}$$

so H_S (Eq. (16.2)) reduces to H_F (Eq. (16.5)) with

$$w = J, \quad \mu = -2h_z \tag{16.17}$$

16.2.3 Majorana operators

Majorana operators provide a convenient alternative representation of Fermi systems when the number of particles is only conserved modulo 2, as in a superconductor. Given a set of N Dirac fermions with annihilation/creation operators $a_j, a_j^\dagger$, we can define a set of $2N$ real Majorana fermion operators as follows:

$$\begin{aligned} c_{2j-1} &= a_j + a_j^\dagger \\ c_{2j} &= \frac{a_j - a_j^\dagger}{i}. \end{aligned} \tag{16.18}$$

These operators are Hermitian and satisfy a fermionic anticommutation relation:

$$\begin{aligned} c_k^\dagger &= c_k \\ c_k^2 &= 1, \quad c_k c_l = -c_l c_k (k \neq l). \end{aligned} \tag{16.19}$$

Or, more compactly,

$$\{c_k, c_l\} = 2\delta_{kl}. \tag{16.20}$$

From any pair of Majorana operators, we can construct an annihilation and creation operator for a standard Dirac fermion ($a = (c_1 + ic_2)/2$ and h.c.), and thus the unique irreducible representation for the pair is a 2-dimensional Hilbert space which is either occupied or unoccupied by the a fermion.

Both models H_S and H_F can be written as

$$H_{\text{maj}} = \frac{i}{2}\left(v \sum_{j=1}^{N} c_{2j-1} c_{2j} + w \sum_{j=1}^{N-1} c_{2j} c_{2j+1}\right) \tag{16.21}$$

where $v = h_z = -\mu/2$ and $w = J$. The $\mathbb{Z}_2$ symmetry of fermionic parity is given in the Majorana language by

$$P_{\text{maj}} = \prod_{k=1}^{N} (-ic_{2k-1} c_{2k}). \tag{16.22}$$

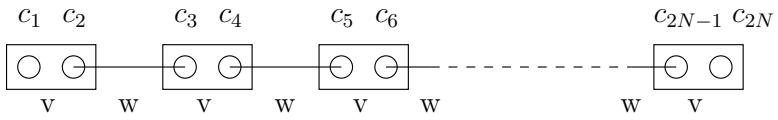


Figure 16.2: Majorana chain representation of 1-d superconductor. Each boxed pair of Majoranas corresponds to one site of the original fermionic chain.

We can view this model graphically as a chain of coupled Majorona modes, two to each of the N sites of the original problem as in Fig. 16.2. If $v = 0$, then the Majorana modes at the ends of the chain are not coupled to anything. This immediately allows us to identify the 2-fold ground state degeneracy in H_{maj} as the tensor factor given by the 2-dimensional representation of the boundary pair c_1, c_{2N}.

We will see in Sec. 16.2.4 that if $v \neq 0$ but $|v| < w$, the operators c_1 and c_{2N} are replaced by some *boundary mode operators* b_l, b_r. The effective Hamiltonian for this piece of the system is then

$$H_{\text{eff}} = \frac{i}{2}\epsilon b_l b_r = \epsilon(a^\dagger a - \frac{1}{2}) \tag{16.23}$$

where $\epsilon \sim e^{-N/\xi}$ and a, $a^\dagger$ are the Dirac fermion operators constructed from the boundary pair. Thus, the ground state degeneracy is lifted by only an exponentially small splitting in system size.

16.2.4 General properties of quadratic fermionic Hamiltonians

We now step back and consider a generic quadratic fermionic Hamiltonian:

$$H(A) = \frac{i}{4}\sum_{j,k} A_{jk} c_j c_k \tag{16.24}$$

where A is a real, skew-symmetric matrix and the c_j are Majorana fermion operators. The normalization $\frac{i}{4}$ is convenient because it has the property that

$$[-iH(A), -iH(B)] = -iH\left([A, B]\right) \tag{16.25}$$

where $A, B \in \mathfrak{so}(2N)$, and $H(A), H(B)$ act on the Fock space $\mathfrak{F}_N = \mathbb{C}^{2^N}$. Thus $H(\cdot)$ provides a natural representation of $\mathfrak{so}(2N)$.

We now bring $H(A)$ to a canonical form:

$$H_{\text{canonical}} = \frac{i}{2}\sum_{k=1}^{m} \epsilon_k b'_k b''_k = \sum_{k=1}^{m} \epsilon_k(\tilde{a}_k^\dagger \tilde{a}_k - \frac{1}{2}) \tag{16.26}$$

where b'_k, b''_k are appropriate real linear combinations of the original c_j satisfying the same Majorana fermion commutation relations and the $\tilde{a}_k, \tilde{a}_k^\dagger$ are the annihilation and creation operators associated to the b'_k, b''_k pair of Majoranas. This form for H follows immediately from the standard block diagonalization of real skew symmetric matrices

$$A = Q \begin{pmatrix} 0 & \epsilon_1 & & & \\ -\epsilon_1 & 0 & & & \\ & & 0 & \epsilon_2 & \\ & & -\epsilon_2 & 0 & \\ & & & & \cdots \end{pmatrix} Q^T, \quad Q \in O(2N), \epsilon_k \geq 0 \tag{16.27}$$

From this form it is easy to check that the eigenvalues of A are $\pm i\epsilon_k$ and that the eigenvectors are the coefficients of c in $\tilde{a}_k$, $\tilde{a}_k^\dagger$.

If some of the ϵ_k vanish, then we refer to the associated fermions as *zero modes*. In particular, these will lead to ground state degeneracies, since occupation or nonoccupation of such modes does not affect the energy. For the Majorana chain of Eq. (16.21), we have

$$A = \begin{pmatrix} 0 & v & & & & \\ -v & 0 & w & & & \\ & -w & 0 & v & & \\ & & -v & 0 & w & \\ & & & -w & 0 & \\ & & & & & \cdots \end{pmatrix} \tag{16.28}$$

We can find a vector u such that $uA = 0$ by inspection:

$$u = (1, 0, \frac{v}{w}, 0, \left(\frac{v}{w}\right)^2, 0, \cdots) \tag{16.29}$$

This vector leads to a left boundary mode

$$b_l = \sum u_k c_k \tag{16.30}$$

while an analogous calculation starting at the right end will find a right boundary mode b_r. These modes form a Majorana canonical pair, leading to a two-fold degeneracy of the ground state of the chain. Clearly, $u_k \sim e^{-k/\xi}$ falls off exponentially from the edges of the chain with correlation length $\xi^{-1} = \ln\left|\frac{w}{v}\right|$, as expected in section 16.2.3.

16.2.5 Why are the boundary modes robust?

In the simple case of a quadratic fermion Hamiltonian, we know that the modes correspond to eigenvalues of a skew-symmetric real matrix. These come in pairs $\pm i\epsilon$, in general, and the case $\epsilon = 0$ is special. In particular, if the pair of Majoranas corresponding to a zero mode are physically well separated, we expect perturbations to have trouble lifting the boundary degeneracy.

More generally, for interacting fermions, we can extend the symmetry group $\mathbb{Z}_2$, generated by $P = P_{\text{maj}}$, to a *non-commuting* algebra acting on the the ground state space $\mathfrak{L}$. First, in the noninteracting limit, at $v = 0$, we define

$$X = Y \prod_{k=1}^{j} (-ic_{2k-1}c_{2k}) \tag{16.31}$$

where $Y = c_{2j+1}$ is a local Majorana operator at site $2j + 1$. A straightforward calculation shows that

$$XP = -PX \tag{16.32}$$

and that $[H, X] = 0$ so that the algebra generated by X, P acts on $\mathfrak{L}$ nontrivially. We now allow Y to vary as we adiabatically turn on interactions and, so long as an energy gap is maintained, we expect Y to remain a local operator near $2j$, which we can separate from the boundary by suitably large choice of j. That is, to find Y, one needs to know the ground state or at least the structure of the ground state near $2j$. This is a nontrivial operation but see [3] for more details.

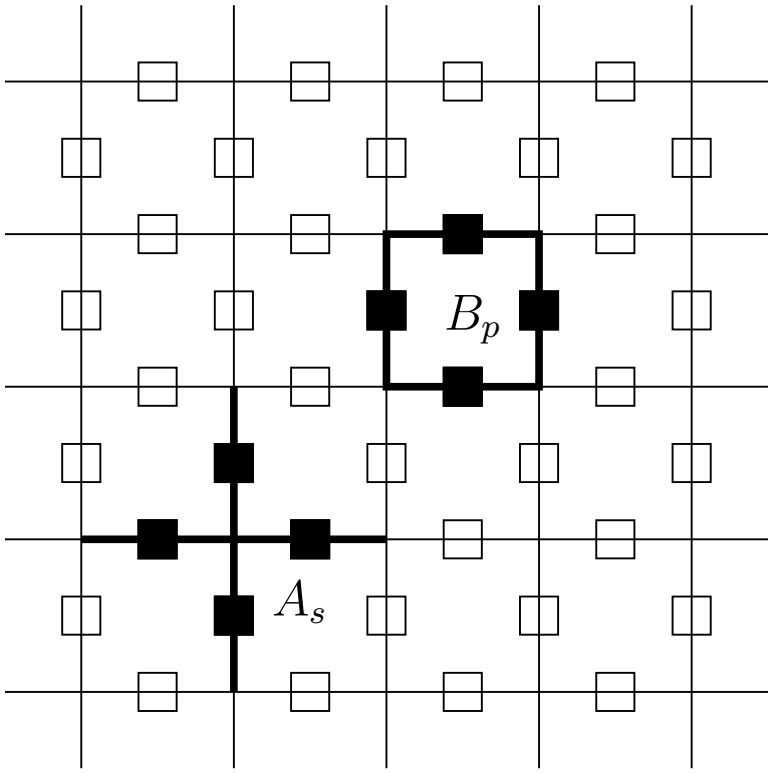


Figure 16.3: A piece of the toric code. The spins live on the edges of the square lattice. The spins adjacent to a star operator A_s and a plaquette operator B_p are shown.

16.3 The two-dimensional toric code

The toric code is an exactly solvable spin 1/2 model on the square lattice. It exhibits a ground state degeneracy of 4^g when embedded on a surface of genus g and a quasiparticle spectrum with both bosonic and fermionic sectors. Although we will not introduce it as such, the model can be viewed as an Ising gauge theory at a particularly simple point in parameter space (see Sec. 16.4.5). Many of the topological features of the toric code model were essentially understood by [8], but they did not propose an exactly solved model. A more detailed exposition of the toric code may be found in [5].

We consider a square lattice, possibly embedded into a nontrivial surface such as a torus, and place spins on the edges, as in Fig. 16.3. The Hamiltonian is given by

$$H_T = -J_e \sum_s A_s - J_m \sum_p B_p \tag{16.33}$$

where s runs over the vertices (stars) of the lattice and p runs over the plaquettes. The star operator acts on the four spins surrounding a vertex s,

$$A_s = \prod_{j \in \mathrm{star}(s)} \sigma_j^x \tag{16.34}$$

while the plaquette operator acts on the four spins surrounding a plaquette,

$$B_p = \prod_{j \in \partial p} \sigma_j^z. \tag{16.35}$$

Clearly, the A_s all commute with one another, as do the B_p. Slightly less trivially,

$$A_s B_p = B_p A_s \tag{16.36}$$

because any given star and plaquette share an even number of edges (either none or two) and therefore the minus signs arising from the commutation of σ^x and σ^z on those edges cancel. Since all of the terms of H_T commute, we expect to be able to solve it term by term.

In particular, we will solve H_T working in the σ^z basis. Define classical variables $s_j = \pm 1$ to label the σ^z basis states. For each classical spin configuration $\{s\}$, we can define the plaquette flux

$$w_p(s) = \prod_{j \in \partial p} s_j. \tag{16.37}$$

If $w_p = -1$, we say that there is a *vortex* on plaquette p.

16.3.1 Ground states

To find the ground states $|\Psi\rangle$ of H_T, we need to minimize the energy, which means maximize the energy of each of the A_s and B_p terms. The plaquette terms provide the condition

$$B_p |\Psi\rangle = |\Psi\rangle \tag{16.38}$$

which holds if and only if

$$|\Psi\rangle = \sum_{\{s: w_p(s)=1 \ \forall p\}} c_s |s\rangle \tag{16.39}$$

. That is, the ground state contains no vortices. The group of star operators act on the configurations s by flipping spins. Thus, the star conditions

$$A_s |\Psi\rangle = |\Psi\rangle \tag{16.40}$$

hold if and only if *all of the c_s are equal for each orbit of the action of star operators*. In particular, if the spin flips of A_s are ergodic, as they are on the plane, all c_s must be equal and the ground state is uniquely determined.

On the torus, the star operators preserve the *cohomology class* of a vortex-free spin configuration. In more physical terms, we can define conserved numbers given by the Wilson loop like functions

$$w_l(s) = \prod_{j \in l} s_j, \quad l = l_1, l_2 \tag{16.41}$$

where l_1 and l_2 are two independent non-trivial cycles on the square lattice wrapping the torus (Fig. 16.4). Any given star will overlap with a loop l in either zero or two edges and therefore A_s preserves w_l. Since there are two independent loops on the torus, each of which can have $w_l = \pm 1$, there is a four-fold degenerate ground state:

$$|\Psi\rangle = \sum_{\{s: w_p(s)=1 \ \forall p\}} c_{w_{l_1} w_{l_2}} |s\rangle . \tag{16.42}$$

16.3.2 Excitations

The excitations of the toric code come in two varieties: the *electric charges* and *magnetic vortices* of a $\mathbb{Z}_2$ gauge theory. We will see this connection more explicitly later. In the following, we restrict attention to the planar system for simplicity.

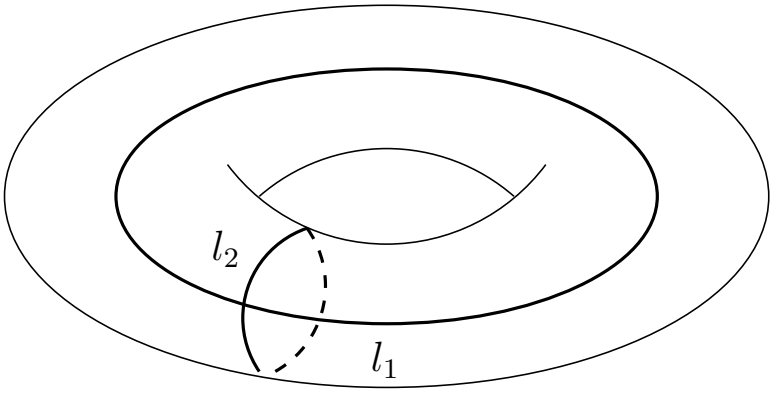


Figure 16.4: Large cycles on the torus.

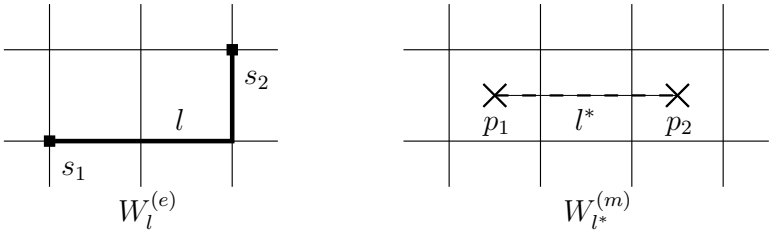


Figure 16.5: Electric and magnetic path operators.

To find the electric charges, let us define the electric path operator

$$W_l^{(e)} = \prod_{j \in l} \sigma_j^z \tag{16.43}$$

where l is a path in the lattice going from s_1 to s_2 (see Fig. 16.5). This operator clearly commutes with the plaquette operators B_p and with all of the star operators A_s except for at the end points s_1 and s_2, where only one edge overlaps between the star and the path and we have

$$W_l^{(e)} A_{s_1} = -A_{s_1} W_l^{(e)}. \tag{16.44}$$

Therefore, the state

$$|\Psi_{s_1,s_2}\rangle = W_l^{(e)} |\Psi_0\rangle , \tag{16.45}$$

where $|\Psi_0\rangle$ is the planar ground state, is an eigenstate of the Hamiltonian with excitations (charges) at s_1 and s_2 that each cost energy $2J_e$ to create relative to the ground state.

An analogous construction will find the magnetic vortices: we can define a dual path operator

$$W_{l^*}^{(m)} = \prod_{j \in l^*} \sigma_j^x \tag{16.46}$$

where the path l^* lies in the dual lattice (see Fig. 16.5) and goes from p_1 to p_2. In this case, the stars A_s all commute with $W_{l^*}^{(m)}$, as do all of the plaquette operators B_p except the two at the end points of l^*, which anticommute. Thus, the $W_{l^*}^{(m)}$ operator creates a pair of magnetic vortices on the plaquettes p_1 and p_2 at an energy of $2J_m$ each.

16.4 Abelian anyons and quasiparticle statistics

Let us discuss what can possibly happen if we exchange two particles in two dimensions. To ensure that particle statistics is well-defined, we assume that there is no long-range interaction

and that the phase is gapped. If we drag two particles around one another adiabatically,

then we expect both dynamical phase accumulation and a statistical effect due to the exchange. We are well acquainted with this effect for everyday bosons and fermions, for which:

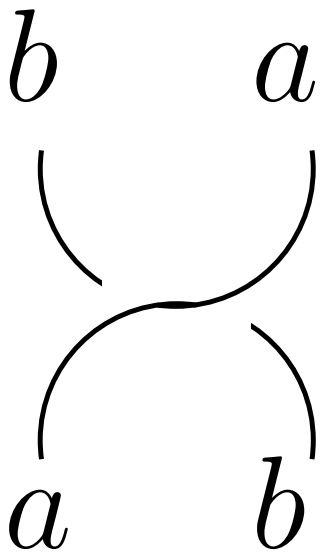
$$\begin{array}{lrcl} \text{Bosons:} & |\Psi\rangle & \mapsto & |\Psi\rangle \\ \text{Fermions:} & |\Psi\rangle & \mapsto & -|\Psi\rangle \end{array} \tag{16.47}$$

where we have dropped the dynamical phase so as to focus on the statistics. In both of these standard cases, a full rotation (two exchanges),

leaves $|\Psi\rangle$ unchanged.

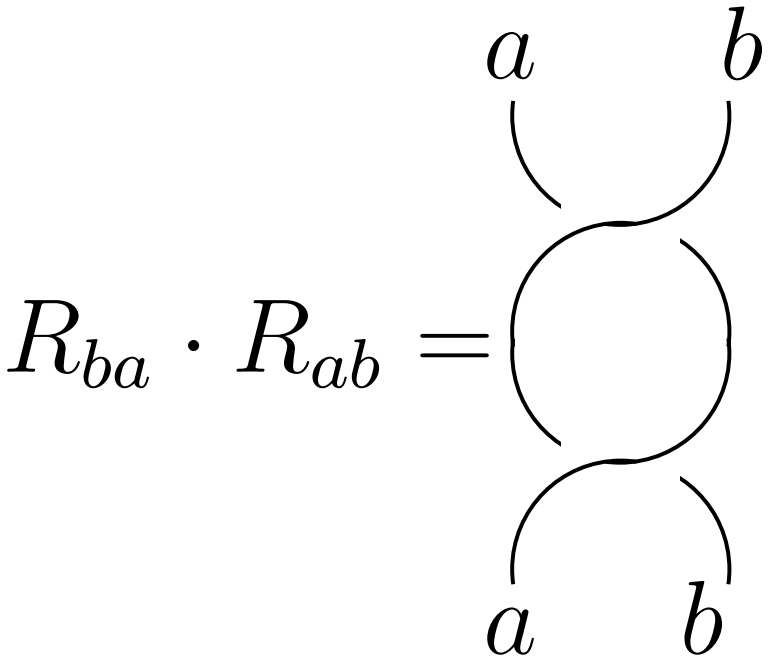
In principle,

$$R_{ab} = \tag{16.48}$$



is an arbitrary phase factor or even an operator (*braiding operator*). If the two particles are

distinguishable ($a \neq b$), then R_{ab} does not have an invariant meaning, but the *mutual statistics*

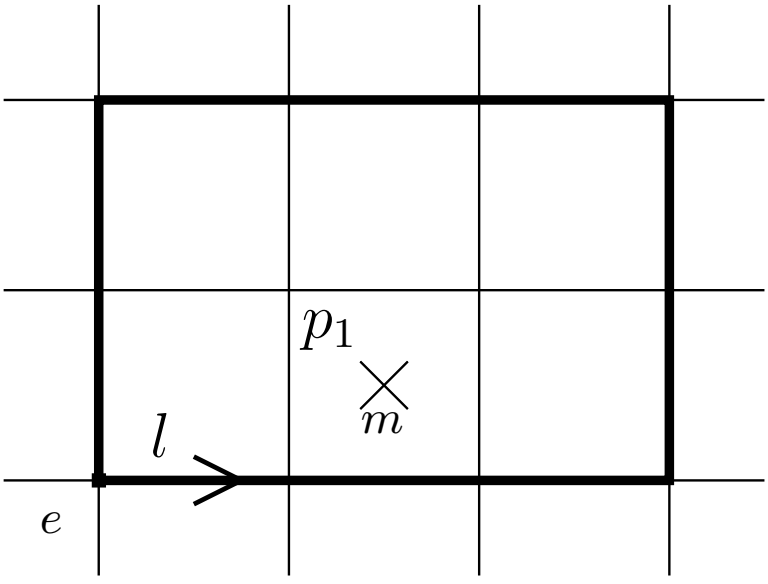


(16.49)

does.

Let us illustrate this in the toric code model. In section 16.3.2 we found two kinds of quasiparticle excitations in the toric code: electric charges (e) and magnetic vortices (m). Since path operators of the same type commute with one another, it is easy to show that each of these are bosons. However, they have nontrivial mutual statistics.

To calculate the mutual statistics, consider taking a charge e around a vortex m.



Let $|\xi\rangle$ be some state containing a magnetic vortex at p_1. Under the full braiding operation,

$$\begin{aligned} |\xi\rangle &\mapsto \left(\prod_{j\in l} \sigma_j^z\right) |\xi\rangle \\ &= \left(\prod_{p \text{ inside } l} B_p\right) |\xi\rangle \end{aligned} \tag{16.50}$$

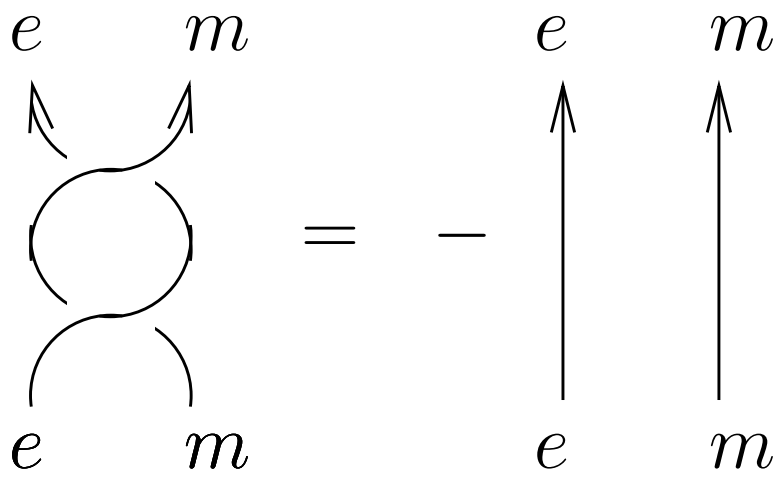
where the second line is a Stokes' theorem like result relating the product around a loop to the products of internal loops. Since

$$B_{p_1} |\xi\rangle = - |\xi\rangle \tag{16.51}$$

for the plaquette p_1 containing the vortex, we have that

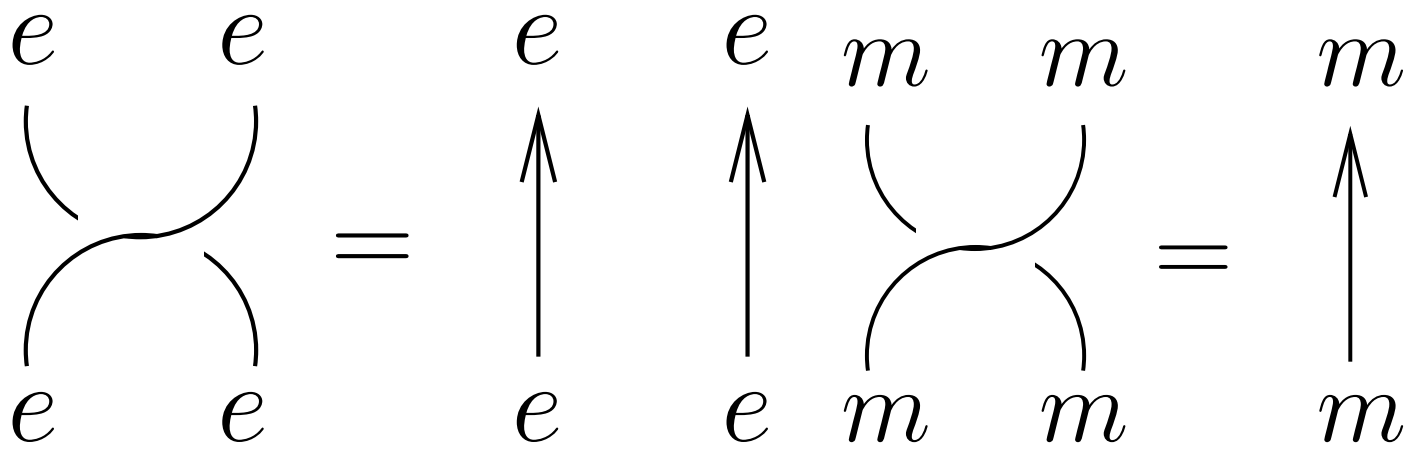
$$|\xi\rangle \mapsto - |\xi\rangle \,, \tag{16.52}$$

or



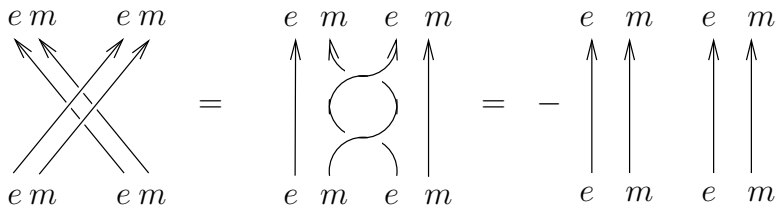
(16.53)

Using the bosonic self-statistics equations,



(16.54)

we can derive the nontrivial corollary that composite $e - m$ particles are fermions:



(16.55)

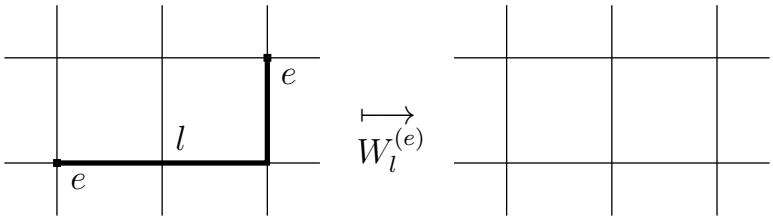
16.4.1 Superselection sectors and fusion rules

Initially, we exhibited two kinds of bosonic excitations in the toric code model (charges e and vortices m) in the solution of the Hamiltonian. After a bit of work, we discovered that a composite $e - m$ object has a meaningful characterization within the model as well, at least in that it has fermionic statistics. This begs the question, how many particle types exist in the toric code model and how can we identify them?

We take an algebraic definition of a particle type: each type corresponds to a *superselection sector*, which is a representation of the local operator algebra. In particular, we say that two particles (or composite objects) are *of the same type*

$$a \sim b \tag{16.56}$$

if a can be transformed to b by some operator acting in a finite region. For example, in the toric code, two e-particles are equivalent to having no particles at all,



(16.57)

by acting with an appropriate, geometrically bounded electric path operator $W_l^{(e)}$.

We introduce the notation

$$e \times e = 1 \tag{16.58}$$

to represent the *fusion rule* that two e-particles are equivalent to the vacuum sector 1. In the toric code, there are 4 superselection sectors:

$$1,\ e,\ m,\ \text{and}\ \epsilon = e \times m \tag{16.59}$$

with the fusion rules:

$$\begin{array}{ll} e \times e = 1 & e \times m = \epsilon \\ m \times m = 1 & e \times \epsilon = m \\ \epsilon \times \epsilon = 1 & m \times \epsilon = e \end{array} \tag{16.60}$$

16.4.2 Mutual statistics implies degeneracy on the torus

This is an argument due to [1]. Suppose that there are at least two particle types, e and m with -1 mutual statistics. Let us define an operator Z acting on the ground state in an abstract fashion (not refering to the actual model) which creates an e pair, wraps one particle around the torus and annihilates the pair. In the toric code, this will be the path operator $W_l^{(e)} = \prod_{j \in l} \sigma_j^z$ for a loop l winding one of the nontrivial cycles on the torus, but we need not know that specifically.

We can define another operator X that creates a pair of the other type m and winds around the other nontrivial cycle on the torus. But now a bit of geometric introspection reveals that the combination,

$$Z^{-1}X^{-1}ZX = \quad \textcircled{m} \quad \textcircled{e} \quad = -1 \tag{16.61}$$

Thus, there are two non-commuting operators acting on the ground state space $\mathfrak{L}$, and we conclude dim $\mathfrak{L} > 1$. In fact, there are four such operators, each of the two particle types can be moved around each of the two nontrivial cycles. Working out the commutation relations of these operators implies that dim $\mathfrak{L} = 4$.

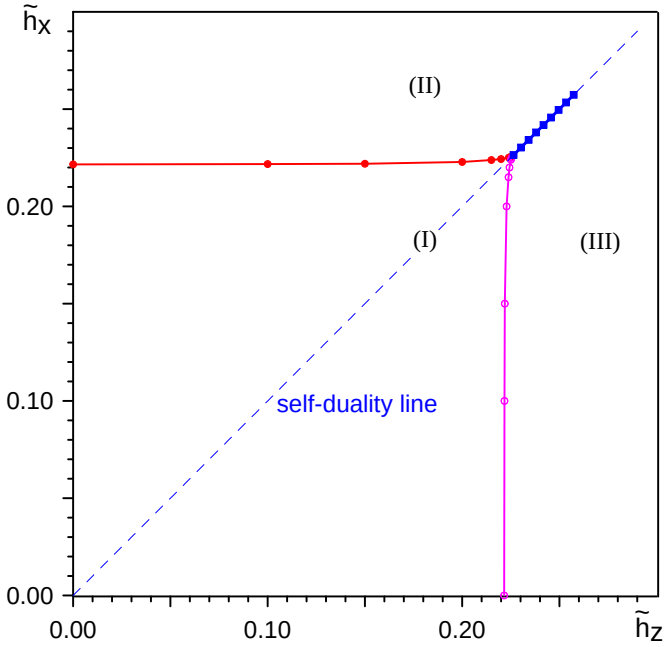


Figure 16.6: Numerically determined phase diagram of the toric code in a field from [9]. (I) labels the topological phase, (II) and (III) the vortex and charge condensates (*i.e.* the paramagnetic phase). The numerics were done using discrete imaginary time with a rather large quantization step.

16.4.3 The toric code in a field: perturbation analysis

We now apply a magnetic field to the toric code that will realistically allow the quasiparticles to hop and, unfortunately, destroy its exact solvability (see [9]). To wit:

$$H = -J_e \sum_s A_s - J_m \sum_p B_p - \sum_j \left(h_x \sigma_j^x + h_z \sigma_j^z \right) \tag{16.62}$$

For example, with $h_x = 0$ but $h_z \neq 0$, we can view the perturbation as an electric path operator of length 1 on each edge. Hence, it can cause charge pair creation and annihilation (at an energy cost $\sim 4J_e$) or hop existing charges by one lattice displacement, at no cost. For small h_z this provides a nontrivial tight-binding dispersion to the charges,

$$\epsilon(q) \approx 2J_e - 2h_z(\cos q_x + \cos q_y) \tag{16.63}$$

but does not close the gap or lead to a change in the topological degeneracy of the ground state in the thermodynamic limit.

At large $h_z \gg J_e, J_m$, the model should simply align with the applied field as a paramagnet. Clearly, in this limit the topological degeneracy has been destroyed and we have a unique spin-polarized ground state. The phase transition can be understood from the topological side as a bose condensation of the charges, which proliferate as h_z increases.

The same argument is applicable if $h_x \gg J_e, J_m$. If h_x increases while $h_z = 0$, then vortices condense. However, the high-field phase is just a paramagnet, so one can continuously rotate the field between the x- and z-direction without inducing a phase transition. Thus, the charge and vortex condensates are actually the same phase! This property was first discovered by [2] for a 3D classical $\mathbb{Z}_2$ gauge Higgs model, where it appears rather mysterious.

16.4.4 Robustness of the topological degeneracy

The splitting of the ground state levels due to virtual quasiparticle tunneling is given by

$$\delta E \sim \Delta e^{-L/\xi} \tag{16.64}$$

This follows from the effective Hamiltonian

$$H_{\text{eff}} = -(t_{1Z}Z_1 + t_{2Z}Z_2 + t_{1X}X_1 + t_{2X}X_2) \tag{16.65}$$

where the Z_i, X_i operators are the winding loop operators of Sec. 16.4.2. Physically, this is simply a statement of the fact that the only way to act upon the ground state is to wind quasiparticles around the torus. This is a process exponentially suppressed in system size.

16.4.5 Emergent symmetry: gauge formulation

There are two ways to introduce symmetry operators in the perturbed toric code model.

1. One can define *loop operators* (e.g. Z_1, Z_2, X_1, X_2), the definition of which depends on the actual ground state of the perturbed Hamiltonian. This is similar to the definition of the operator Y in the 1D case of Sec. 16.2.5, which also requires detailed knowledge of the ground state.

2. One can exploit *gauge invariance* by rewriting the model in a gauge invariant form. This can be done for any spin model by introducing redundancy. In this case, the symmetry does not depend on the model but is only manifest in the topological phase.

We will take the second approach in order to avoid the difficulty of defining the appropriate loop operators and also to introduce the important gauge formulation of the model. To gauge the model we proceed in steps:

1. Introduce one extra spin μ_v per vertex that always remains in the state

$$\frac{1}{\sqrt{2}}\left(|\uparrow\rangle + |\downarrow\rangle\right). \tag{16.66}$$

   This state is characterized by the condition

$$\mu_v^x |\Psi\rangle = |\Psi\rangle, \tag{16.67}$$

   where μ_v^x is the Pauli spin matrix for the spin μ at vertex v.

2. Change spin operators from σ_{uv}, μ_v to $\tilde{\sigma}_{uv}, \tilde{\mu}_v$ where we represent the classical value of each old spin s_{uv} as $\tilde{m}_u \tilde{s}_{uv} \tilde{m}_v$. Here s_{uv} is the spin on the edge connecting u and v and m_u, m_v are the classical values of the new spins (*i.e.* the labels in the μ^z basis).

Thus the complete transformation is given by

$$\begin{aligned}
\sigma_{uv}^z &= \tilde{\mu}_u^z \tilde{\sigma}_{uv}^z \tilde{\mu}_v^z \\
\sigma_{uv}^x &= \tilde{\sigma}_{uv}^x \\
\mu_u^z &= \tilde{\mu}_u^z \\
\mu_u^x &= \tilde{\mu}_u^x \prod_{j \in \text{star}(u)} \tilde{\sigma}_j^x = \tilde{\mu}_u^x \tilde{A}_u
\end{aligned} \tag{16.68}$$

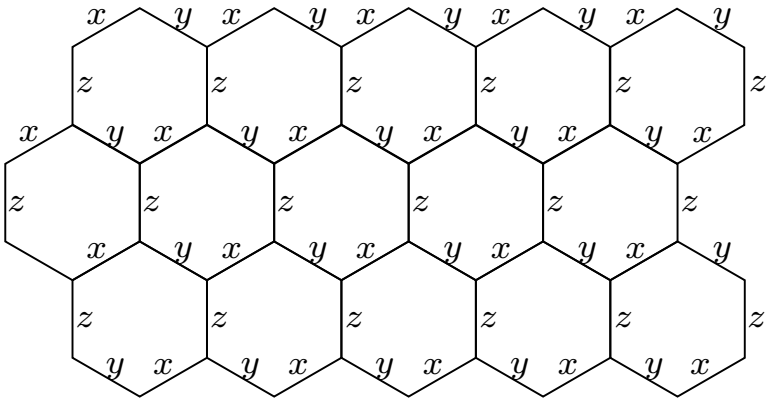


Figure 16.7: The honeycomb model has spins living on the vertices of a honeycomb lattice with nearest neighbor interactions that are link-orientation dependent. x-links have $\sigma^x\sigma^x$ interactions, y-links have $\sigma^y\sigma^y$ interactions and z-links have $\sigma^z\sigma^z$ interactions.

and the constraint Eq. (16.67) becomes the standard $\mathbb{Z}_2$ gauge constraint:

$$\tilde{\mu}_u^x \tilde{A}_u \left|\Psi\right\rangle = \left|\Psi\right\rangle . \tag{16.69}$$

On states satisfying the gauge constraint Eq. (16.69), $A_u = \tilde{A}_u = \tilde{\mu}_u^x$. Therefore,

$$A_u \left|\Psi\right\rangle = \tilde{\mu}_u^x \left|\Psi\right\rangle \tag{16.70}$$

and we can rewrite the Hamiltonian as

$$H = -J_e \sum_v \tilde{\mu}_v^x - J_m \sum_p \tilde{B}_p - \sum_{\langle u,v\rangle} (h_x \tilde{\sigma}_{uv}^x + h_z \tilde{\mu}_u \tilde{\sigma}_{uv}^z \tilde{\mu}_v) \tag{16.71}$$

subject to the gauge constraint.

Viewed as a standard $\mathbb{Z}_2$ gauge theory, the protected topological degeneracy of the ground state is physically familiar as the protected degeneracy associated with the choice of flux threading the $2g$ holes of the genus g surface.

16.5 The honeycomb lattice model

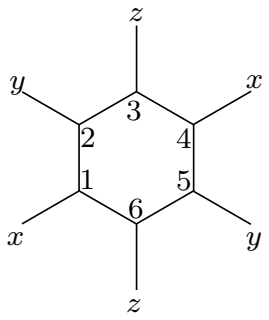
We now investigate the properties of another exactly solvable spin model in two dimensions, the *honeycomb lattice model*. This model exhibits a number of gapped phases that are perturbatively related to the toric code of the previous sections. Moreover, in the presence of time-reversal symmetry breaking terms, a new topological phase arises with different topological properties, including nontrivial *spectral Chern number*. An extended treatment of the properties of this model with much greater detail can be found in [6].

In the honeycomb lattice model, the degrees of freedom are spins living on the vertices of a honeycomb lattice with nearest neighbor interactions. The unusual feature of this model is that the interactions are link orientation dependent (see Fig. 16.7). The Hamiltonian is

$$H = -J_x \sum_{x \text{ links}} \sigma_j^x \sigma_k^x - J_y \sum_{y \text{ links}} \sigma_j^y \sigma_k^y - J_z \sum_{z \text{ links}} \sigma_j^z \sigma_k^z \tag{16.72}$$

We might expect this model to be integrable because $[H, W_p] = 0$ for an extensive collection of

plaquette operators



$$W_p = \sigma_1^x \sigma_2^y \sigma_3^z \sigma_4^x \sigma_5^y \sigma_6^z \tag{16.73}$$

where the spins and labels follow from the figure for each plaquette. Unfortunately, this is not quite enough: there are two spins but only one constraint per hexagon so that half of each spin remains unconstrained. In fact, the remaining degrees of freedom are Majorana operators!

16.5.1 A (redundant) representation of a spin by 4 Majorana operators

We consider a collection of four Majorana operators c, b^x, b^y and b^z that act on the 4-dimensional Fock space $\mathfrak{F}$. We define the following three operators

$$\begin{aligned} \tilde{\sigma}^x &= ib^x c \\ \tilde{\sigma}^y &= ib^y c \\ \tilde{\sigma}^y &= ib^y c. \end{aligned} \tag{16.74}$$

These operators do not obey the spin algebra relations on the full Fock space, but we clearly have two extra dimensions of wiggle room. In fact, the physical state space is identified with a two-dimensional subspace $\mathfrak{L} \subset \mathfrak{F}$ given by the constraint

$$D\,|\Psi\rangle = |\Psi\rangle\,, \qquad \text{where } D = b^x b^y b^z c \tag{16.75}$$

Within $\mathfrak{L}$, the $\tilde{\sigma}^\alpha$ act as σ^α act on the actual spin. Of course, $\tilde{\sigma}^\alpha$ also act on $\mathfrak{L}^\perp$, but we can ignore these states by enforcing the constraint.

To be careful, we need to check two consistency conditions:

1. $\tilde{\sigma}^\alpha$ preserves the subspace $\mathfrak{L}$, which follows from $[\tilde{\sigma}^\alpha, D] = 0$.

2. The $\tilde{\sigma}^\alpha$ satisfy the correct algebraic relations when restricted to $\mathfrak{L}$. For example,

$$\tilde{\sigma}^x \tilde{\sigma}^y \tilde{\sigma}^z = (ib^x c)(ib^y c)(ib^z c) = i^3(-1) b^x b^y b^z c^3 = iD = i \tag{16.76}$$

   where the last equality only holds in the physical subspace $\mathfrak{L}$.

16.5.2 Solving the Honeycomb Model using Majoranas

We now use the Majorana representation of spins just introduced to rewrite each spin of the entire honeycomb model as in Fig. 16.8. This will greatly expand the 2^N-dimensional Hilbert space to the Fock space $\mathfrak{F}$ of dimension 2^{2N}, but the physical space $\mathfrak{L} \subset \mathfrak{F}$ is fixed by the gauge condition

$$D_j\,|\Psi\rangle = |\Psi\rangle \quad \text{for all } j \tag{16.77}$$

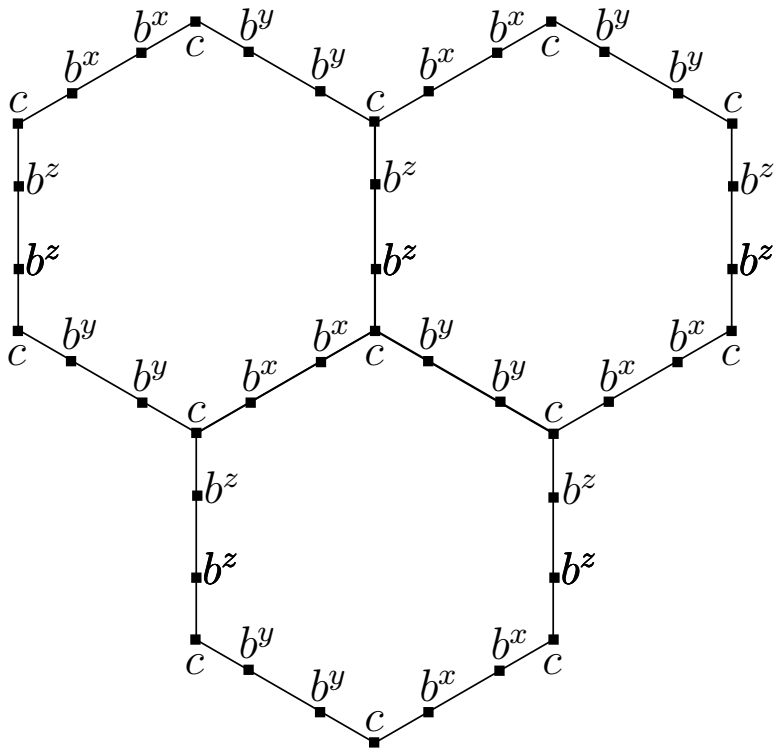


Figure 16.8: Majorana representation of honeycomb model.

where $D_j = b_j^x b_j^y b_j^z c$. We define a projector onto $\mathfrak{L}$ by

$$\Pi_{\mathfrak{L}} = \prod_j \left(\frac{1 + D_j}{2} \right) \tag{16.78}$$

In the Majorana representation, the Hamiltonian (16.72) becomes

$$\begin{aligned} \tilde{H} &= \frac{i}{4} \sum_{\langle j,k \rangle} \hat{A}_{jk} c_j c_k \\ \hat{A}_{jk} &= 2 J_{\alpha(j,k)} \hat{u}_{jk} \\ \hat{u}_{jk} &= i b_j^{\alpha(j,k)} b_k^{\alpha(j,k)} \end{aligned} \tag{16.79}$$

where $\alpha(j,k) = x, y, z$ is the direction of the link between j and k.

We have suggestively written the Hamiltonian $\tilde{H}$ as if it were a simple quadratic fermion Hamiltonian as in Sec. 16.2.4, but of course $\hat{A}_{jk}$ is secretly an operator rather than a real skew-symmetric matrix. However, each operator b_j^α enters only one term of the Hamiltonian and therefore $\hat{u}_{jk}$ commute with each other and with $\tilde{H}$! Thus, we can fix $u_{jk} = \pm 1$, defining an orthogonal decomposition of the full Fock space:

$$\mathfrak{F} = \bigoplus_u \mathfrak{F}_u, \quad \text{where } |\Psi\rangle \in \mathfrak{F}_u \text{ iff } \hat{u}_{jk} |\Psi\rangle = u_{jk} |\Psi\rangle \quad \forall\ j,k \tag{16.80}$$

Within each subspace $\mathfrak{F}_u$, we need to solve the quadratic Hamiltonian

$$\begin{aligned} \tilde{H}_u &= \frac{i}{4} \sum_{\langle j,k \rangle} A_{jk} c_j c_k \\ A_{jk} &= 2 J_{\alpha(j,k)} u_{jk} \end{aligned} \tag{16.81}$$

which we know how to do in principle. On the other hand, the integrals of motion W_p (the hexagon operators) define a decomposition of the physical subspace $\mathfrak{L}$ labeled by the eigenvalues $w_p = \pm 1$:

$$\mathfrak{L} = \bigoplus_w \mathfrak{L}_w, \quad \text{where } |\Psi\rangle \in \mathfrak{L}_w \text{ iff } W_p |\Psi\rangle = w_p |\Psi\rangle \quad \forall\ p \tag{16.82}$$

We can relate these two decompositions by expressing W_p in the Majorana representation and noting that within the physical subspace

$$\tilde{W}_p = \prod_{\langle j,k\rangle \in \partial p} \hat{u}_{jk} \tag{16.83}$$

Thus, we find

$$\mathfrak{L}_w = \Pi_{\mathfrak{L}} \mathfrak{F}_u \tag{16.84}$$

where $w_p = \prod_{(j,k)\in\partial p} u_{jk}$.

So we have a procedure for finding the ground state of the honeycomb model:

1. Fix $w_p = \pm 1$ for all p.
2. Find u_{jk} satisfying
$$w_p = \prod_{(j,k)\in\partial p} u_{jk}. \tag{16.85}$$
There is a small subtletly here in that $u_{jk} = -u_{kj}$ so we must be careful about ordering. We can consistently take j in the even sublattice of the honeycomb and k in the odd sublattice in equation (16.85).
3. Solve for the ground state of the quadratic Hamiltonian (16.81), finding the energy $E(w)$.
4. Project the found state onto the physical subspace (*i.e.* symmetrize over gauge transformations).
5. Repeat for all w; pick the w that minimizes the energy.

If there were no further structure to $E(w)$, this would be an intractable search problem in the space of w_p. Fortunately, due to a theorem by Lieb 1994, the ground state has no vortices. That is,

$$E(w) = \min \text{ if } w_p = 1\ \forall\ p \tag{16.86}$$

Using this choice of w_p, it is easy to solve the model and produce the phase diagram of Fig. 16.9. The gapless phase has two Dirac points in the fermionic spectrum.

16.5.3 Fermionic spectrum in the honeycomb lattice model

We just need to diagonalize the Hamiltonian

$$\begin{aligned} \tilde{H}_u &= \frac{i}{4} \sum_{\langle j,k\rangle} A_{jk} c_j c_k \\ A_{jk} &= 2 J_{\alpha(j,k)} u_{jk} \\ u_{jk} &= \begin{cases} +1 & \text{if } j \in \text{even sublattice} \\ -1 & \text{otherwise} \end{cases} \end{aligned} \tag{16.87}$$

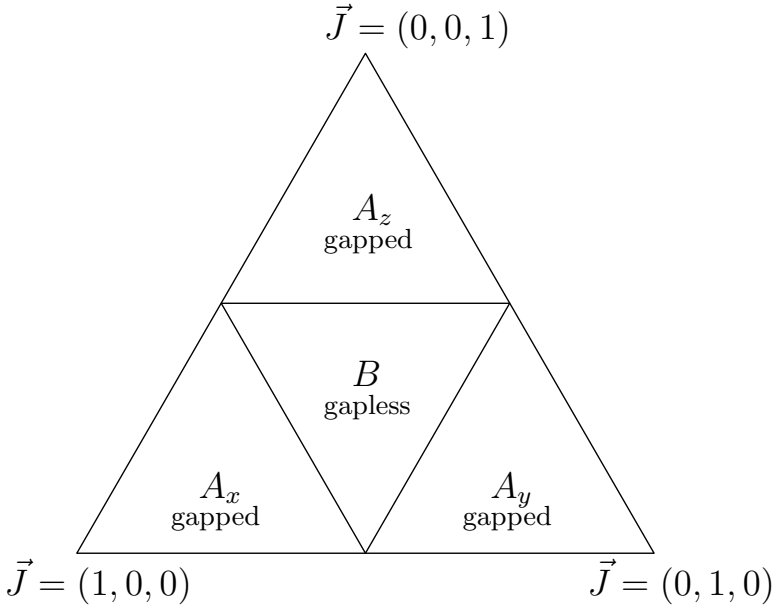


Figure 16.9: Phase diagram of honeycomb model. This is a slice through the positive octant in $\vec{J}$ coupling space along the $J_x + J_y + J_z = 1$ plane. The other octants are analogous.

Figure 16.10: Direct and reciprocal lattices of the honeycomb. The points $\pm\vec{q}_*$ are the two Dirac points of the gapless phase B.

This is equivalent to finding the eigenvalues and eigenvectors of the matrix iA. Since the honeycomb lattice has two sites per unit cell, by applying the Fourier transform we get a 2×2 matrix $A(\vec{q})$:

$$\begin{aligned} iA(\vec{q}) &= \begin{pmatrix} 0 & if(\vec{q}) \\ -if(\vec{q}) & 0 \end{pmatrix} \\ \epsilon(\vec{q}) &= \pm|f(\vec{q})| \end{aligned} \tag{16.88}$$

where $f(\vec{q})$ is some complex function that depends on the couplings J_x, J_y, J_z. In the gapless phase (phase B in Fig. 16.9), $f(\vec{q})$ has two zeros which correspond to Dirac points (see Fig. 16.10). At the transition to phase A, the Dirac points merge and disappear.

16.5.4 Quasiparticle statistics in the gapped phase

It appears that there are two particle types: fermions and vortices (hexagons with $w_p = -1$). The vortices are associated with a $\mathbb{Z}_2$ gauge field, where u_{jk} plays the role of vector potential. Taking a fermion around a vortex results in the multiplication of the state by -1 (compared to the no-vortex case). However, the details such as the fusion rules are not obvious.

Let us look at the model from a different perspective. If $J_x = J_y = 0, J_z > 0$, the system is just a set of dimers (see Fig. 16.11). Each dimer can be in two states: $\uparrow\uparrow$ and $\downarrow\downarrow$. The other two states have $2J_z$ higher energy. Thus, the ground state is highly degenerate.

If $J_x, J_y \ll J_z$, we can use perturbation theory relative to the noninteracting dimer point.

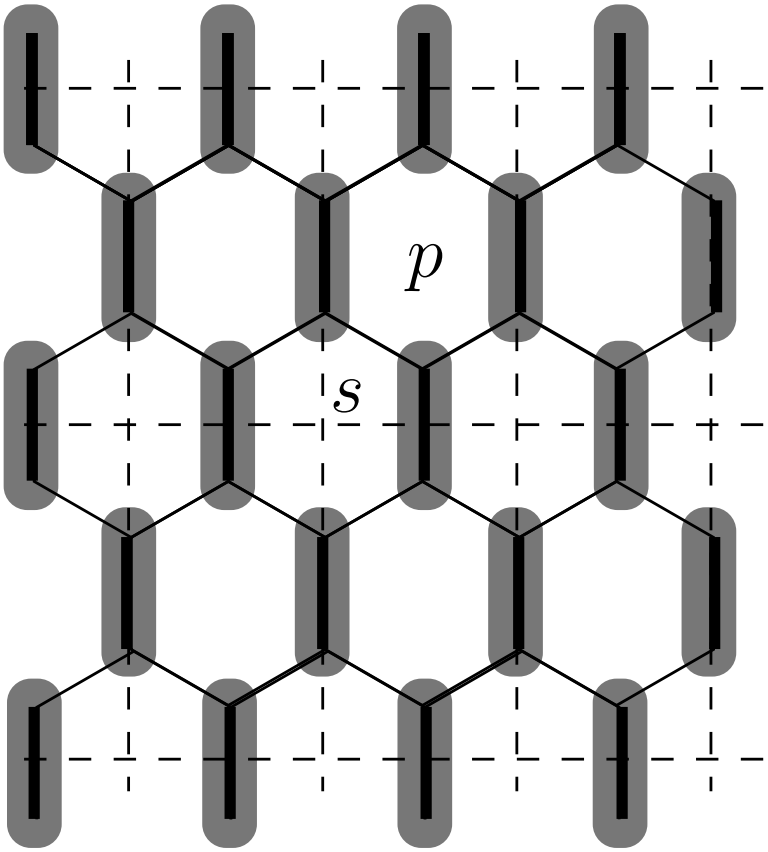


Figure 16.11: The vertical dimers on the honeycomb lattice themselves form the edges of a (dashed) square lattice. The plaquettes of alternate rows of the hexagonal lattice correspond to the stars and plaquettes of the square lattice. This is *weak breaking of translational symmetry.*

Let us characterize each dimer by an effective spin:

$$|\Uparrow\rangle = |\uparrow\uparrow\rangle\,; \qquad |\Downarrow\rangle = |\downarrow\downarrow\rangle\,. \tag{16.89}$$

At 4th order of perturbation theory, we get:

$$H_{\text{eff}}^{(4)} = \text{const} - \frac{J_x^2 J_y^2}{16 J_z^3} \sum_p Q_p \tag{16.90}$$

where p runs over the square plaquettes of the dimer lattice (see Fig. 16.11) and

$$Q_p = \sigma_{p_1}^y \sigma_{p_2}^x \sigma_{p_3}^y \sigma_{p_4}^x \tag{16.91}$$

is a plaquette operator on the effective spin space $|\Uparrow\rangle$, $|\Downarrow\rangle$. By adjusting the unit cell and rotating the spins, we can reduce this Hamiltonian to the toric code!

The vertices and plaquettes of the new lattice correspond to alternating rows of hexagons. Thus, vortices on even rows belong to one superselection sector and vortices on odd rows to the other. It is impossible to move a vortex from an even row to an odd row by a local operator without producing other particles (*e.g.* fermions). The fermions and $e-m$ pairs belong to the same superselection sector, ϵ, though these are different physical states.

16.5.5 Nonabelian phase

In the gapless phase B, vortex statistics are not well-defined. However, a gap can be opened by applying a perturbation that breaks the time-reversal symmetry, such as a magnetic field. Unfortunately the honeycomb model in a field is not exactly solvable. [10] studied an exactly solvable spin model where the time-reversal symmetry is spontaneously broken, but we will satisfy ourselves by introducing a T-breaking next nearest neighbor interaction on the fermionic level (which can be represented by a 3-spin interaction in the original spin language).

Written in terms of Majorana fermions, we consider the Hamiltonian

$$H = \frac{i}{4} \sum_{\langle j,k \rangle} A_{jk} c_j c_k \tag{16.92}$$

where A_{jk} now has chiral terms connecting Majoranas beyond nearest neighbor in the honeycomb lattice (see Fig. 16.12). After Fourier transforming, we find

$$iA(\vec{q}) = \begin{pmatrix} \Delta(\vec{q}) & if(\vec{q}) \\ -if(\vec{q}) & -\Delta(\vec{q}) \end{pmatrix} \tag{16.93}$$

with the massive dispersion relation

$$\epsilon(\vec{q}) = \pm\sqrt{f(\vec{q})^2 + \Delta(\vec{q})^2}. \tag{16.94}$$

Within this massive phase, we will find nontrivial topological invariants of the quasiparticle spectrum. Let $iA(\vec{q})$ be a nondegenerate Hermitian matrix that continously depends on $\vec{q}$. In our case, A acts in $\mathbb{C}^2$, but in general it can be $\mathbb{C}^n$ for any n. Let us keep track of the "negative eigenspace" of $iA(\vec{q})$: the subspace $\mathfrak{L}(\vec{q}) \subseteq \mathbb{C}^n$ spanned by eigenvectors corresponding to negative eigenvalues. For matrix (16.93), $\dim\ \mathfrak{L}(\vec{q}) = 1$. This defines a map F from momentum space (the torus) to the set of m-dimensional subspaces in $\mathbb{C}^n$. More formally:

$$F:\ \mathbb{T}^2 \longrightarrow U(n)/U(m) \times U(n-m) \tag{16.95}$$

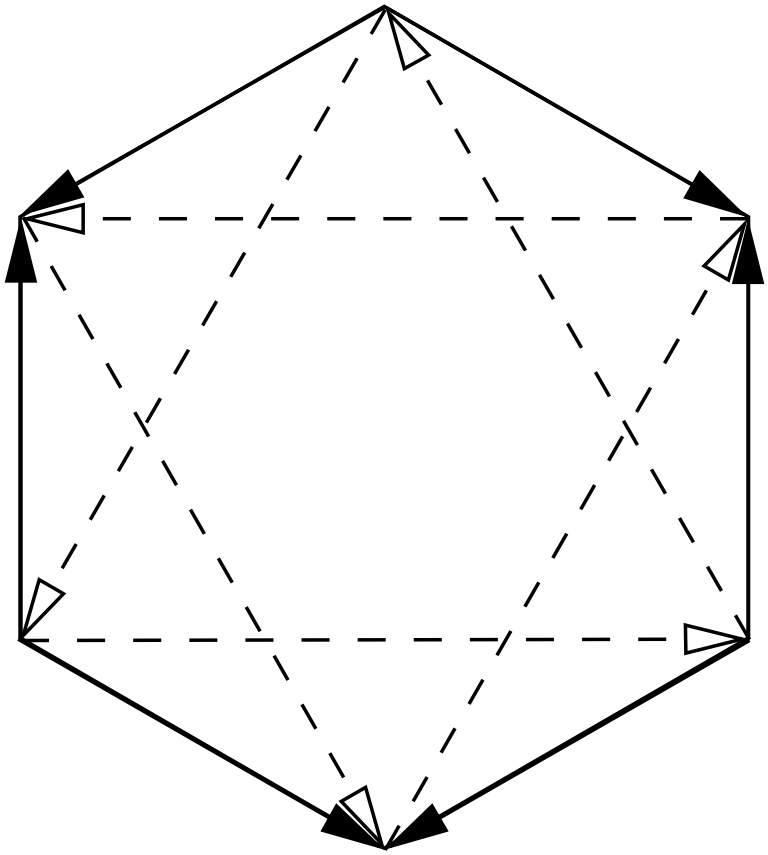


Figure 16.12: Picture of chiral interaction matrix A_{jk}. Forward arrows correspond to positive entries in the skew-symmetric real matrix A_{jk}. Solid arrows are the interactions of the original honeycomb model; dashed arrows give the time-reversal symmetry breaking perturbation.

This map F may have nontrivial topology.

In the honeycomb model with T-breaking, we have $n = 2$, $m = 1$ and $U(2)/U(1) \times U(1) = \mathbb{C}P^1 = S^2$ is the unit sphere. Thus, $F : \mathbb{T}^2 \longrightarrow S^2$ and for the matrix $iA(\vec{q})$ of Eq. (16.93), F has degree 1. That is, the torus wraps around the sphere once. More abstractly, $\mathfrak{L}(\vec{q})$ defines a complex vector bundle over the momentum space $\mathbb{T}^2$. This has an invariant Chern number ν, which in this case is $\nu = 1$.

What is the significance of the spectral Chern number? It is known to characterize the integer quantum Hall effect, where it is known as the "TKNN invariant". For a Majorana system, there is no Hall effect since particles are not conserved. Rather, the spectral Chern number determines the number of chiral modes at the edge:

$$\nu = (\#\text{ of left-movers}) - (\#\text{ of right-movers}). \tag{16.96}$$

16.5.6 Robustness of chiral modes

A chiral edge mode may be described by its Hamiltonian:

$$H_{\text{edge}} = \frac{iv}{4} \int \hat{\eta}(x) \partial_x \hat{\eta}(x) dx \tag{16.97}$$

where $\hat{\eta}(x)$ is a real fermionic field. That is,

$$\hat{\eta}(x)\hat{\eta}(y) + \hat{\eta}(y)\hat{\eta}(x) = 2\delta(x - y). \tag{16.98}$$

At temperature T, each mode carries energy current

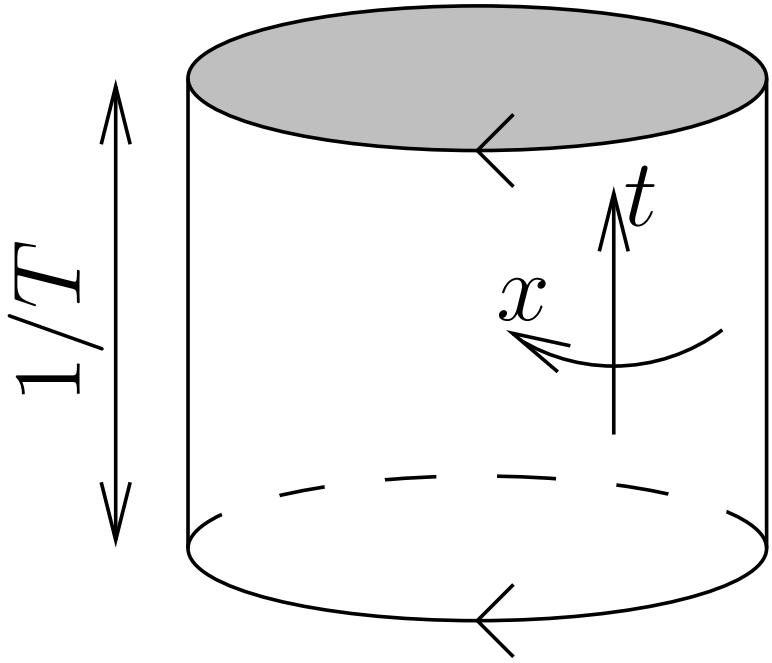
$$I_1 = \frac{\pi}{24} T^2. \tag{16.99}$$

The easiest explanation of this is a straightforward 1-D fermi gas calculation:

$$\begin{aligned} I_1 &= v \int_0^\infty n(q)\epsilon(q) \frac{dq}{4\pi} \\ &= \frac{1}{2\pi} \int_0^\infty \frac{\epsilon d\epsilon}{1 + e^{\epsilon/T}} \\ &= \frac{\pi}{24} T^2 \end{aligned} \tag{16.100}$$

However, it is useful to reexamine this current using conformal field theory (CFT), in order to understand better why the chiral modes are robust. We consider a disc of B phase extended into imaginary time at temperature T. That is, we have a solid cylinder with top and bottom

identified:



We have obtained a solid torus whose surface is a usual torus. The partition function is mostly determined by the surface.

Let the spatial dimensions be much greater than $\frac{1}{T}$. From this point of view, the cylinder looks more like:

According to the usual CFT arguments, we have

$$\begin{aligned} Z &\sim q^{\frac{c}{24}}\bar{q}^{\frac{\bar{c}}{24}} \\ q &= e^{2\pi i\tau} \\ \tau &= i\frac{LT}{v} + \text{twist} \end{aligned} \tag{16.101}$$

Twisting the torus changes the partition function by:

$$\begin{aligned} \tau &\mapsto \tau + 1 \\ Z &\mapsto Ze^{2\pi i\frac{c-\bar{c}}{24}}. \end{aligned} \tag{16.102}$$

On the other hand, the twist parameter ($\operatorname{Re}\tau$) couples to the some component of the energy-momentum tensor, namely, T_{xt}, which corresponds to the energy flow. This relation implies that

$$I = \frac{\pi}{12}(c-\bar{c})T^2. \tag{16.103}$$

The chiral central charge, $c - \bar{c}$, does not depend on the boundary conditions. Indeed, the energy current on the edge cannot change because the energy cannot go into the bulk.

17 Entanglement in quantum critical phenomena by Vidal, Latorre, Rico, Kitaev

Abstract

Quantum phase transitions occur at zero temperature and involve the appearance of long-range correlations. These correlations are not due to thermal fluctuations but to the intricate structure of a strongly entangled ground state of the system. We present a microscopic computation of the scaling properties of the ground-state entanglement in several 1D spin chain models both near and at the quantum critical regimes. We quantify entanglement by using the entropy of the ground state when the system is traced down to L spins. This entropy is seen to scale logarithmically with L, with a coefficient that corresponds to the central charge associated to the conformal theory that describes the universal properties of the quantum phase transition. Thus we show that entanglement, a key concept of quantum information science, obeys universal scaling laws as dictated by the representations of the conformal group and its classification motivated by string theory. This connection unveils a monotonicity law for ground-state entanglement along the renormalization group flow. We also identify a majorization rule possibly associated to conformal invariance and apply the present results to interpret the breakdown of density matrix renormalization group techniques near a critical point.

The study of entanglement in composite systems is one of the major goals of quantum information science [1, 2], where entangled states are regarded as a valuable resource for processing information in novel ways. For instance, the entanglement between systems A and B in a joint pure state $|\Psi_{AB}\rangle$ can be used, together with a classical channel, to *teleport* or send quantum information [3]. From this resource-oriented perspective, the *entropy of entanglement* $E(\Psi_{AB})$ measures the entanglement contained in $|\Psi_{AB}\rangle$ [4]. It is defined as the von Neumann entropy of the reduced density matrix ρ_A (equivalently ρ_B),

$$E(\Psi_{AB}) = -\mathrm{tr}\,(\rho_A \log_2 \rho_A)\,, \tag{17.1}$$

and directly determines, among other aspects, how much quantum information can be teleported by using $|\Psi_{AB}\rangle$.

On the other hand, entanglement is appointed to play a central role in the study of strongly correlated quantum systems [5, 6, 7], since a highly entangled ground state is at the heart of a large variety of collective quantum phenomena. Milestone examples are the entangled ground states used to explain superconductivity and the fractional quantum Hall effect, namely the BCS ansatz [8] and the Laughlin ansatz [9]. Ground-state entanglement is, most promisingly, also a key factor to understand quantum phase transitions [10, 11], where it is directly responsible for the appearance of long-range correlations. Consequently, a gain of insight into phenomena including, among others, Mott insulator-superfluid transitions, quantum magnet-paramagnet transitions and phase transitions in a Fermi liquid is expected by studying the structure of entanglement in the corresponding underlying ground states.

In the following we analyze the ground-state entanglement near and at a quantum critical point in a series of 1D spin-1/2 chain models. In particular, we consider the hamiltonians

$$H_{XY} = -\sum_{l=0}^{N-1} \left(\frac{a}{2}[(1+\gamma)\sigma_l^x \sigma_{l+1}^x + (1-\gamma)\sigma_l^y \sigma_{l+1}^y] + \sigma_l^z \right) \tag{17.2}$$

and

$$H_{XXZ} = -\sum_{l=0}^{N-1} \left(\sigma_l^x \sigma_{l+1}^x + \sigma_l^y \sigma_{l+1}^y + \Delta \sigma_l^z \sigma_{l+1}^z + \lambda \sigma_l^z \right), \tag{17.3}$$

which contain both first-neighbor interactions and an external magnetic field, and are used to describe a range of $1D$ quantum systems [10]. Notice that $H_{XY}(\gamma = 1)$ corresponds to the Ising chain, whereas $H_{XXZ}(\Delta = 1)$ describes spins with isotropic Heisenberg interaction. Both Hamiltonians coincide for $\gamma = \Delta = 0$, where they become the XX model.

Osterloh *et al* [12] and Osborne and Nielsen [11] have recently considered the entanglement in the XY spin model, Eq. (17.2), in the neighborhood of a quantum phase transition. Their analysis, focused on *single-spin* entropies [11] and on *two-spin* quantum correlations [12, 11], suggestively shows that these one- and two-spin entanglement measures are picked either near or at the critical point. Here, alternatively, we undertake the study of the *entanglement between a block of L contiguous spins and the rest of the chain*, when the spin chain is in its ground state $|\Psi_g\rangle$. Thus, the aim in the following is to compute the entropy of entanglement, Eq. (17.1), for the state $|\Psi_g\rangle$ according to bipartite partitions parameterized by L,

$$S_L \equiv -\mathrm{tr}\,(\rho_L \log_2 \rho_L)\,, \tag{17.4}$$

where $\rho_L \equiv \mathrm{tr}_{\bar{\mathcal{B}}_L} |\Psi_g\rangle\langle\Psi_g|$ is the reduced density matrix for $\mathcal{B}_L$, a block of L spins.

The XY model, Eq. (17.2), is an *exactly solvable* model, in that H_{XY} can be diagonalized by first using a Jordan-Wigner transformation into fermionic modes and by subsequently concatenating a Fourier transformation and a Bogoliubov transformation (see for instance [10]). The calculation of S_L, as sketched below, also uses the fact that the ground state $|\Psi_g\rangle$ of H_{XY} and the corresponding density matrices ρ_L are all *gaussian* states that can be completely characterized by means of certain correlation matrix of second moments.

More specifically, let us introduce two Majorana operators, c_{2l} and c_{2l+1}, on each site $l = 0, \cdots, N-1$ of the spin chain,

$$c_{2l} \equiv \left(\prod_{m=0}^{l-1} \sigma_m^z\right) \sigma_l^x; \quad c_{2l+1} \equiv \left(\prod_{m=0}^{l-1} \sigma_m^z\right) \sigma_l^y. \tag{17.5}$$

Operators c_m are hermitian and obey the anti-commutation relations $\{c_m, c_n\} = 2\delta_{mn}$. Hamiltonian H_{XY} can be rewritten as

$$H_{XY} = i \sum_{l=0}^{N-1} \Big(\frac{a}{2} \left[(1+\gamma)\, c_{2l+1} c_{2l+2} - (1-\gamma)\, c_{2l} c_{2l+3} \right] + c_{2l} c_{2l+1} \Big)\,,$$

and can be subsequently diagonalized by canonically transforming the operators c_m. The expectation value of c_m when the system is in the ground state, i.e. $\langle c_m \rangle \equiv \langle \Psi_g | c_m | \Psi_g \rangle$, vanishes for all m due to the $\mathcal{Z}_2$ symmetry $(\sigma_l^x, \sigma_l^y, \sigma_l^z) \to (-\sigma_l^x, -\sigma_l^y, \sigma_l^z)$ $\forall l$ of H_{XY}. In turn, the expectation values

$$\langle c_m c_n \rangle = \delta_{mn} + i B_{mn}, \tag{17.6}$$

completely characterize $|\Psi_g\rangle$, for any other expectation value can be expressed, by using Wick's theorem, in terms of $\langle c_m c_n \rangle$. Matrix B reads [13]

$$B = \begin{bmatrix} \Pi_0 & \Pi_1 & \cdots & \Pi_{N-1} \\ \Pi_{-1} & \Pi_0 & & \vdots \\ \vdots & & \ddots & \vdots \\ \Pi_{1-N} & \cdots & \cdots & \Pi_0 \end{bmatrix}, \quad \Pi_l = \begin{bmatrix} 0 & g_l \\ -g_{-l} & 0 \end{bmatrix}, \tag{17.7}$$

with real coefficients g_l given, when $N \to \infty$, by

$$g_l = \frac{1}{2\pi} \int_0^{2\pi} d\phi e^{-il\phi} \frac{a\cos\phi - 1 - ia\gamma\sin\phi}{|a\cos\phi - 1 - ia\gamma\sin\phi|}. \tag{17.8}$$

From Eqs. (17.7)-(17.8) we can extract the entropy S_L of Eq. (17.4) as follows. First we compute the correlation matrix of the state ρ_L for block $\mathcal{B}_L$, namely $\delta_{mn} + i(B_L)_{mn}$, where

$$B_L = \begin{bmatrix} \Pi_0 & \Pi_1 & \cdots & \Pi_{L-1} \\ \Pi_{-1} & \Pi_0 & & \vdots \\ \vdots & & \ddots & \vdots \\ \Pi_{1-L} & \cdots & \cdots & \Pi_0 \end{bmatrix} \tag{17.9}$$

is constructed by eliminating $2(N-L)$ contiguous columns and rows from B, those corresponding to the $N-L$ traced-out spins. Let $V \in SO(2L)$ denote an orthogonal matrix that brings B_L into a block-diagonal form, that is

$$\tilde{B}_L = V B_L V^T = \oplus_{m=0}^{L-1} \nu_m \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad \nu_m \geq 0. \tag{17.10}$$

Then the set of $2L$ Majorana operators $d_m \equiv \sum_{n=0}^{2L-1} V_{mn} c_n$, obeying $\{d_m, d_n\} = 2\delta_{mn}$, have a block-diagonal correlation matrix $\langle d_m d_n \rangle = \delta_{mn} + i(\tilde{B}_L)_{mn}$. Therefore, the L fermionic operators $b_l \equiv (d_{2l} + i d_{2l+1})/2$, obeying $\{b_m, b_n\} = 0$ and $\{b_m^\dagger b_n\} = \delta_{mn}$, have expectation values

$$\langle b_m \rangle = 0, \quad \langle b_m b_n \rangle = 0, \quad \langle b_m^\dagger b_n \rangle = \delta_{mn} \frac{1+\nu_m}{2}. \tag{17.11}$$

Eq. (17.11) indicates that the above fermionic modes are in a *product* or *uncorrelated* state, that is

$$\rho_L = \varrho_0 \otimes \cdots \otimes \varrho_{L-1}, \tag{17.12}$$

where ϱ_m denotes the mixed state of mode m. The entropy of ρ_L is a sum over the entropy $H_2((1+\nu_m)/2)$ of each mode [$H_2(x) = -x \log_2 x - (1-x)\log_2(1-x)$ is the binary entropy] and thus reads

$$S_L = \sum_{m=0}^{L-1} H_2\left(\frac{1+\nu_m}{2}\right). \tag{17.13}$$

For arbitrary values of (a, γ) in H_{XY} and in the thermodynamic limit, $N \to \infty$, one can evaluate Eq. (17.8) numerically, diagonalize B_L in Eq. (17.9) to obtain ν_m and then evaluate Eq. (17.13). The computational effort grows only polynomically with L and produces reliable values of S_L for blocks with up to several tens of spins. However, further analytical characterization is possible in some cases, which speeds the computation significantly. For instance, for the XX model with magnetic field, $\gamma = 0$ and $1/a \in [-1, 1]$, one obtains $g_0 = \phi_a/\pi - 2$ and $g_l = 2\sin(l\phi_a)/l\pi$ for $l \neq 0$, where $\phi_a = \arccos(1/a)$, from which S_L can be numerically determined. We obtain, up to $L = 100$ spins,

$$S_L^{XX} \approx \frac{1}{3}\log_2(L) + k_1(a), \tag{17.14}$$

where $k_1(a)$ depends only on a. For the Ising model with critical magnetic field, $\gamma = 1, a = 1$, one finds $g_l = -2/l$ for odd l and $g_l = 0$ for even l and, for up to $L = 100$ spins,

$$S_L^{Ising} \approx \frac{1}{6}\log_2(L) + k_2, \qquad k_2 \approx \pi/3. \tag{17.15}$$

Finally, for the Ising model with magnetic field, $\gamma = 1$, and for a close to 1, Kitaev has obtained an analytical expression for the entropy of half of an infinite chain [15]. To use this result in our setting we need to double its value because the entropy resides near the boundary. Thus we get

$$S_{N/2}^{Ising} \approx \frac{1}{6}\log_2 \frac{1}{|1-a|}. \tag{17.16}$$

The XXZ model, Eq. (17.3), cannot be analyzed using the previous method. Instead we have used the Bethe ansatz [16] to exactly determine, through a numerical procedure, the ground state $\left|\Psi_g^{(20)}\right\rangle$ of H_{XXZ} for a chain of up to $N = 20$ spins, from which $S_L^{(20)}$ can be computed. Recall that in the XXZ model the non-analyticity of the ground-state energy characterizing a phase transition occurs already for a finite number N of spins in the chain, since it is due to level-crossing. It turns out that, correspondingly, already for $N = 20$ spins one can observe a distinct, characteristic behavior of $S_L^{(20)}$ depending on whether the values (Δ, λ) in Eq. (17.3) belong to a critical regime.

The results of the computation of S_L for the spin chains (17.2) and (17.3) can be summarized as follows.

Non-critical regime. For those values (a, γ) or (Δ, λ) for which the models are non-critical, the entropy of entanglement S_L either vanishes for all L [*e.g.* when a sufficiently strong magnetic field aligns all spins into a product, unentangled state] or grows monotonically as a function of L until it reaches a *saturation* value S_{max}. For instance, in the infinite Ising chain the saturation entropy S_{max} is given by Eq. (17.16). As shown in Fig. (**??**), S_L often approaches S_{max} already for a small number L of spins.

Critical regime. Instead, critical ground-states are characterized by an entropy S_L that diverges logarithmically with L,

$$S_L \approx \frac{c + \bar{c}}{6} \log_2(L) + k, \tag{17.17}$$

with a coefficient given by the holomorphic and antiholomorphic *central charges* c and $\bar{c}$ of the conformal field theory that describes the universal properties of the phase transition [17], see Fig. (17.1). This expression was derived by Holzhey, Larsen and Wilczek [18] for the *geometric entropy* (analogous of Eq. (17.4) for a conformal field theory), and our calculation confirms it for several critical spin chains. Thus, the critical Ising model corresponds to a free fermionic field theory, with central charges $c_f = \bar{c}_f = 1/2$, whereas the rest of critical regimes in (17.2) and (17.3) are described by a free bosonic field theory, $c_b = \bar{c}_b = 1$ (cf. Eqs. (17.14) and (17.15)). In particular, the marginal deformation $0 < \gamma \leq 1$ for $a = 1$ shows scaling for every γ with universal coefficient $c = \bar{c} = 1/2$. It is possible to compare the subleading correction between two different values of γ. The behavior we obtain is described by

$$\lim_{L\to\infty} [S_L(\gamma = 1) - S_L(\gamma)] = -\frac{c + \bar{c}}{6} \log_2 \gamma \ . \tag{17.18}$$

The singular behavior at $\gamma = 0$ is the signature of the fact that that point belongs to the abrupt change of universality class for the XX model.

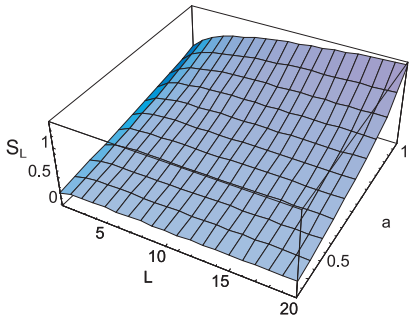


Figure 17.1: Numerical calculation of critical entanglement S_L for 1D spin chains. Points (+) come from an infinite Ising chain with critical magnetic field, $H_{XY}(a = 1, \gamma = 1)$ in Eq. (17.2), and corresponds to $S_L^{Ising} \approx \log_2(L)/6 + k_2$. Curve (×) comes from an infinite XX spin chain without magnetic field, $H_{XY}(a = \infty, \gamma = 0)$ in Eq. (17.2), and corresponds to $S_L^{XX} \approx \log_2(L)/3 + k_1$. Thus the growth in L of entanglement in the XX model, asymptotically described by a free boson, is twice that in the Ising model, corresponding to a free fermion, $S_{L+1}^{XX} - S_L^{XX} \approx 2(S_{L+1}^{Ising} - S_L^{Ising})$. Finally, curve (∗) comes from a XXX chain of 20 spins without magnetic field, $H_{XXZ}(\Delta = 1, \lambda = 0)$ in Eq. (17.3). These finite-chain results, obtained using the Bethe ansatz, combine the logarithmic behavior ($L = 1, \cdots, 5$) of a free boson field theory with a finite-size saturation effect ($L = 6, \cdots, 10$). We have added the lines $\frac{c+\bar{c}}{6}[\log_2(L) + \pi]$ both for bosons and fermions to highlight their remarkable agreement with the numerical diagonalization.

The above characterizations motivate a number of observations, that we move to discuss.

Critical and non-critical ground states contain structurally different forms of quantum correlations. Non-critical ground-state entanglement corresponds to a weak, *semi-local* form of entanglement driven by the appearance of a length scale, *e.g.* a mass gap. Indeed, for any L, the reduced density matrix ρ_L is supported on a small, bounded subspace of the Hilbert space of the L spins, and can be obtained by diagonalizing the hamiltonian corresponding to the block $\mathcal{B}_L$ and only a few extra *neighboring* spins, as skillfully exploited in White's density matrix renormalization group (DMRG) techniques [19]. We note here that a bounded rank for ρ_L (relatedly, a saturation value for S_L) is instrumental for the success of DMRG schemes, where only of a finite number of eigenvectors of ρ_L can be kept. Critical bound-state entanglement corresponds, on the contrary, to a stronger form of entanglement, one that embraces the system at all length scales simultaneously. DMRG techniques have reportedly failed to reproduce quantum critical behavior [20] and we may, in view of Eq. (17.17), be in a position to understand why. Indeed, the divergent character of S_L is just one particular manifestation of the fact that the number of relevant eigenvectors of ρ_L unboundedly grows with L. If, as is the case in DMRG schemes, only a finite number of levels can be considered, then a sufficiently large L will always make the computation of ρ_L impossible (arguably, even in an approximate sense) by using such schemes. This strongly suggests that overcoming the above difficulties necessarily requires techniques that do not attempt to reproduce the critical behavior of the ground state through a local, real space construction.

Another remarkable, far-reaching fact is that, as mentioned below Eq. (17.17), our results coincides with entropy computations performed in conformal field theory. There, a *geometric* or *fine-grained* entropy analogous to Eq. (17.4) but for a continuous field theory has been considered by several authors, including Srednicki [21], Callan and Wilczek [22], Holzhey et al [18] and Fiola et al [23]. Thus, starting from non-relativistic spin chain models, and by performing a microscopic analysis of a relevant quantity in quantum information, we have obtained a universal scaling law for entanglement that is in full agreement with previous findings

in the context of, say, black-hole thermodynamics in 1+1 dimensions [18, 23].

The above connection has a number of implications to be exploited. For instance, Srednicki [21] has obtained the behavior of entropy in 2+1 and 3+1 dimensional conformal field theories. For a region $\mathcal{R}$ in 2 or 3 spatial dimensions, the entropy of $\mathcal{R}$ is proportional to the size $\sigma(\mathcal{R})$ of its boundary,

$$S_{\mathcal{R}} \approx \kappa\sigma(\mathcal{R}). \tag{17.19}$$

That is, the entropy per unit of boundary area, κ, is independent of the size of $\mathcal{R}$. [This is in sharp contrast with the same quantity in 1D, where the boundary consists of two points and $S_{\mathcal{R}}/\sigma(\mathcal{R})$ diverges logarithmically with the length L of $\mathcal{R}$]. Accordingly, Eq. (17.19) also describes the critical ground-state entanglement of 2D and 3D spin lattices.

Also the fact that the entropy of entanglement for $1D$ critical spin chains, Eq. (17.17), matches well-known conformal field theory parameters carries an extra bonus. The coefficient in control of the divergent behavior of S_L at critical points is the central charge, which is subject to Zamolodchikov's c-theorem [24]. The c-theorem states that the central charges associated to the ultraviolet and infrared end points of renormalization group flows, labeled by C_{UV} and C_{IR}, obey the inequality $C_{UV} > C_{IR}$ for unitary theories. This powerful result establishes an irreversible arrow as renormalization group transformations are performed. The translation of this idea to the quantum information setting is that entanglement decreases along renormalization group flows. An infrared theory carries less global entanglement than the ultraviolet theory where it flowed from. The c-theorem seems natural as renormalization group transformations integrate out short distance degrees of freedom, accompanied with their quantum correlations. Yet, it is not at all trivial due to, first, the infinite degrees of freedom (needing regularization) existing in a quantum field theory and, second, the rescaling step in the renormalization group transformation. It is noteworthy, then, that entanglement decreases both (*i*) under the *local operations and classical communication* and (*ii*) along *renormalization group trajectories*. The former case corresponds to *local manipulation* of an entangled system while the second is made out of a block-spin transformation followed by a *rescaling* of the system. Both actions do reduce quantum correlations and become irreversible [24, 25].

One more remark. From Eqs. (17.8)-(17.9) the complete spectrum of ρ_L can be extracted. The 2^L eigenvalues are given by

$$\lambda_{x_1 x_2 \cdots x_L} = \prod_{m=0}^{L-1} \frac{1 + (-1)^{x_m}\nu_m}{2}, \quad x_m = 0, 1 \ \forall m. \tag{17.20}$$

This allows us to look in more detail to the reshuffling of the ground state as more sites are incorporated in the block $\mathcal{B}_L$. Every time a new spin is added, the amount of local surprise due to quantum correlations with the rest of the chain increases, and so does the entropy. But critical quantum correlations entangle every single subset of the system, and the way they are reordered is far more subtle than the relation hinted by entropy arguments. We have numerically verified that also a majorization relation [26] holds for the ground-state reduced density matrices of the infinite XY spin chain, namely

$$\vec{\lambda}_{L+2} \prec \vec{\lambda}_L \quad \forall L, \tag{17.21}$$

where the jump in steps of two is forced by the subtleties of the microscopic model. Thus, a critical ground state orderly redistributes weights, so as to accommodate for the new correlations, according to a detailed, exponentially large set of inequalities as contained in Eq. (17.21). In this sense, majorization may be a signature –admittedly a very refined one– of conformal invariance.

But the majorization counterpart in the continuum conformal field theory is not yet known. Perhaps, then, the correspondence between concepts of quantum information science and conformal field theory, between critical ground-state entanglement and geometrical entropy, can also be exploited in the reverse direction.

This work was supported by the by the Spanish grants GC2001SGR-00065 and MCYT FPA2001-3598, by the National Science Foundation of USA under grant EIA–0086038, and by the European Union under grant ISF1999-11053.

References

[1] C. H. Bennett and D. P. DiVincenzo, Nature **404**, 247 - 255 (2000).

[2] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum communication* (Cambridge Univ. Press, Cambridge, 2000).

[3] C. H. Bennett, G. Brassard, C. Crépeau, R. Josza, A. Peres and W.K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

[4] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A **53**, 2046-2052 (1996).

[5] J. Preskill, J. Mod. Opt. **47** (2000) 127-137,

[6] T. J. Osborne and M. A. Nielsen, *Entanglement, quantum phase transitions, and density matrix renormalization*, quant-ph/0109024.

[7] P. Zanardi and X. Wang, *Fermionic entanglement in itinerant systems*, J. Phys. A **35** (2002) 7947

[8] J. Bardeen, L. N. Cooper and J. R. Schrieffer, Phys. Rev. **108**, 1175 (1957).

[9] R. B. Laughlin, Phys. Rev. Lett. **50**, 1395 (1983).

[10] S. Sachdev, *Quantum phase transitions*, (Cambridge University Press, Cambridge, 1999).

[11] T. J. Osborne and M. A. Nielsen, *Entanglement in a simple quantum phase transition*, quant-ph/0202162.

[12] A. Osterloh, L. Amico, G. Falci and R. Fazio, *Scaling of entanglement close to a quantum phase transition*, Nature **416** (2002) 608-610.

[13] A more detailed analysis of these manipulations, that can be extracted from [14], will be presented somewhere else. We note that, for the sake of simplicity, we do not discuss finite N corrections to Eq. (17.7). In the thermodynamic limit, $N \to \infty$, they do not contribute to Eq. (17.9) for finite L, and therefore do not affect the computation of S_L.

[14] E. Lieb, T. Schultz and D. Mattis, Annals of Phys. **16** 407 (1961).

[15] A. Kitaev, *private communication.*

[16] H. A. Bethe, Z. Physik **71**, 205 (1931).

[17] Paul Ginsparg, *Applied conformal field theory*, Les Houches Summer School 1988, pp 1-168.

[18] C. Holzhey, F. Larsen and F. Wilczek, Nucl. Phys. B **424** (1994) 443-467.

[19] S. R. White, Phys. Rev. B **48**, 10345-10356 (1993).

[20] S. Rommer and S. Östlund, *Density matrix renormalization*, Dresden, 1998 (Springer, Berlin, 1999), pp 67-89.

[21] M. Srednicki, Phys. Rev. Lett. **71** (1993) 666-669.

[22] C. G. Callan and F. Wilczek, Phys. Lett. **B333** (1994) 55-61.

[23] T. M. Fiola, J. Preskill, A. Strominger and S. P. Trivedi, Phys. Rev. D **50** (1994) 3987-4014.

[24] A. B. Zamolodchikov JETP Lett. **43** (1986) 730; A. Cappelli, D. Friedan and J. I. Latorre, Nucl. Phys. B **352** (1991) 616; S. Forte and J. I. Latorre, Nucl. Phys. B **535** (1998) 709.

[25] G. Vidal and J. I. Cirac, Phys. Rev. Lett. **86**, (2001) 5803-5806.

[26] R. Bhatia, *Matrix Analisis*, Graduate Texts in Mathematics vol. 169, Springer-Verlag, 1996.

18 What limits the simulation of quantum computers? by Zhou, Stoudenmire, Waintal

Abstract

An ultimate goal of quantum computing is to perform calculations beyond the reach of any classical computer. It is therefore imperative that useful quantum computers be very difficult to simulate classically; otherwise classical computers could be used for the applications envisioned for the quantum ones. *Perfect* quantum computers are unarguably exponentially difficult to simulate: the classical resources required grow exponentially with the number of qubits N or the depth D of the circuit. This difficulty has triggered recent experiments on deep, random circuits that aim to demonstrate that quantum devices may already perform tasks beyond the reach of classical computing. These *real* quantum computing devices, however, suffer from many sources of decoherence and imprecision which limit the degree of entanglement that can actually be reached to a fraction of its theoretical maximum. They are characterized by an exponentially decaying fidelity $\mathcal{F} \sim (1-\epsilon)^{ND}$ with an error rate ϵ per operation as small as $\approx 1\%$ for current devices with several dozen qubits or even smaller for smaller devices.

In this work, we provide new insights on the computing capabilities of real quantum computers by demonstrating that they can be simulated at a tiny fraction of the cost that would be needed for a perfect quantum computer. Our algorithms compress the representations of quantum wavefunctions using matrix product states (MPS), which are able to capture states with low to moderate entanglement very accurately. This compression introduces a finite error rate ϵ so that the algorithms closely mimic the behavior of real quantum computing devices. The computing time of our algorithm increases only linearly with N and D in sharp contrast with exact simulation algorithms. We illustrate our algorithms with simulations of random circuits for qubits connected in both one and two dimensional lattices. We find that ϵ can be decreased at a polynomial cost in computing power down to a minimum error ϵ_∞. Getting below ϵ_∞ requires computing resources that increase exponentially with ϵ_∞/ϵ. For a two dimensional array of $N = 54$ qubits and a circuit with Control-Z gates, error rates better than state-of-the-art devices can be obtained on a laptop in a few hours. For more complex gates such as a swap gate followed by a controlled rotation, the error rate increases by a factor three for similar computing time. Our results suggest that, despite the high fidelity reached by quantum devices, only a tiny fraction ($\sim 10^{-8}$) of the system Hilbert space is actually being exploited.

18.1 Introduction

Operating a quantum computer is a race against the clock. The same phenomenon enabling the potential computing power of quantum computers—entanglement—is also responsible for decoherence when it occurs with unmonitored degrees of freedom. The main challenge of quantum computing is to quickly build entanglement between the qubits before imperfections or decoherence overly corrupt the quantum state. This decoherence is an intrinsic characteristic of any quantum computer and its origin and consequences must be understood thoughtfully. But in all hardware realizations, it means each operation incurs a loss of fidelity relative to the ideal target quantum state.

As different experimental platforms for quantum manipulation make rapid, impressive advances, there has been a justifiable interest in the computational capability of near-term quantum computers [1]. One of the key questions is when and how to achieve the goal of "quantum supremacy" [2], which is the crossover point where a quantum system ceases to be within reach of simulation on a classical computer. Precise circuits and fidelity metrics have been designed to meet this goal [3]. Recently, an experiment using $N = 53$ qubits and a circuit of depth $D = 20$ has reached a multi-qubit fidelity $\mathcal{F} = 0.002$ [4]. According to the authors, such an experiment would take thousands of years to be simulated on the largest existing supercomputers. This statement was then challenged by another estimate which claims that only two days would be needed [5]. Such a disparity between estimates raises the question of the difficulty of simulating a quantum computer and consequently of the true computing power realized in a quantum computer.

The implicit assumption behind quantum supremacy as well as the most appealing applications of quantum computing is that a quantum computer is exponentially hard to simulate. Indeed, in recent years many techniques have been developed to simulate quantum computers, and they all have an exponential cost in some parameter. A brute force approach where one holds the full quantum state in memory as a large vector of size 2^N (N: number of qubits) requires a computing time and memory that scales exponentially with N but linearly with the depth D of the circuit. Other approaches require a computing time that scale exponentially with the number of two-qubit gates [6, 7, 8, 9], with the number of non-Clifford gates [10] and/or with the number of gates that are non-diagonal in a chosen basis [11, 12]. All these techniques can simulate *perfect* quantum computers. In all cases, the required computing resources are exponential so that getting beyond $N = 50$ and a depth $D = 20$ for an arbitrary circuit is extremely difficult.

In this article, we show that *real* quantum computers can be simulated at a tiny fraction of the cost that would be needed for a *perfect* quantum computer. To do so, we take advantage of the fact that in real quantum computers, decoherence limits the amount of entanglement that can be built into the quantum state to a fraction of what the exponentially large Hilbert space would suggest. Our algorithms use a compressed wavefunction representation that achieves very high accuracy for states with low to moderate entanglement. This compression introduces a finite error rate ϵ per two-qubit gate. Hence, in this class of algorithms the limiting factor is the fidelity with which the calculation is performed while the computing time is linear in both the number of qubits N and the depth D. These algorithms "mimic" actual quantum computers both in the sense of how they scale with N and D, and in the sense that the main difficulty lies in increasing the fidelity of the calculation: a small finite error ϵ is made each time a two-qubit gate is applied to the state. Therefore, they offer a better reference point than exact simulation algorithms for assessing the computing power harvested by actual quantum chips.

Our algorithms are based on tensor networks and more precisely on matrix product states (MPS) [13]. MPS have been recognized very early as an interesting parameterization of many-qubit quantum states for quantum simulations [6] and its generalizations are used in some of

the most advanced quantum simulation approaches [14]. However, so far, the focus of classical simulations of quantum hardware has been building essentially exact simulations techniques and little attention has been devoted to approximate techniques. Interestingly these exact techniques can require one to go well beyond double precision calculations [15] which already hints at the link between error rate and underlying computing difficulty.

The historical success of MPS has *not* been for exact calculations but, in contrast, for the development of controlled, approximate techniques to address quantum many-body physics problems. This includes the celebrated density matrix renormalization group (DMRG) algorithm [16] which has provided precise solutions to a number of one-dimensional and quasi-one-dimensional problems, as well as time-dependent extensions [17] and generalizations to higher dimensions through projected entangled pair states (PEPS) [18] or multi-scale entanglement renormalization ansatz (MERA) [19] tensor networks. At the root of these successes is the fact that MPS naturally organizes states according to the amount of entanglement entropy between different parts of the system. Hence, slightly entangled systems can be easily represented with MPS. As entanglement entropy grows, one eventually truncates the basis. The associated error can be made arbitrarily small by keeping a larger set of basis states.

In this article, we construct such an approximate technique in the context of quantum computing. Our chief result is that, for fidelities comparable to those reached experimentally, the computational requirement for simulating an imperfect quantum computer is only a tiny fraction of the requirements for a perfect one.

18.2 Possible strategies for approximate simulations of quantum circuits

Let us start by discussing possible strategies for simulating quantum circuits in an approximate manner. Suppose that we have partitioned the qubits into two different sets A and B with respectively N_A and N_B qubits ($N_A + N_B = N$). Let us consider the two-qubit gates that connect A and B and ignore gates internal to A or B. Performing a singular value decomposition (SVD) of such a gate, it can be written as a sum of terms that act separately on A and B. This sum contains two terms for the case of usual gates (Control-NOT and Control-Z) and at most four terms for an arbitrary two-qubit gate. It follows that computing the state after n of these gates amounts to keeping track of 2^n (up to 4^n) different amplitudes. These amplitudes are the discrete analogue of Feynman paths and are referred to as such in the literature. For the random circuits that will be considered in this article, these 2^n amplitudes have essentially random phases. It follows that if one keep track of just a *single* path, one reaches an overall multi-qubit fidelity $\mathcal{F} = (1/2)^n$ (or $\mathcal{F} = (1/4)^n$ in the worst situation). This very simple strategy could be used to simulate an arbitrary large number of qubits with low fidelity per gate in a computing time $\sim n$. However, if one wants to keep a fixed fidelity per gate f defined as $\mathcal{F} = f^n$, in analogy with real quantum computers, the number of paths $N_{\rm path}$ that must be tracked during the simulation is $N_{\rm path} = (2f)^n$, and hence increases exponentially with n. Such a strategy has been used in Ref. [4] to validate the experimental results reported there.

We now seek algorithms where a constant fidelity f can be obtained at a constant computing cost per gate, independent of the total number of gates n. One starts by writing a general state for the bipartite system as

$$|\Psi\rangle = \sum_{a,b} \Psi_{ab} |a\rangle_A |b\rangle_B \tag{18.1}$$

where the states $|a\rangle$ ($|b\rangle$) form an orthonormal basis of A (B). Performing a singular value decomposition (SVD)

$$\Psi_{ab} = \sum_{\mu} U_{a\mu} S_\mu V_{\mu b}, \tag{18.2}$$

one can define an orthonormal basis

$$|\mu\rangle_A = \sum_a U_{\mu a}|a\rangle_A \tag{18.3}$$

(with similar notation for the B subsystem) and arrive at the usual Schmidt decomposition of $|\Psi\rangle$:

$$|\Psi\rangle = \sum_\mu S_\mu |\mu\rangle_A |\mu\rangle_B \tag{18.4}$$

in terms of a finite number of singular values S_μ. States with only one non-zero singular value $S_0 = 1$ are simple, unentangled product states. A measure of the number of significant singular values needed to describe the state to high accuracy is given by the entanglement entropy

$$S = -\text{Tr } \rho_A \log \rho_A = -\text{Tr } \rho_B \log \rho_B = -\sum_\mu S_\mu^2 \log S_\mu^2 \tag{18.5}$$

where ρ_A (ρ_B) is the reduced density matrix for the subsystem A (B). The general strategy of DMRG-like algorithms is to keep only a finite number χ of the singular values. After a two-qubit gate that connects A and B, one performs a SVD decomposition of Ψ_{ab} and truncate the state by keeping only the χ largest singular values. When $\chi \gg e^S$ this procedure is essentially exact. As the entanglement increases, this procedure lead to a certain fidelity per gate $f < 1$ that can be controlled by increasing the parameter χ. Of interest to the present article is the typical value of f that can be reached in a reasonable computing time.

18.3 Noisy algorithm in one dimension

Above we motivated the truncated SVD of a two-qubit wavefunction as an approximation strategy that works well for wavefunctions with only a moderate amount of entanglement. A natural generalization of this strategy to the N-qubit case is to use matrix product states (MPS), which can be viewed as a simultaneous Schmidt decomposition of the wavefunction across N different partitions [6] or equivalently a sequence of compatible SVD factorizations of the wavefunction, grouping qubits $1, 2, \ldots, j$ and $j+1, \ldots, N$ and performing an approximate SVD of the resulting matrix [13].

18.3.1 MPS representation of the state

We first consider a one dimensional network of N qubits where two-qubit gates can be only applied directly between nearest neighbors. (Within this connectivity, gates acting on other non-neighboring qubits are still possible at the cost of using $\sim N$ SWAP operations to bring the qubits onto neighboring sites.) We define our MPS state in terms of N tensors $M(n)$ as

$$|\Psi\rangle = \sum_x \Psi_x |x\rangle = \sum_{i_1 \ldots i_N} \sum_{\mu_1 \ldots \mu_{N-1}} M(1)^{i_1}_{\mu_1} M(2)^{i_2}_{\mu_1 \mu_2} M(3)^{i_3}_{\mu_2 \mu_3} \ldots M(N)^{i_N}_{\mu_{N-1}} |i_1 i_2 i_3 \ldots i_N\rangle \tag{18.6}$$

where the "physical" indices $i_n \in \{0, 1\}$ span the 2^N dimensional Hilbert space while the bond (or virtual) indices $\mu_n \in \{1, ..., \chi_n\}$ control the maximum degree of entanglement allowed by the MPS. $|x\rangle$ is a shorthand for $|i_1 i_2 ... i_N\rangle$. If the χ_n are allowed to grow exponentially large as a function of N, then the MPS form of the wavefunction becomes exact and can represent any wavefunction [13]. In contrast, we will enforce $\chi_n \leq \chi$ in what follows so that the resulting MPS represents an approximation of the true wavefunction. The parameter χ controls the error rate made by our algorithm as well as the computational and memory costs required to run it.

As we will see below, applying a two-qubit gate takes $\sim \chi^3$ operations and the overall memory footprint is $N\chi^2$. A sketch of the MPS structure is shown in Fig. 18.1b.

To be acceptable, our algorithm must provide the same features that a real quantum computer would provide. Applying a one-qubit gate U on qubit n can be done exactly and without increasing any of the χ_n: it simply amounts to updating the corresponding tensor $M(n) \to M'(n)$:

$$M'(n)^{i'_n}_{\mu_{n-1}\mu_n}(n) = \sum_{i_n} U_{i'_n i_n} M(n)^{i_n}_{\mu_{n-1}\mu_n}. \tag{18.7}$$

as shown in Fig. 18.2(a). Calculating the overlap between different MPS states or calculating individual wavefunction amplitudes $\langle i_1 i_2 ... i_{N-1} i_N | \Psi \rangle$ can be done with contraction algorithms which, for MPS, can be done exactly in $\sim N\chi^3$ operations (see e.g. [13] for a detailed description of standard MPS algorithms). It follows that one can also sample from the distribution $|\langle i_1 i_2 ... i_{N-1} i_N | \Psi \rangle|^2$ within the same complexity. Quantum measurements (sampling of a given qubit followed by its projection) can also be done efficiently in a straightforward manner [20].

To perform a two-qubit gate U between qubit n and qubit $n+1$, one first transforms the MPS into the so-called "canonical form" centered around the qubits of interest, through a series of QR factorizations [13]. This step is crucial for the accuracy of truncations of the MPS. The steps to apply the gate are then shown in Fig. 18.2(b). One first forms the two-qubit tensor

$$T^{i_n i_{n+1}}_{\mu_{n-1}\mu_{n+1}} = \sum_{\mu_n} M(n)^{i_n}_{\mu_{n-1}\mu_n} M(n+1)^{i_{n+1}}_{\mu_n \mu_{n+1}}. \tag{18.8}$$

Then one applies the two-qubit gate U and obtains

$$(T')^{i'_n i'_{n+1}}_{\mu_{n-1}\mu_{n+1}} = \sum_{i_n i_{n+1}} U_{i'_n i'_{n+1}, i_n i_{n+1}} T^{i_n i_{n+1}}_{\mu_{n-1}\mu_{n+1}}. \tag{18.9}$$

In a last stage, considering the tensor T' as a matrix with indices spanned by (i'_n, μ_{n-1}) and (i'_{n+1}, μ_{n+1}), one performs a singular value decomposition and writes

$$(T')^{i'_n i'_{n+1}}_{\mu_{n-1}\mu_{n+1}} = \sum_{\mu_n} X^{i'_n}_{\mu_{n-1}\mu_n} S_{\mu_n} Y^{i'_{n+1}}_{\mu_n \mu_{n+1}} \tag{18.10}$$

where the tensors X and Y are formed of orthogonal vectors while the vector S_μ contains the singular values of T'. Here S_μ has up to 2χ components (irrespective of the nature of the two-qubit gate) so that exact algorithms imply a doubling of χ after each application of a two-qubit gate. In the spirit of DMRG like algorithms, we truncate S_μ and keep only its χ largest components to obtain S'_μ. The new MPS tensors are then simply given by

$$M'(n)^{i_n}_{\mu_{n-1}\mu_n} = X^{i_n}_{\mu_{n-1}\mu_n} S'_{\mu_n} \tag{18.11}$$

$$M'(n+1)^{i_{n+1}}_{\mu_n \mu_{n+1}} = Y^{i_{n+1}}_{\mu_n \mu_{n+1}} \tag{18.12}$$

which completes the algorithm. Overall, the cost of applying a two-qubit gate is dominated by the SVD step which scales as χ^3. We emphasize that such an algorithm can do anything that a quantum computer does but the reverse statement is not true: in the MPS approach, one holds the full wavefunction in memory which provides much more information than can be obtained from samples of the wavefunction. For instance, one can compute bipartite entanglement entropy of an MPS, and it is straightforward to calculate quantities such as observables or correlation functions without any statistical errors. The MPS format also satisfies the sample and query access criteria needed for quantum inspired de-quantizing algorithms [21].

18.3.2 Random Quantum Circuit

Fig. 18.1a shows the quantum circuit used in our numerical experiments. It consists of alternating layers of one-qubit and two-qubit gates. This circuit has been designed following the proposal of [3] in order to create strongly entangled states in as few operations as possible. It it believed to be one of the most difficult circuit to simulate on a classical computer since its many-qubit quantum state is extremely sensitive to modification of any of the gates. The one-qubit gates U_n represented as colored squares in Fig. 18.1a are chosen randomly such as to remove any structure or symmetry from the many qubit state. A gate U_n is a rotation $U_n = \exp(-i\theta_n \vec{\sigma}.\vec{m}_n)$ of angle θ_n around a unit vector $\vec{m}_n = (\sin\alpha_n \cos\phi_n, \sin\alpha_n \sin\phi_n, \cos\alpha_n)$ ($\vec{\sigma}$ is the vector of Pauli matrices). We take the angles θ_n, α_n, and ϕ_n to be uniformly distributed (note that the resulting matrix U_n is *n*ot distributed according to the Haar distribution of $U(2)$). While the U_n are random, the actual sequence used is carefully recorded for comparison with e.g. exact calculations. We call the number of two-qubit gate layers applied the depth D of the circuit, focusing on the number of two-qubit gate layers because those are the only source of imperfection in our calculations. In real quantum computers, two-qubit gates also dominate the errors over one-qubit gates in terms of fidelity. However real quantum computers also have other sources of error (decoherence, unknown couplings between qubits, leakage to non-computational states...) not present in the algorithm. After a depth $D \sim N$, the state obtained with the circuit of Fig. 18.1a is totally scrambled and well described by a Porter-Thomas distribution. This is illustrated in Fig. 18.3 where the cumulative distribution of $p_x = |\langle x|\Psi\rangle|^2$ is compared to the Porter-Thomas form for various maximum MPS bond dimensions (main panel) and for various depths using exact calculations (inset). One indeed observes that the distribution quickly approaches the chaotic Porter-Thomas distribution as one increases the bond dimension χ.

18.3.3 Effective two-qubit gate fidelity

Let us introduce the main quantity of interest for this study, the effective two-qubit fidelity f_n. The effective two-qubit fidelity f_n is the computational analogue to the fidelity reported experimentally for two-qubit gates. $f_n = 1$ for a perfect calculation, but the truncation of the MPS will induce $0 < f_n < 1$.

Let us call $|\Psi_T(n)\rangle$ the MPS state after a sequence of n individual two-qubit gates ($n \approx (N-1)D/2$ for the circuit of Fig. 18.1a). Up to irrelevant one-qubit gates, $|\Psi_T(n)\rangle$ is obtained by applying one Control-Z gate C_Z onto $|\Psi_T(n-1)\rangle$ followed by the truncation operation which introduces a finite error. We define the effective fidelity f_n as,

$$f_n = |\langle \Psi_T(n)|C_Z|\Psi_T(n-1)\rangle|^2 \tag{18.13}$$

and the corresponding error rate ϵ_n as,

$$\epsilon_n = 1 - f_n. \tag{18.14}$$

f_n can be calculated using the contraction algorithm in $N\chi^3$ operations. However, when the MPS is in canonical form, f_n is simply obtained without any additional calculations as,

$$f_n = \left(\sum_{\mu=1}^{\chi} S_\mu^2\right) / \left(\sum_{\mu=1}^{2\chi} S_\mu^2\right) \tag{18.15}$$

where recall that 2χ is the maximum possible number of non-zero singular values of the tensor T' in Eq. (18.10). The denominator above is always equal to one for a state which is normalized before it is acted on by a two-qubit gate. We have explicitly checked the equivalence between the two algorithms.

A typical simulation is shown in Fig. 18.4 for the circuit with the Control-Z gate. At small depth $D < 2\log_2\chi$, the simulation is exact and $f_n = 1$. Above this threshold, one starts to truncate the MPS after each two-qubit gate. We observe a transient regime where f_n decreases after which f_n quickly saturates at a constant value, here around 0.988. The first thing to notice in Fig. 18.4 is that these simulations are many orders of magnitude easier than an equivalent *perfect* calculation: simulating the exact state for $N = 60$ and $D = 200$ would be out of reach even with thousand of years of computing time on the largest existing supercomputer. Yet here, these simulations of a *noisy* quantum computer have been performed on a laptop. The averaged fidelity for a modest $\chi = 64$ is better than 99% which already corresponds to qubits of very good quality. This is rather remarkable since the percentage of the Hilbert space spanned by the MPS ansatz is only a very tiny fraction $\sim 10^{-13}$ percent of the whole Hilbert space. After the transient regime, f_n is, up to some fluctuations, independent of both D and N. The second statement is true up to small $1/N$ corrections. These corrections arise from the fact that the fidelity associated with gates applied on the edge of the system (i.e. associated to matrices $M(i)$ with $i < 2\log_2\chi$ or $N - i < 2\log_2\chi$) is always equal to unity since the entanglement entropy associated to the subsystem of qubits $i < a$ is bounded by $S \leq a\log 2$.

Our main goal is to understand how the residual error $\epsilon_n = 1 - f_n$ decreases as one increases the bond dimension χ. As χ approaches $\chi = 2^{N/2}$, one must have $\epsilon_n \to 0$. This is because reshaping the wavefunction as a $2^{N/2} \times 2^{N/2}$ matrix implies a maximum rank of $2^{N/2}$ for any factorization of the wavefunction, thus an MPS with $\chi = 2^{N/2}$ remains exact. However, here we are interested in the regime $\chi \ll 2^{N/2}$ which remains accessible to simulations. Fig. 18.5 shows how the residual error $\epsilon_n = 1 - f_n$ decreases with increasing the bond dimension. The main finding of Fig. 18.5 is that the residual error per gate at large depth D and number of particle N eventually saturates at a finite value, in this case around $\epsilon_\infty \approx 10^{-2}$. In other words, this algorithm can simulate any 1D quantum computer that has a two-qubit gate fidelity smaller than $f_\infty = 99\%$ *at a linear cost in both* N *and* D. As the depth or number of qubits is reduced, the average fidelity increases. The black cross in Fig. 18.5 corresponds to a calculation where only the last part of the circuit has been taken into account in the calculation of the average fidelity, i.e. the average is performed for $D > 100$ where the system has already entered its stationary regime. Note that in that regime, there remains a small logarithmic decrease of the error: as χ increases a number $\propto \log_2\chi$ of gates close to the edges of the system become exact, as discussed above. The black line in Fig. 18.5 corresponds to calculation made in a larger system of $N = 240$ qubits where we have restricted the calculation of the fidelity to the gates for qubits in the center of the system (i.e. away from the edges where the fidelity is perfect) as well as removed the small depth regime (only gates for $100 \leq D \leq 200$ are taken into account). For this case, we observe a clear saturation of the error rate to a finite value ϵ_∞. As we shall see, decreasing the error rate beyond ϵ_∞ requires an exponential effort.

18.4 Links between two-qubit and multi-qubit fidelity

Before investigating the origin of ϵ_∞, we make a short detour to discuss how the effective two-qubit fidelity f_n is related to the actual N-qubit fidelity $\mathcal{F}$ of the state and is related to practical estimates of the fidelity that can be measured experimentally.

18.4.1 Multi-qubit fidelity

Let us call $|\Psi_P(n)\rangle$ the exact perfect state after n two-qubit gates—meaning it is never truncated or otherwise approximated at any stage of its evolution by the circuit—while $|\Psi_T(n)\rangle$

is the truncated MPS state (P stands for Perfect and T for Truncated). The N-qubit fidelity $\mathcal{F}$ is defined as,

$$\mathcal{F}(n) = |\langle \Psi_P(n) | \Psi_T(n) \rangle|^2 \tag{18.16}$$

The fidelity $\mathcal{F}$ is a direct measure of how reliable is our truncated state. As the errors accumulate, it is natural to expect that the fidelities f_n are multiplicative,

$$\mathcal{F}(n) \approx \prod_{i=1}^{n} f_i. \tag{18.17}$$

Eq. (18.17) is indeed a very accurate approximation. An analytical argument will be given below. The validity of Eq. (18.17) can also been shown by numerical simulations. Fig. 18.6 shows the fidelity versus D for $N = 20$ particles obtained in two independent ways. The symbols corresponds to a direct calculation of $\mathcal{F}$ while the lines correspond to the the right hand side of Eq. (18.17). We find an almost perfect match in all the regimes that we have studied. Eq. (18.17) is a very useful result: it relates a property of the perfect state (left hand side) to a property solely defined in terms of the MPS (right hand side). It allows us to easily estimate the fidelity in regimes where we do not have access to the exact state anymore. When f_n has reached its stationary value f_∞, Eq. (18.17) simplifies into

$$\mathcal{F}(n) \approx (f_\infty)^n \sim (f_\infty)^{\frac{ND}{2}}. \tag{18.18}$$

In an actual experiment, one cannot measure the f_n but rather one has access to an estimate of $\mathcal{F}(n)$ (see the subsection below). To compare the accuracy of the simulations with the capabilities of actual quantum chips, we therefore define the average two-qubit fidelity f_{av} after n two-qubit gates,

$$f_{\text{av}} = \left(\prod_{i=1}^{n} f_i \right)^{1/n} \approx \mathcal{F}(D)^{\frac{2}{ND}} \tag{18.19}$$

where the second equality is specific to the quantum circuit studied here.

Derivation of Eq. (18.17). Let us define a full basis of orthogonal states $|\alpha\rangle$ such that state $|1\rangle \equiv |\Psi_T(n-1)\rangle$ is our truncated state and we complement state $|1\rangle$ with an arbitrary basis. Writing $|\Psi_P(n-1)\rangle$ in that basis as $|\Psi_P(n-1)\rangle = \sum_{\alpha=1}^{2^N} p_\alpha |\alpha\rangle$, we have $p_1 = \sqrt{\mathcal{F}(n-1)}$. Similarly, we write $|\Psi_T(n)\rangle = \sum_{i=1}^{2^N} t_\alpha C_Z |\alpha\rangle$ with $t_1 = \sqrt{f_n}$. From these definitions, the fact that C_Z is unitary and that $|\Psi_P(n)\rangle = C_Z |\Psi_P(n-1)\rangle$, we have,

$$\mathcal{F}(n) = \left[\sum_{\alpha=1}^{2^N} p_\alpha t_\alpha \right]^2 = \left[\sqrt{\mathcal{F}(n-1) f_n} + \sum_{\alpha=2}^{2^N} p_\alpha t_\alpha \right]^2 \tag{18.20}$$

As the fidelity goes down, the p_α and t_α become increasingly decorrelated, in particular in sign. Assuming random signs between the p_α and the t_α and using that $p_\alpha \sim 1/\sqrt{2^N}$, we find that the second term in the above equation is at most of order $1/\sqrt{2^N}$ and is therefore negligible. Eq. (18.17) follows directly.

We end this subsection by proving a weaker but exact bound for shallow circuits without the above assumption.

The Schwartz inequality implies that,

$$\left(\sum_{\alpha=2}^{2^N} p_\alpha t_\alpha \right)^2 \leq \sum_{\alpha=2}^{2^N} p_\alpha^2 \sum_{\alpha=2}^{2^N} t_\alpha^2 \leq \epsilon_n \tag{18.21}$$

from which we obtain,

$$|\sqrt{\mathcal{F}(n)} - \sqrt{f_n \mathcal{F}(n-1)}| \leq \sqrt{\epsilon_n} \tag{18.22}$$

The Eq. (18.22) bound is exact, but saturating this bound in practice implies that all the terms $p_\alpha t_\alpha$ interfere constructively which is not realized in actual circuits. Eq. (18.22) implies that,

$$\begin{aligned} \mathcal{F}(n) &\geq \left(\sqrt{f_n \mathcal{F}(n-1)} - \sqrt{\epsilon_n}\right)^2 \\ &\geq \mathcal{F}(n-1) - 2\sqrt{\epsilon_n} \end{aligned} \tag{18.23}$$

from which one can prove that,

$$\mathcal{F}(n) \geq 1 - 2\sum_{i=1}^{n} \sqrt{\epsilon_i} \tag{18.24}$$

The exact statement Eq. (18.24) can be useful for small depth circuits where the actual decrease of the fidelity $\mathcal{F}(n)$ is indeed linear with n, before one enters into the true exponential regime.

18.4.2 Other fidelity metrics

So far we have used the overlap $\mathcal{F}$ between the exact state $|\Psi_P\rangle$ and our approximate state $|\Psi_T\rangle$ as our metric for the fidelity of the calculation. It is a natural metric as it measures the probability for the approximate state to be in the exact state one. It is bounded $0 \leq \mathcal{F} \leq 1$ and is nicely related to the probabilities per gate f_n through the formulas of the preceding subsection.

However $\mathcal{F}$ cannot be directly measured experimentally, so that other fidelity metrics must be designed. Indeed, in an actual quantum computer, the only existing output are samples of bitstrings $x = i_1 i_2 ... i_N$ distributed according to $|\langle x|\Psi_T\rangle|^2$. A natural metric is the cross entropy defined as

$$\mathcal{C} = -\sum_x |\langle x|\Psi_T\rangle|^2 \log |\langle x|\Psi_P\rangle|^2 \tag{18.25}$$

Cross entropy is a standard tool of machine learning and has several interesting properties. First it is measurable through sampling as

$$\mathcal{C} = -\lim_{M\to\infty} \frac{1}{M} \sum_{m=1}^{M} \log |\langle x_m|\Psi_P\rangle|^2 \tag{18.26}$$

where the x_m are the output of the quantum computer when the experiment is repeated M times. Second, the cross entropy between two distributions $|\langle x|\Psi_T\rangle|^2$ and $|\langle x|\Psi_P\rangle|^2$ is maximum when the two distribution are identical. Hence it is a genuine measure of the likelihood of the two distributions. Cross entropy was proposed in [3] as a fidelity metric. Note however that the cross entropy is not a symmetric function of the two distributions. In particular it is strongly affected by particular configurations x where $|\langle x|\Psi_P\rangle|^2$ is very low but $|\langle x|\Psi_T\rangle|^2$ is not.

Cross entropy was eventually abandoned by the Google team and replaced [4] by the cross entropy benchmarking (XEB) defined as

$$\mathcal{B} = -1 + 2^N \sum_x |\langle x|\Psi_T\rangle|^2 |\langle x|\Psi_P\rangle|^2 \tag{18.27}$$

XEB is also sampleable and is symmetric with respect to the two distributions. When the approximate state is the uniform distribution, the XEB metric vanishes, $\mathcal{B} = 0$ indicating a total lack of fidelity. However, when the approximate state is actually exact, the value of the XEB metric can be arbitrary. When the approximate state is exact *and* distributed according

to the Porter Thomas distribution (which happens in our circuits after a few cycles), then the XEB metric gets a well defined $\mathcal{B} = 1$ value. The XEB metric is not in general a good measure of the likelihood between two distributions: for a given perfect state, it is maximum when the approximate state is sharply peaked around the values of x where the perfect state is maximum. In our circuit the initial value of XEB is exponentially high $\mathcal{B} = 2^N - 1$ and quickly decreases as the distribution approaches the Porter-Thomas one. Calling D^* the depth after which XEB has reached unity (ideally D^* would the depth after which $|\langle x|\Psi_P\rangle|^2$ corresponds to Porter-Thomas), we find empirically that

$$\mathcal{F}_n \approx \mathcal{F}(D^*)\mathcal{B}_n \tag{18.28}$$

Equation (18.28) could be used to estimate the actual fidelity $\mathcal{F}$ from XEB measurements.

Figure 18.7 show an example of calculations contrasting the fidelity $\mathcal{F}$ with the XEB metric. Here we have used no truncation but added some noise on the two qubit gate so as to induce a finite fidelity per gate f. We find that both $\mathcal{F}$ and XEB decay exponentially with consistent decay rates. However, the large difference of the initial values at $D = 0$ leads to a shift of the fidelity which is significantly lower than the XEB curve. This shift increases as the fidelity is lowered and corresponds typically to one order of magnitude for a typical experimental value $f = 99\%$.

18.5 Random Tensor Theory of ϵ_∞

We now turn back to the discussion of the asymptotic value f_∞ reached by the two-qubit gate fidelity in our calculations. The first remark of importance is that f_∞ is a property associated with a single tensor of the full MPS state: if we apply a gate between qubit i and qubit $i+1$, only the associated T' tensor defined in Eq. (18.10) comes into play. Since the whole goal of our quantum circuit is to scramble the wavefunction as efficiently as possible, a natural hypothesis is that the tensors $M(i)$ and $M(i+1)$ become eventually well described by totally random tensors. In this section we explore this possibility and calculate the properties of the associated tensor T' as well as the corresponding two-qubit gate fidelity $f_{\rm GTE}$. We find that the distribution of singular values of T' obtained from the random ensemble closely matches what we observe in the MPS state.

In the spirit of random matrix theory [22, 23], we introduce the Gaussian tensor ensemble (GTE) where a tensor $M^i_{\mu\nu}$ is supposed to be totally random. The GTE can be thought of as a "worse case scenario" where the quantum circuit is so chaotic that the tensors are left with no structure. In the GTE, the tensor M are distributed according to

$$P\left[M^i_{\mu\nu}\right] \propto \exp\left[-\frac{1}{2}\sum_{\mu\nu i}|M^i_{\mu\nu}|^2\right] \tag{18.29}$$

where the sum over ν spans $1\dots\chi$, the sum over i spans $0, 1$ and the sum over μ span $1\dots\beta\chi$. In the remaining of this section, we restrict ourselves to $\beta = 1$ which corresponds to the tensors of Eq.(18.6). We shall have an example of $\beta = 2$ for the grouped-qubit algorithm we will discuss in section 18.6. From two such tensors, we apply a two-qubit gate following Eq.(18.8)-(18.12) constructing the associated tensor T and T' and the SVD of T'. From the $2\beta\chi$ singular values S_μ of T', we can obtain the associated fidelity $f_{\rm GTE}$ through Eq. (18.15).

Fig. 18.8 studies the distribution of the singular values S_μ for tensor T' obtained from the GTE. The singular values are sorted in order of decreasing magnitude and plotted as a function of the index $\mu = 1, \dots, 2\chi$. Plotting χS^2_μ as a function of μ/χ, we observe that all the different values of χ collapse onto a single curve. In other words, we find that there is some function

$g(x)$ such that

$$S_\mu^2 = \frac{1}{\chi} g\left(\frac{\mu}{\chi}\right). \tag{18.30}$$

This scaling is already valid for rather small values of χ. This observation can probably be put on firm mathematical grounds - it is consistent with the usual scaling of the semi-circular law of the so-called Gaussian unitary ensemble - but for the moment it is merely an empirical statement made from numerical evidence. It follows from this scaling that f_{GTE} very quickly converges to

$$f_{\mathrm{GTE}} = \frac{\int_0^1 dx\ g(x)}{\int_0^{2\beta} dx\ g(x)}. \tag{18.31}$$

In other word, one finds a finite value of the fidelity that is independent of χ. The resulting f_{GTE} depends on the other hand on the two-qubit gate used. Control-Z (C_Z) and control-NOT (C_X) are equivalent (they are related to each other through a change of basis of the second qubit) and corresponds to $f_{\mathrm{GTE}} = 96.2\%$. Gates like the iSWAP gate (iS) or iSWAP followed by a $\pi/6$ rotation over the z-axis ($iS_{\pi/6}$, close to what is used in [4]) have 4 different singular values which roughly doubles the error with respect to C_Z ($f_{\mathrm{GTE}} = 93.2\%$).

Fig. 18.9 shows how the distribution of the singular values in the GTE compares to the one obtained in the MPS simulation. We find a close agreement between GTE and the MPS simulations when looking at the T' tensor for a gate in the center of the system and at large depth. The agreement is not perfect however, and we observe that the asymptotic fidelity of MPS simulations is always better than the one found in GTE,

$$f_\infty \geq f_{\mathrm{GTE}}. \tag{18.32}$$

To try and understand why the inequality in Eq. (18.32) is not saturated, we plot in Fig. 18.9 the distribution of the singular value of the initial tensor M (dotted line). After truncation, the distribution of the singular values of M' are given by the dashed line restricted to $0 \leq \mu/\chi \leq 1$ (up to a small shift due to the normalization of the state). These two distributions differ very significantly. In order to saturate the bound of Eq. (18.32) we would need extra steps to scramble the distribution of M' back to the distribution of M (i.e. go from the dashed line to the dotted line). However, since in our protocol only a single one-qubit gate separates one truncation from the next one, we find that it is not sufficiently chaotic and therefore we never reach the "worse case scenario" of the GTE.

To summarize, f_{GTE} can be thought as a lower bound for the fidelity found in the simulations for large enough χ (typically $\chi \geq 300$ in practice) and large enough depth. Getting beyond the asymptotic value requires algorithms that have an exponential cost. In the following section we describe possible strategies.

18.6 Algorithms for getting beyond ϵ_∞

The algorithm discussed above can also be used for 2D arrays, since any two qubit gates between distant qubits can always be written as a combination of gates on neighboring qubits using SWAP gates. However, this is inefficient and leads to a decrease of the effective f as the transverse dimension of the 2D array increases. Another limitation of the above algorithm is that one cannot efficiently simulate systems that have a fidelity above f_∞.

There are multiple strategies that could be used to go beyond the above algorithm. In particular, recent progress in the algorithms for contracting tensor networks, such as [9] could be interesting candidates in 2D. Below, we follow a very simple strategy where we keep using MPS states, but group the qubits so that each tensor now represents several qubits.

18.6.1 Grouped MPS State and Extraction Algorithm

We now consider the MPS structure sketched in Fig. 18.1c where each tensor addresses several qubits. We now have $P \leq N$ tensors $M(n)$ each addressing N_n qubits with $\sum_{n=1}^{P} N_n = N$. The tensors $M(1)$ and $M(P)$ possess $N_n + 1$ indices while the others possess $N_n + 2$ indices,

$$M(n)_{\mu\nu}^{i_1 i_2 \ldots i_{N_n}} \tag{18.33}$$

The number of elements of these tensors is $\chi^2 2^{N_n}$ so that the computing time now increases exponentially with the number of qubits per tensor. On the other hand, the two qubit gates that are performed inside a given tensor $M(n)$ are now handled exactly, so that the average fidelity of a circuit increases.

To perform a two-qubit gate between neighboring tensors $M(n)$ and $M(n+1)$, one proceeds in three steps. The first two are shown diagrammatically in Fig. 18.10. In the first step, one performs a QR decomposition of the two tensors to "extract" smaller tensors corresponding to the involved qubits. Assuming (without loss of generality) that the two qubit gate involves qubit N_n of tensor $M(n)$ and qubit 1 of tensor $M(n+1)$, one decomposes $M(n)$ as

$$M(n)_{\mu\nu}^{i_1 i_2 \ldots i_{N_n}} = \sum_{\sigma=1}^{2\chi} Q(n)_{\mu,\sigma}^{i_1 i_2 \ldots i_{N_n - 1}} R(n)_{\sigma,\nu}^{i_{N_n}} \tag{18.34}$$

where the "vectors" of $Q(n)$ indexed by σ are orthonormal. The important point here is that the index σ takes only 2χ values. Similarly, we write:

$$M(n+1)_{\nu\rho}^{i'_1 i'_2 \ldots i'_{N_{n+1}}} = \sum_{\sigma=1}^{2\chi} R(n+1)_{\nu,\sigma'}^{i'_1} Q(n+1)_{\sigma',\rho}^{i'_2 \ldots i'_{N_{n+1}}} \tag{18.35}$$

The second step follows Eqs. (18.8)-(18.12) of the algorithm of Section 18.3 with the replacement $M(n) \to R(n)$ and $M(n+1) \to R(n+1)$, and is shown for the present case in Fig. 18.10(b). In the last step the new tensors $M'(n)$ and $M'(n+1)$ are obtained by contracting $Q(n)$ with $R'(n)$ and $R'(n+1)$ with $Q(n+1)$.

The main difference between the algorithm of Section 18.3 and the grouped MPS algorithm is that the resulting tensor T' of Eq. (18.10) now has 4χ singular values instead of 2χ. As a result, upon truncation to keep only χ singular values, we anticipate that the fidelity per gate will be smaller than in the 1D case. However, as we shall see, this decrease will be more than compensated by the gain of having perfect gates within one tensor. In the terminology of random tensors, the grouped MPS algorithm corresponds to $\beta = 2$. For the C_Z gate, the GTE fidelity drops from $f_{\rm GTE}(\beta = 1) = 96.2\%$ down to $f_{\rm GTE}(\beta = 2) = 87.4\%$.

18.6.2 Application to a two dimensional circuit

We now show the results of simulations performed on a 2D circuit. To put the results into the perspective of what can be achieved experimentally, we choose a circuit very close to the one used by the Google team in their "supremacy" experiment [4]. We consider a 2D grid of 54 qubits as shown in Fig. 18.11a. The circuit is shown in Fig. 18.11b and alternates one-qubit gates applied to each qubit (same distribution as in the 1D case) with two-qubits gates (Control-Z) applied on different pairs of qubits according to the color shown. Except for the choices of one- and two-qubit gates, and the number of qubits (53 versus 54), the setup is identical to the "supremacy sequence" of the Google experiment [4]. In Ref.[4] a XEB fidelity $\mathcal{B} = 0.002$ was reached after a depth $D = 20$ corresponding to a total of 430 two-qubit gates. Ignoring the difference between XEB and the fidelity $\mathcal{F}$, this translates into $\epsilon_{\rm av} = 1.4\%$ which we shall use as our reference value to evaluate the performance of the grouped MPS algorithm.

Fig. 18.11c shows various strategies for grouping the qubits. The $[1^{12}]$ grouping corresponds to 12 tensors that contains one column of qubit each (i.e. alternatively 5 and 4 qubits). The $[6, 6]$ grouping is the most expensive computationally with two tensors of 27 qubit each. Note that the tensors on the edges are less computationally costly than the middle ones, since they only have one bond index. The results of the simulations are shown in Fig. 18.12 for a depth of $D = 20$. While the error rate is significantly larger than in the 1D case, we find that it can be brought down to less than 1.4% (which corresponds to a global fidelity of $\mathcal{F} = 0.002$) on a single core computer. The computing times of the data points of Fig. 18.12 range from a few seconds to less than 48 hours for the most expensive points on a non-parallel code (single core calculation). We find that the grouping strategy is effective, but not as efficient as the maximum gain that one could expect: even though some of the gates become perfect upon grouping, we observe a decrease of the fidelity for the noisy gates which reduces the overall gain. For $\chi = 320$ and the $[4, 2, 2, 4]$ partition where the final fidelity is slightly better than $\mathcal{F} = 0.002$ (see Fig. 18.12), the memory footprint of the calculation is 4.5 GB of memory which represents only 1.5×10^{-6} percent of the size of the total Hilbert space spanned by the 2^{54} qubits.

18.6.3 Split-and-Merge algorithm for more complex gates

We end this article with results in a configuration that closely matches the one of Ref. [4]. The one-qubit gates are chosen at random between $\sqrt{X}$, $\sqrt{Y}$ and $\sqrt{W}$ while the two-qubit gate iS_θ is a combination of iSWAP followed by a controlled rotation along the z axis

$$iS_\theta = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & -i & 0 \\ 0 & -i & 0 & 0 \\ 0 & 0 & 0 & e^{-i\theta} \end{pmatrix} \tag{18.36}$$

This gate has four different singular values and is therefore expected to produce more entanglement than the C_Z gate. The link between number of singular values and the actual growth of entanglement is not totally straightforward, however. Indeed, the pure iSWAP gate has four different singular values ± 1 and $\pm i$; yet as it preserves the structure of product states, it is trivial to simulate with perfect fidelity. In what follows, we use $\theta = 1$ which is non-trivial to simulate.

The algorithm of the previous subsection behaves rather poorly for the iS_θ gate. For instance, for $\chi = 128$, and the $[4, 2, 2, 4]$ grouping, the two-qubit gate fidelity drops from $f \approx 98\%$ (C_Z) to $f \approx 92\%$ (iS_θ). However, a simple modification of the algorithm allows one to recover a much higher fidelity $f \approx 95\%$.

To study iS_θ, we therefore switch to a "Split-and-Merge" strategy: instead of "extracting" qubits one-by-one to perform two-qubit gates as in Section 18.6.1, we extract one full column of qubits at a time. In the Split-and-Merge strategy, we use two different groupings of the qubits, for instance switching between the $[4, 2, 2, 4]$ grouping and the $[5, 2, 5]$ grouping (hereafter referred to as the $[4, 2, 2, 4] \leftrightarrow [5, 2, 5]$ grouping strategy). Switching from one grouping to another induces truncation errors. However, once the switching has been done, many two-qubit gates can be performed exactly. A schematic of the Split and Merge strategy is shown in Fig. 18.13 for the $[4, 2, 2, 4] \leftrightarrow [5, 2, 5]$ case.

Fig. 18.14 shows our numerical results for ϵ_{av} versus χ. The curves are very similar to those obtained for C_Z at similar computational cost, but with an error rate roughly three times larger than with C_Z.

To conclude this section, we have shown that for the Control-Z gate a simple grouping strategy allows one to reach the same fidelity as the Google experiment [4] in a matter of hours on a single core computer (i.e. $f_{\rm av} \geq 98.6\%$). For the more challenging iS_θ gate, this fidelity drops down to 95% for similar computing time.

A natural question that arises is whether these algorithms may be used to defeat the claim of quantum supremacy put forward in [4], i.e. raise the fidelity from 95% to $> 98\%$. We have not be able to do so on a single core implementation. However, the Split-and-Merge is to a large extent trivially parallelizable since most tensor operations contain "spectator" indices whose different values can be fixed, and the resulting tensor "slices" dispatched to different computing cores or nodes. Extrapolations from our results suggest that such a parallel implementation should be able to reach fidelities in the $98 - 99\%$ range with a few hundred cores and a few terabytes of memory. However, such a calculation has not be attempted at the moment. Let us note, in any case, that not too much emphasis should be put on quantum supremacy by itself. It is not because a task is difficult to simulate that it provides a useful output. Also, there is no question that quantum many-body problems are extremely difficult to simulate. The insight that we get from the present work is an estimate of the relation between the accuracy reached in the quantum state and the underlying amount of entanglement that could potentially be exploited.

18.7 Discussion

In this work, we have discussed a practical algorithm that allows to simulate a quantum computer in a time which grows linearly with the number of qubits N and the depth D at the cost of having a finite fidelity f per two-qubit operation. The fidelity f can be increased at a polynomial cost up to a finite value f_∞; increasing it further has an exponential cost in the fidelity. Our main observation is that fidelities of the order of 99%, which are typical fidelities found in state of the art experiments, can be reproduced at a moderate computational cost.

Is a fidelity of 99% large or small? From an experimental physics perspective, it is certainly quite an achievement to keep several dozen qubits at this level of fidelity. From a quantum information and classical algorithms point of view, a question is what is the level of entanglement—hence the actual fraction of the Hilbert space that can truly been accessed—associated with this level of fidelity. Our MPS ansatz can provide an estimate (or at least an upper bound for one may come up with better algorithms) for this fraction. Since the MPS ansatz only spans a very tiny fraction of the overall Hilbert space, it follows that the computational power associated with fidelities in the 99% range is much more limited than the full size 2^N of the Hilbert space would suggest. We conclude that increasing the computational power of a quantum computer will primarily require increasing the fidelity/precision with which the different operations are performed [24]. Secondarily, one could try to improve its connectivity with e.g. quantum buses [25] as we have seen that 1D simulations are far easier than 2D ones. However, increasing the number of qubits will remain ineffective until better fidelities have been reached.

As a side comment, our approach could also be used to get lower bounds for quantum error correction (QEC) schemes [26]. Suppose that for a certain connectivity, one has an algorithm that can reach a fidelity f in polynomial time in N and D. Then, it is reasonable to expect that any QEC code has a threshold $p > f$. If it were not the case, one could build a logical quantum computer with a classical one at a polynomial cost by simply simulating the QEC protocols on the classical computer. In this respect, extending our approach to a truly 2D algorithm (beyond the quasi-1D one discussed in this article) would be particularly interesting. Indeed, 2D surface codes have a particularly low threshold $p \approx 99\%$. How close to $f = 99\%$ can one get at a polynomial cost in 2D is currently an open question.

Finally, it would be interesting to perform a similar study, but of how well MPS of practical sizes can approximate circuits designed for *useful* tasks. Goals could include estimating minimum fidelities needed to perform these tasks with a high success probability and understanding crossovers where useful quantum algorithms begin to offer advantages over classical approaches.

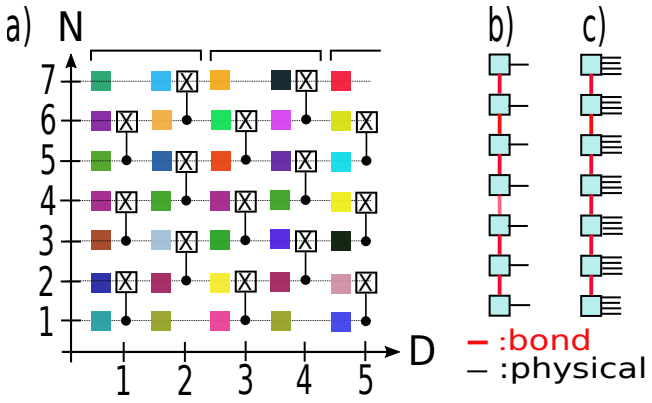


Figure 18.1: a) Sketch of the quantum circuit with N qubits. The colored squares indicate arbitrary one-qubit gates while the dots connected to a cross indicate a two qubit gate such as Control-NOT or Control-Z. The depth D counts the number of two-qubit gates performed in the sequence. b) structure of the Matrix Product States (MPS) for 1D circuits. Red lines indicate bond (or virtual) indices while thin black lines correspond to physical indices. c) MPS structure for quasi-one dimensional structures.

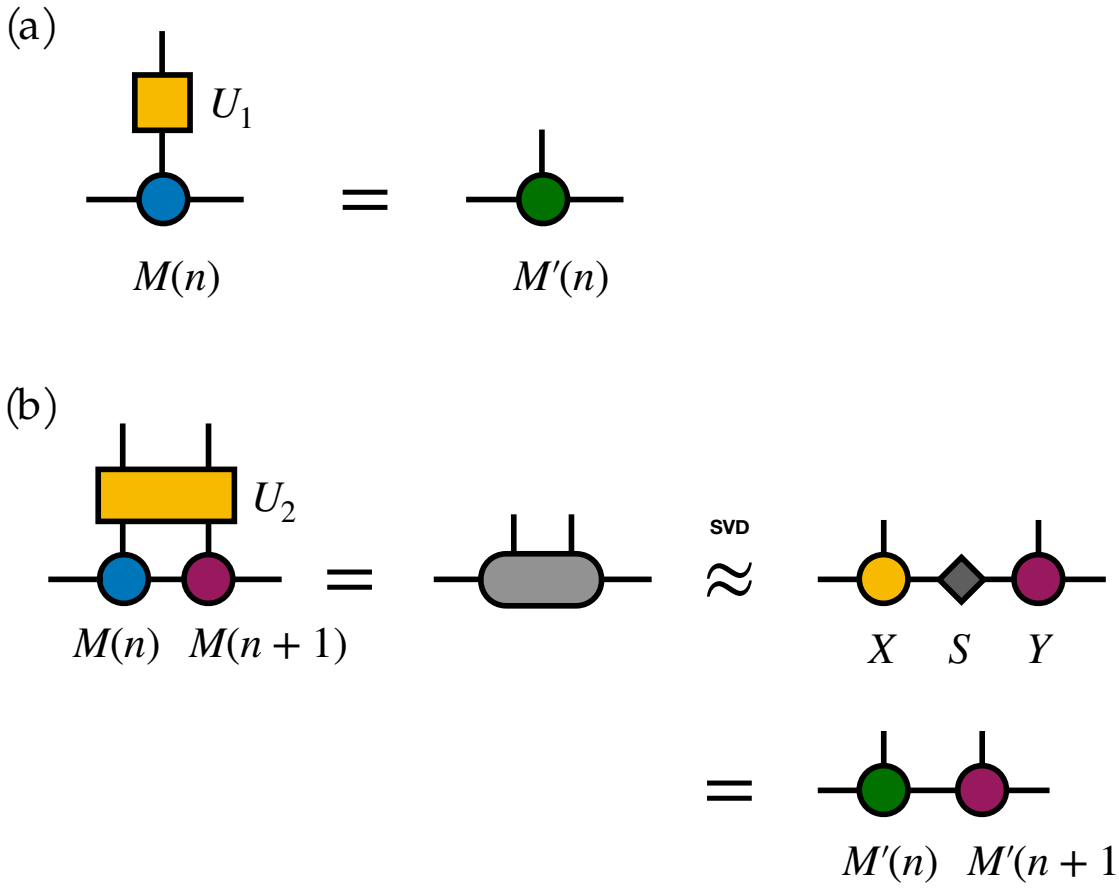


Figure 18.2: (a) Applying a single qubit gate to an MPS can be done without approximation by multiplying the gate by a single MPS tensor. (b) To apply a two-qubit gate to qubits n and $n+1$, one contracts the corresponding tensors together, then applies the gate. To restore the MPS form, the resulting tensor is decomposed with an SVD truncated to keep the largest χ singular values, and the matrix of singular values is multiplied into one of the unitary factors X or Y.

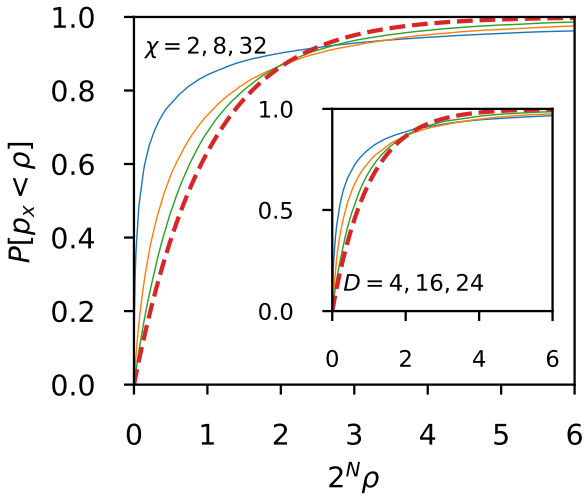


Figure 18.3: Cumulative distribution $P(p_x < \rho)$ where $p_x = |\langle x|\Psi\rangle|^2$ for $N = 15$. The dashed line corresponds to the Porter-Thomas distribution $P_{PT}(\rho) = 1 - (1-\rho)^{2^N-1}$. Main panel: $D = 24$ and various MPS truncation levels $\chi = 2$ (blue), 8 (orange), and 32 (green). Inset: exact results for $D = 2$ (blue), 16 (orange), and 24 (green)

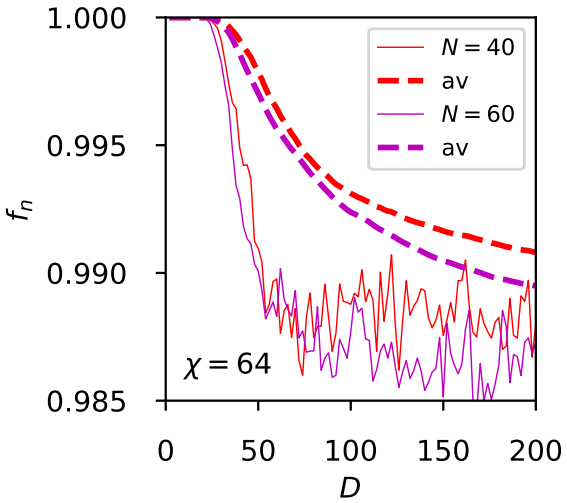


Figure 18.4: Effective two-qubit gate fidelity f_n as a function of the depth D of the circuit for $\chi = 64$ and the Control-Z gate for $N = 40$ (red) and $N = 60$ (magenta). The thin lines correspond to the geometric average of f_n over one full sequence, i.e. all the two-qubits gates performed between depth $D-2$ and depth D ($N-1$ two-qubits gates). The thick dashed lines correspond to f_{av}, the geometric average of f_n over all two-qubit gates since the beginning of the circuit up to depth D.

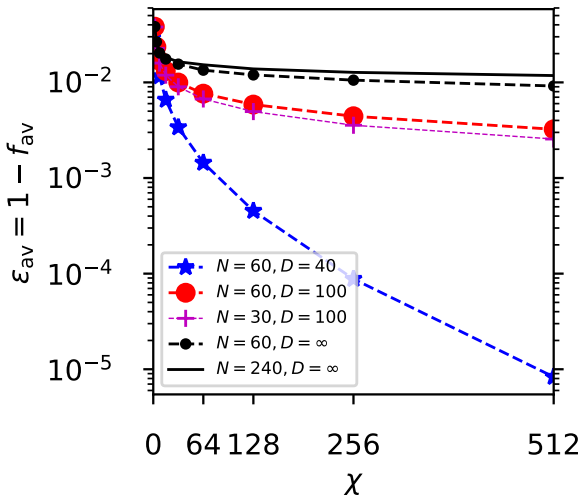


Figure 18.5: Geometric average of the residual error per gate $\epsilon_{\rm av} = 1 - f_{\rm av}$ as a function of the bond dimension χ. The average is performed over the entire circuit except for the black curves ($D = \infty$) where it is restricted to the regime where the fidelity has reached its asymptotic value ($100 \leq D \leq 200$). For the largest system $N = 240$, we have also excluded the gates on the edges of the system in our calculation as they have by construction perfect fidelity.

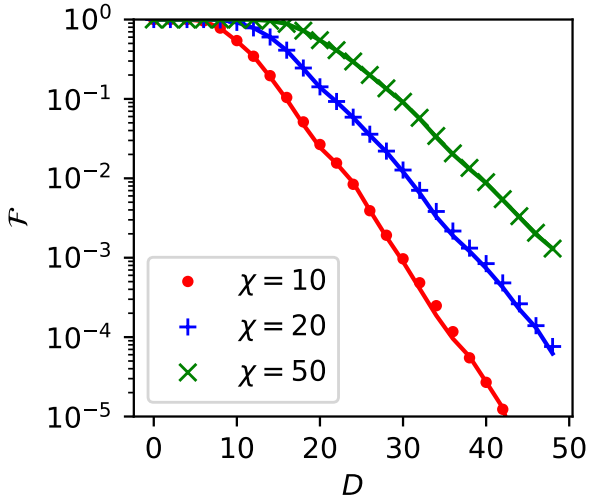


Figure 18.6: Fidelity $\mathcal{F}$ versus depth D for $N = 20$ and various values of $\chi = 10, 20, 50$. The symbols correspond to a direct calculation of $\mathcal{F}$ obtained by comparing with an exact calculation. The lines corresponds to the right hand side of Eq. (18.17).

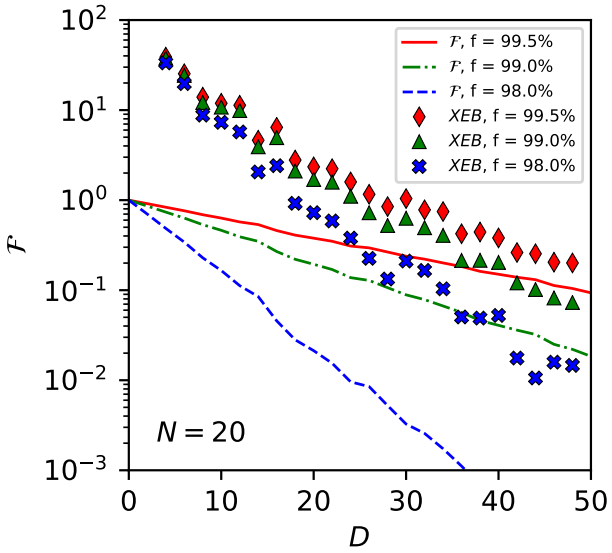


Figure 18.7: Comparison between the fidelity $\mathcal{F}$ (lines) and the XEB metric $\mathcal{B}$ (markers) as a function of depth D. Different colors label different levels of noise on the two-qubit gates, respectively $f = 99.5\%$ (red), $f = 99\%$ (green) and $f = 98\%$ (blue). The calculations were performed for the 1D random circuit with $N = 20$ qubits.

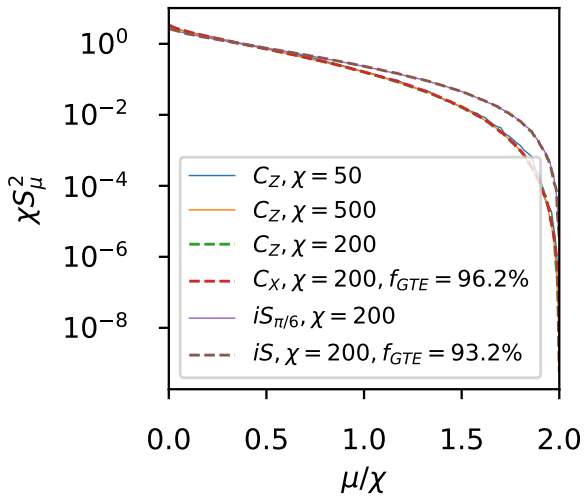


Figure 18.8: Squared singular values S_μ^2 of the matrix T' obtained from the GTE ensemble. We find a perfect scaling of the form $S_\mu^2 = g(\mu/\chi)/\chi$ where μ is the index of the μ^{th} singular value. The two bundles of curves correspond respectively to the C_X,C_Z gates (two non-zero eigenvalues) and the $iS_{\pi/6}/iS$ gates (four non-zero eigenvalues). Within one bundle, the different curves are indistinguishable.

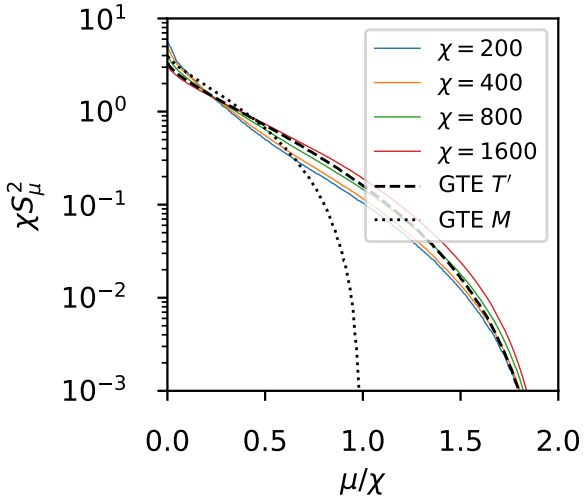


Figure 18.9: Squared singular values S_μ^2 of the matrix T' obtained from the MPS simulations of $N = 30$ qubits and a depth of $D = 60$ for various values of χ. The singular values correspond to a gate C_X performed in the middle of the system. Dotted line: Squared singular values of the M matrix in in the GTE. Dashed line: Squared singular values of T' in the GTE.

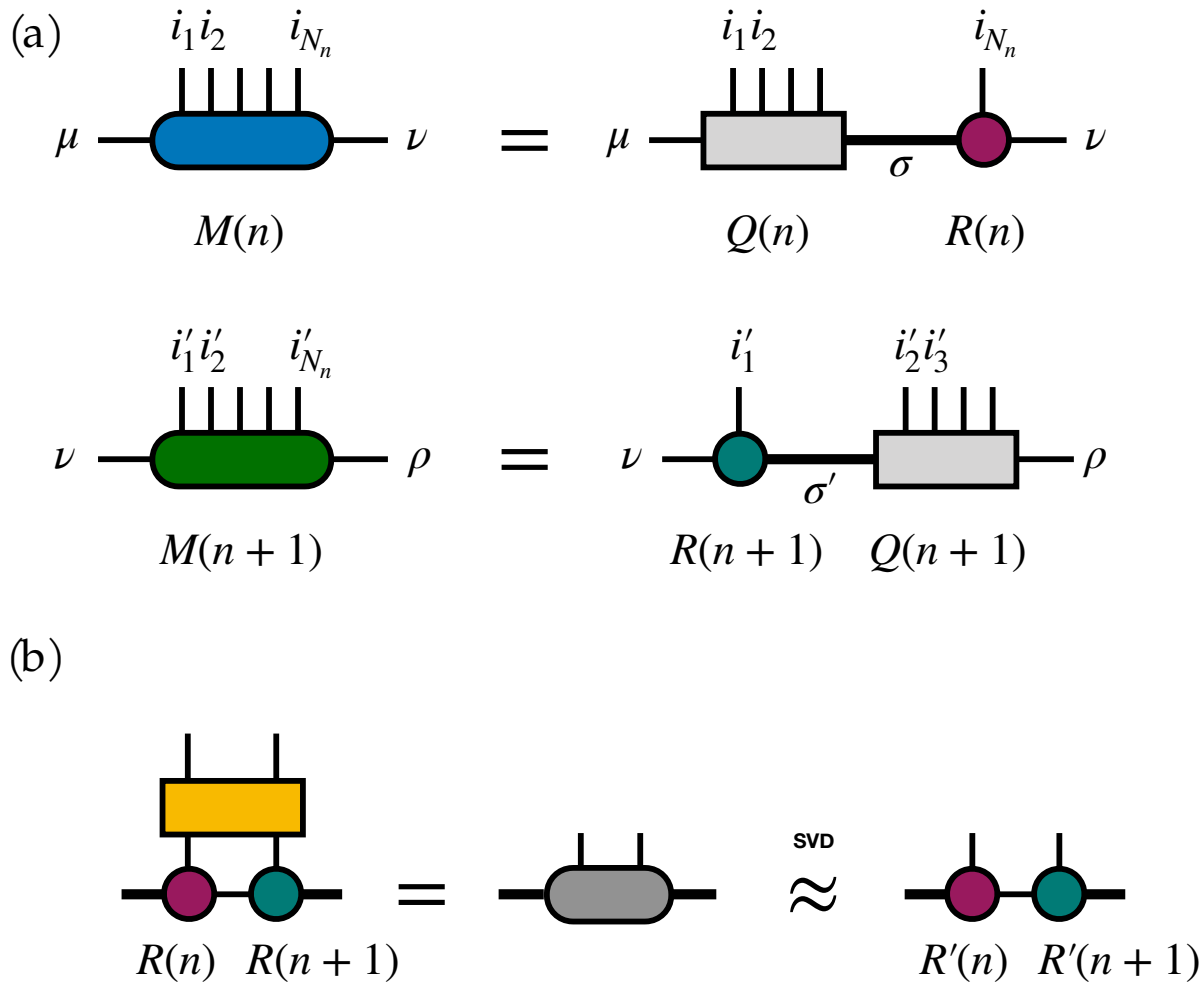


Figure 18.10: Main steps for applying a gate which acts across two grouped MPS tensors, as described in Eqs. (18.34)–(18.35). In (a) the grouped MPS tensors $M(n)$ and $M(n+1)$ are exactly factorized using QR decompositions, such that the $R(n)$ and $R(n+1)$ tensors carry the qubit indices acted on by the gate and the newly introduced indices σ and σ' range over 2χ values. In (b) the gate acts on the product of $R(n)$ and $R(n+1)$, and the resulting tensor is factorized using an SVD truncated to χ singular values. Finally, to update the MPS (not shown), one computes the new tensors $M'(n) = Q(n)R'(n)$ and $M'(n+1) = R'(n+1)Q(n+1)$ which diagrammatically looks like step (a) but in reverse.

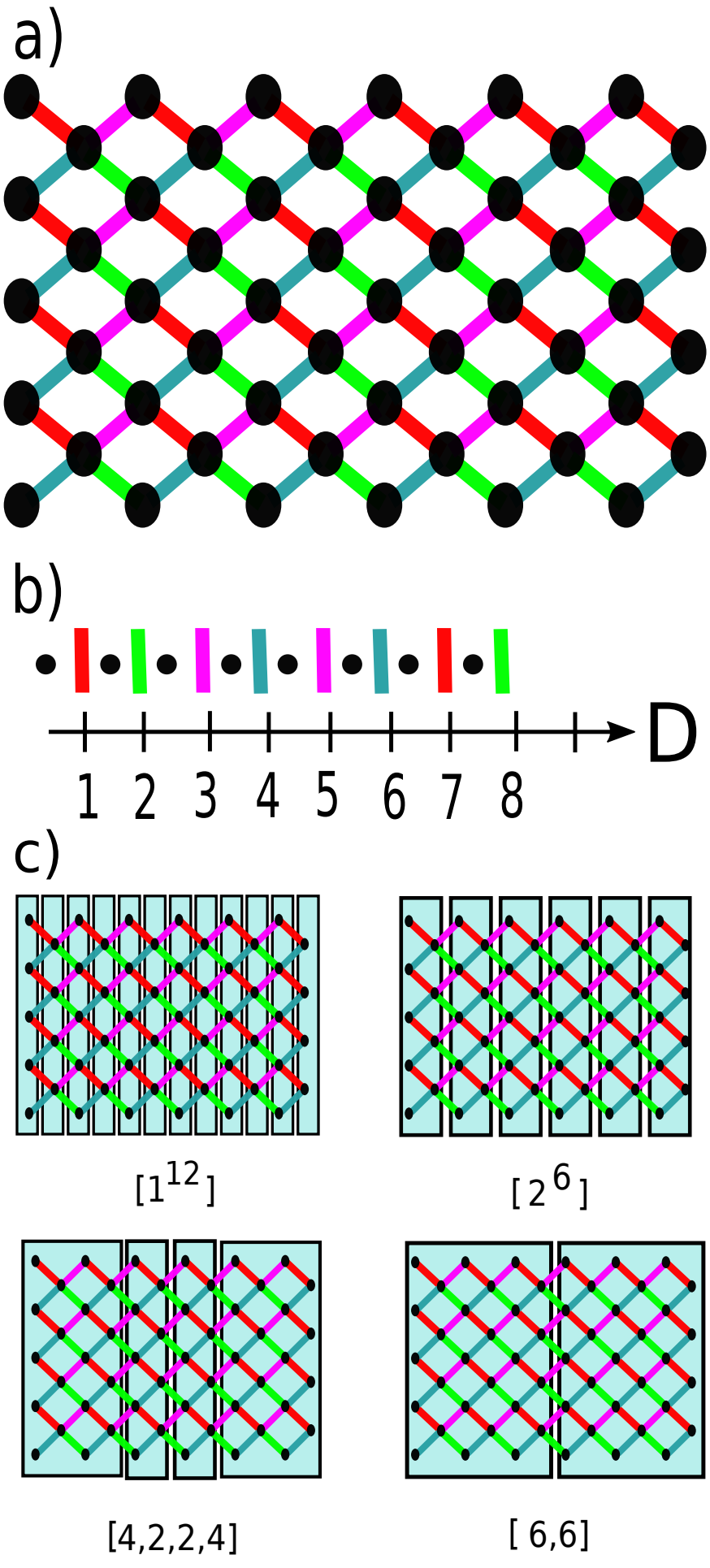


Figure 18.11: a) Sketch of the quantum circuit with 54 qubits in a 2D grid. The qubits are represented by the black dots while the two-qubit gates by the color links. b) The circuit alternates one-qubit gates (black dots) with two-qubit gates (here the Control-Z gate). The

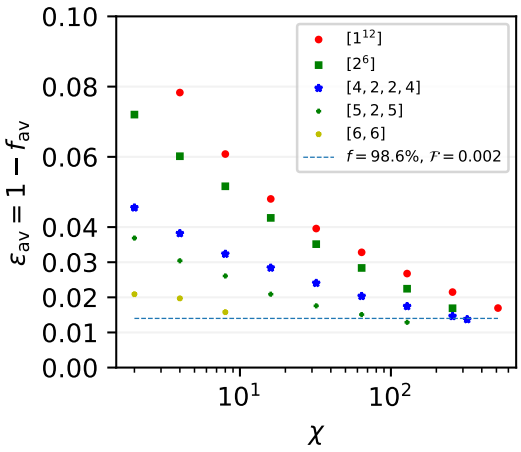


Figure 18.12: Residual error per gate $\epsilon_{\text{av}} = 1 - f_{\text{av}}$ as a function of the bond dimension χ for the $2D$ circuit of Fig. 18.11 for a depth $D = 20$. The different curves correspond to different groupings. The horizontal dashed line corresponds to the error rate associated with a global fidelity $\mathcal{F} = 0.002$.

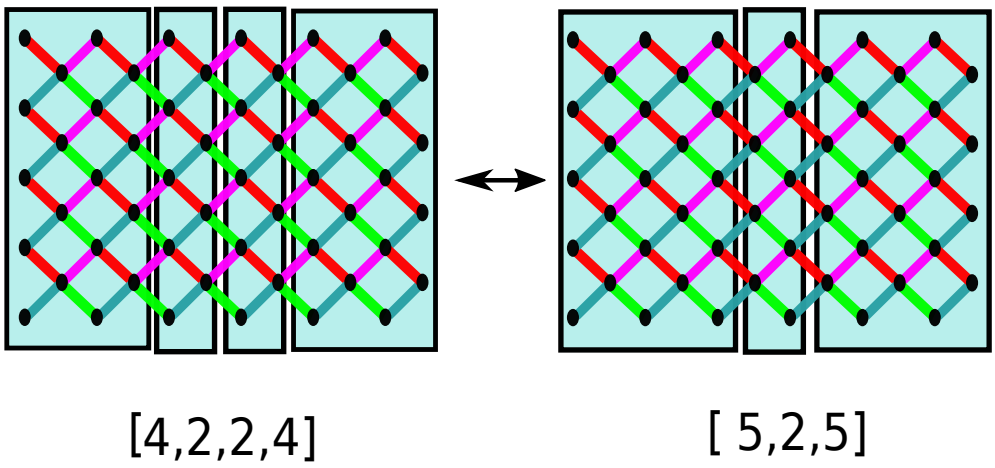


Figure 18.13: Schematic of the Split-and-Merge algorithm for the $[4, 2, 2, 4] \leftrightarrow [5, 2, 5]$. The two-qubit gates shown in red and dark green are performed in the $[4, 2, 2, 4]$ configuration and one switches to the $[5, 2, 5]$ to perform the light green and purple gates.

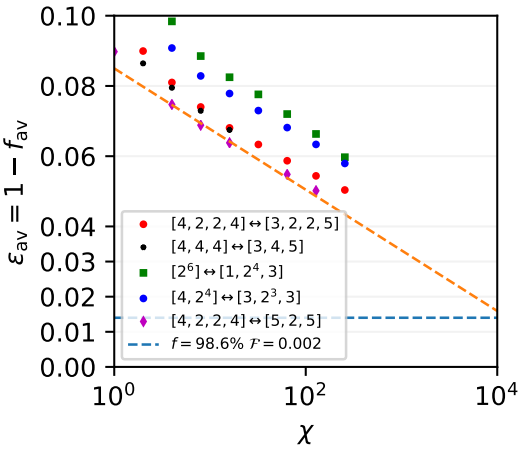


Figure 18.14: Residual error per gate $\epsilon_{\text{av}} = 1 - f_{\text{av}}$ as a function of the bond dimension χ for the iS_θ gate for a 2D circuit with $N = 54$ qubits and a depth $D = 20$. The different curves correspond to different groupings. The horizontal dashed line corresponds to the error rate associated with a global fidelity $\mathcal{F} = 0.002$. The orange line is just a guide to the eye.

19 How the Result of a Measurement of a Component of the Spin of a Spin-$\frac{1}{2}$ Particle Can Turn Out to be 100 by Aharonov, Albert, and Vaidman (1987)

Abstract

We have found that the usual measuring procedure for preselected and postselected ensembles of quantum systems gives unusual results. Under some natural conditions of weakness of the measurement, its result consistently defines a new kind of value for a quantum variable, which we call the weak value. A description of the measurement of the weak value of a component of a spin for an ensemble of preselected and postselected spin-$\frac{1}{2}$ particles is presented.

This paper will describe an experiment which measures a spin component of a spin $-\frac{1}{2}$ particle and yields a result which is far from the range of "allowed" values. We shall start with a brief description of the standard measuring procedure. Considering measurements on an ensemble of preselected and postselected systems, we shall define a new concept: a weak value of a quantum variable. And, finally, we shall describe the measurement of the weak value on the example of a spin $-\frac{1}{2}$ particle.

In quantum theory, the result of a measurement of a variable A which has discrete eigenvalues a_i must necessarily be one of those values. The Hamiltonian of the standard measurement procedure [1,2] is

$$H = -g(t)qA, \tag{1}$$

where $g(t)$ is a normalized function with a compact support near the time of measurement, and q is a canonical variable of the measuring device with a conjugate momentum π. The initial state of the measuring device in the ideal case has to be such that π is well defined. After the interaction (1) we can ascertain the value of A from the final value of π: $A = \delta\pi$.

As a reasonable approximation for a real situation, we may take the initial state of the measuring device as a Gaussian in the q (and consequently also in the π) representation. For this case, the Hamiltonian (1) leads to the transformation

$$\begin{aligned} & e^{-i\int H dt} e^{-\pi^2/4(\Delta\pi)^2} \sum_i \alpha_i \left| A = a_i \right\rangle \\ & = \sum_i a_i e^{-(\pi - a_i)^2/4(\Delta\pi)^2} \left| A = a_i \right\rangle , \end{aligned} \tag{2}$$

where $\sum_i \alpha_i \left| A = a_i \right\rangle$ is the initial state of our system. If the spread of the π distribution $\Delta\pi$ is much smaller than the differences between the a_i, then, after the interaction, we shall be left with the mixture of Gaussians located around a_i correlated with different eigenstates of A. A measurement of π will then indicate the value of A.

In the opposite limit, where $\Delta\pi$ is much bigger than all
a_i, the final probability distribution will be again close to a Gaussian with the spread $\Delta\pi$. The center of the Gaussian will be at the mean value of A : $\langle A \rangle = \Sigma_i \left|\alpha_i\right|^2 a_i$. One measurement like this will give no information because $\Delta\pi \gg \langle A \rangle$; but we can make this same measurement on each member of an ensemble of N particles prepared in the same state, and that will reduce the relevant uncertainty by the factor $1/\sqrt{N}$, while the mean value of the average will remain $\langle A \rangle$. By enlarging the number N of particles in the ensemble, we can make the measurement of $\langle A \rangle$ with any desired precision.

The outcome of the measurement is the average of the obtained values π of the measuring devices. As we explained earlier, it will yield, for a sufficiently large ensemble, the value $\langle A \rangle$. We now raise the question: Can we change the above outcome by taking into account the values of π of only a part of the original ensemble, performing a particular postselection? We may, of course, achieve this rather trivially, by selecting only measuring devices with large values of π which we can always find, since the original distribution of π has nonvanishing tails. But suppose we allow only postselection performed on the particles themselves; how then can we maximize the outcome for the average of π? It might appear at first that the best method for this will be to select all particles for which the final state corresponds to the eigenvalue $a_{\max}$. But this is not the case. Surprisingly, we found that by making other postselections we can obtain much bigger outcomes.

Indeed, we shall now show that the above measurements (with large $\Delta\pi$), when applied to preselected and postselected ensembles, may yield new values which lie outside the "allowed" range, i.e., outside the interval $[\min(a_i), \max(a_i)]$. The procedure of the measurement is as follows. We start with a large ensemble of particles prepared in the same initial state. Every particle interacts with a separate measuring device, and then the measurement which selects the final state is performed. Finally, we take into account only the "readings" of the measuring devices corresponding to the postselected particles.

Let us consider an ensemble of particles with an initial state $|\psi_{\text{in}}\rangle$ and a final state $|\psi_f\rangle$. At a time in between we switch on the interaction (1) where the initial state of each of the measuring devices is $\left[1/\sqrt{\Delta}(2\pi)^{1/4}\right] \times \exp(-q^2/4\Delta^2)$. After the postselection the state of the measuring device (up to a normalization factor) is

$$\begin{aligned} &\langle\psi_f| e^{-i\int H dt} |\psi_{\text{in}}\rangle e^{-q^2/4\Delta^2} \\ &\quad \cong \langle\psi_f|\psi_{\text{in}}\rangle \exp\left(iq\frac{\langle\psi_f| A |\psi_{\text{in}}\rangle}{\langle\psi_f|\psi_{\text{in}}\rangle}\right) e^{-q^2/4\Delta^2} \end{aligned} \tag{3}$$

This formula is valid if the spread Δ is sufficiently small [3]:

$$\Delta \ll \max_n \frac{|\langle\psi_f|\psi_{\text{in}}\rangle|}{\left(|\langle\psi_f| A^n |\psi_{\text{in}}\rangle|^{1/n}\right)} \tag{4}$$

In the π representation, the state of the measuring device is approximately

$$\exp\left[-\Delta^2 (\pi - \langle\psi_f| A |\psi_{\text{in}}\rangle / \langle\psi_f|\psi_{\text{in}}\rangle)^2\right] \tag{5}$$

The standard interpretation of this outcome of the measuring device is that the measured value of A is $\langle\psi_f| A |\psi_{\text{in}}\rangle / \langle\psi_f|\psi_{\text{in}}\rangle$. This is the weak value of A for this preselected and postselected ensemble:

$$A_w \equiv \langle\psi_f| A |\psi_{\text{in}}\rangle / \langle\psi_f|\psi_{\text{in}}\rangle \tag{6}$$

The uncertainty of π for each of the measuring devices is much bigger than the measured value; i.e., $\Delta\pi = 1/2\Delta \gg A_w$ [see Eq. (4)]. However, for an ensemble of N such devices, the uncertainty of the average of π is decreased by the factor of $1/\sqrt{N}$. Therefore, if N is sufficiently large, then $(1/\sqrt{N})\Delta\pi \ll A_w$ and the value of A_w can be ascertained with arbitrary accuracy. As we see from the definition (6). A_w is not bounded by the minimal and the maximal eigenvalues of A.[4]

One may wonder how a superposition of shifts, all smaller than $a_{\max}$, leads to a shift which is much larger than $a_{\max}$. We shall demonstrate this by proving a mathematical identity which

corresponds to the type of experiment considered in the present note (see also Aharonov et al. [5]).

For all functions $f(q)$ which tend to zero faster than exponential, $f(q) < \exp(-\ln \alpha^2 |q|)$, the following equality can be made valid with any precision by our taking N large enough [6]:

$$\sum_{n=-N}^{N} c_n e^{iqn/N} f(q) \cong e^{iaq} f(q) \tag{7}$$

where

$$c_n = \frac{N!}{n!(N-n)!} \left(\frac{1-\alpha^2}{4}\right)^N \left(\frac{1+\alpha}{1-\alpha}\right)^{n/2}$$

The Fourier transform of this equation exhibits the property described above: For function $\tilde{f}(\pi)$ [the Fourier transform of $f(q)$] the superposition of shifts, which are all smaller than 1 , is equivalent to a shift by the arbitrarily large value α, i.e.,

$$\sum_{n=-N}^{N} c_n \tilde{f}(\pi - n/N) \cong \tilde{f}(\pi - \alpha) \tag{8}$$

We shall now describe an experiment that measures the weak value of the z component of a spin- $\frac{1}{2}$ particle and yields an arbitrarily large result for it. A version of this experiment can, we believe, be performed in the laboratory.

We start with a beam of particles moving in the y direction with a well-defined velocity. The particles are initially well localized in the xz plane and have their spins pointed in a direction $\hat{\xi}$. We choose $\hat{\xi}$ in the xz plane with an angle α between $\hat{\xi}$ and $\hat{\mathbf{x}}$ (Fig. 1). The prepared beam comes through a Sterm-Gerlach device which measures the spin weakly in the z direction. The requirement of weakness is fulfilled by our making the gradient of the magnetic field sufficiently small. The motion of the beam changes, therefore, only slightly. This weak measurement causes the spatial part of the wave function to change into a mixture of two slightly shifted functions in the p_z representation, correlated to the two values of σ_z. We then pass the particles through another, normal, Stern-Gerlach device which splits them into two beams corresponding to the two values of σ_x. We keep only the beam with $\sigma_x = 1$, which continues to move freely towards a screen placed in front of it. The screen is placed sufficiently far so that the displacement in the $\hat{\mathbf{z}}$ direction due to the average momentum p_z ac-

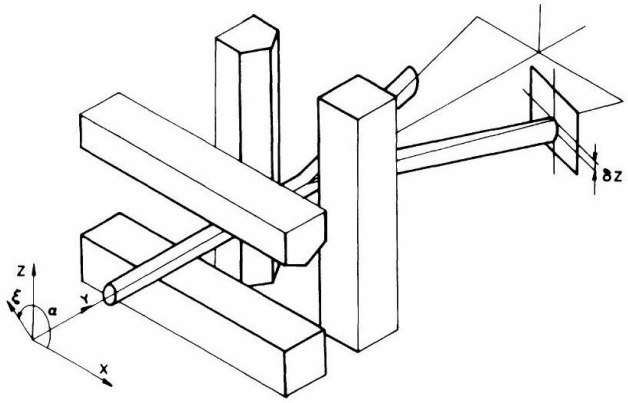


FIG. 1. The experimental device for measurement of the weak value of σ_z. The beam of particles with the spin pointed in the direction $\hat{\boldsymbol{\xi}}$ passes through an inhomogeneous (in the z direction) weak magnetic field and is split by the strong magnet with an inhomogeneous field in the x direction. The beam of particles with $\sigma_x = 1$ comes toward the screen and the deflection of the spot on the screen in the z direction is proportional to the weak value of $\sigma_z : \sigma_{z_w} = (\delta z p_0 \mu / l)\,(\partial B_z/\partial z)^{-1}$.

quired during the above weak interaction will be larger than the initial uncertainty Δz. On the screen we shall obtain a wide spot whose displacement in the direction $\hat{\mathbf{z}}$ is measured. This displacement will yield the weak value of σ_z:

$$\sigma_{z,w} = \langle\uparrow_x| \sigma_z |\uparrow_\xi\rangle / \langle\uparrow_x | \uparrow_\xi\rangle = \tan\frac{1}{2}\alpha \tag{9}$$

A brief mathematical description of this experiment follows. The particles have mass m, magnetic moment μ, and average momentum p_0 in the y direction. Their initial state is

$$|\psi_{\text{in}}\rangle = \Delta^{-3/2}(2\pi)^{-3/4} e^{-x^2/4\Delta^2} e^{-z^2/4\Delta^2} e^{-y^2/4\Delta^2} e^{-ip_0 y} \left(\cos(\alpha/2)\,|\uparrow_x\rangle + \sin(\alpha/2)\,|\downarrow_x\rangle\right) \tag{10}$$

The Hamiltonian of the weak interaction is

$$H_1 = -\mu\,(\partial B_z/\partial z)\, z\sigma_z g\,(y - y_1) \tag{1I}$$

where $g\,(y - y_i)$ has a compact support at the location of the weak Stern-Gerlach device, which is arranged such that $\left(m/p_0 \int g(y)dy = 1\right.$. It is, indeed, essentially a Hamiltonian of the von Neumann type [see Eq. (1)]. Since $y \cong (p_0/m)\,t$, $g\,(y - y_1)$ is effectively a function of time (we arrange the momentum in the y direction such that $p_0 \gg \Delta p_y = 1/2\Delta$); the canonical variable q of Eq. (1) is, here, $\mu\,(\partial B_z/\partial z)\, z$. The change in the momentum in the z direction during the interaction is $\delta p_z = \mu\,(\partial B_z/\ \partial z)\sigma_z$. For our ensemble of preselected and postselected particles, we shall see that $\delta p_z = \mu\,(\partial B_z/\partial z)\tan(\alpha/2)$. The necessary requirement of the weakness of the interaction [see Eq. (4)] is

$$\mu \left|\frac{\partial B_z}{\partial z}\right| \max\left[\left|\tan\frac{\alpha}{2}\right|, 1\right] \ll \Delta p_z = \frac{1}{2\Delta} \tag{12}$$

The Hamiltonian of the second Stern-Gerlach device, which selects the particles with $\sigma_x = 1$, is

$$H_2 = -\mu\,(\partial B_x/\partial x)\, x\sigma_x g\,(y - y_2) \tag{13}$$

The requirement for the splitting of the beam is $\mu\,|\partial B_x/\partial x| \gg \Delta p_x = 1/2\Delta$. If the angle α between the directions of spin in the initial and the final states is close to π, then the requirement has to be stronger, i.e.,

$$\exp\left(-2\Delta^2\mu^2\,|\partial B_x/\partial x|^2 \ll \cot^2(\alpha/2)\right.$$

The direction of the beam with $\sigma_x = 1$ is $\mu\,(\partial B_x/\partial x)\,\hat{\mathbf{x}} + p_0\hat{\mathbf{y}}$. The screen is placed at the distance l such that

$$\frac{l\mu}{p_0}\left|\frac{\partial B_z}{\partial z}\tan\frac{\alpha}{2}\right| \gg \Delta.$$

The wave function of the particle in the z representation, before the collapse on the screen, is approximately

$$\exp\left[-\Delta^2\left(\frac{p_0}{l}\right)^2\left(z - \frac{l\mu}{p_0}\frac{\partial B_z}{\partial z}\tan\frac{\alpha}{2}\right)^2\right] \tag{14}$$

The measured value of the spin component corresponding to this wave function is $\tan(\alpha/2)$. A rough estimation for the number N of particles in the initial beam necessary for our obtaining accuracy of $1/M$ is $N \cong M^3/\cos^2(\alpha/2)$.

In the above description we have not, so far, taken into account the influence of $\partial B_x/\partial x$ and $\partial B_y/\partial y$ which cannot both vanish since $\operatorname{div}\mathbf{B} = 0$. In a standard SternGerlach experiment, one takes care of this problem by adding a large constant magnetic field in the direction of the measured component of the spin. It is interesting to note that the same method can be used in our weak measurement. The strong magnetic field in the z direction will, of course, rotate the direction of the spin and, therefore, during the interaction (11) we have to calculate the weak value sandwiched not between the states $|\uparrow_\xi\rangle$ and $|\uparrow_x\rangle$ [see Eq. (6)], but between the rotated states. It turns out, however, that if we arrange the magnetic field in the z direction, such that it rotates the spin during the interaction by $2n\pi$, then the weak value of σ_z during the whole period of the interaction does not change.

Another striking aspect of this experiment becomes evident when we consider it as a device for measuring a small gradient of the magnetic field $\partial B_z/\partial z$. Our choosing α close to π yields a tremendous amplification. Indeed, any weak coupling with the spin of the particles from our preselected and postselected ensemble will be amplified by the factor $[\cos(\alpha/2)]^{-1}$.

This research was supported in part by the National Science Foundation under Grant No. PHY 8408265.

[3] If condition (4) is valid, then

$$
\begin{aligned}
&\langle\psi_f|\, e^{-i\int H dt}|\,\psi_{\rm in}\,\rangle\, e^{-q^2/4\Delta^2} \\
&\qquad = \sum_{n=0}^{\infty} \frac{(iq)^n}{n!}\,\langle\psi_f|\,A^n\,|\psi_{\rm in}\,\rangle\, e^{-q^2/4\Delta^2} \\
&\qquad \cong \langle\psi_f|\psi_{\rm in}\,\rangle \left(1 + \frac{iq\,(\langle\psi_f|\,A\,|\psi_{\rm in}\,\rangle)}{\langle\psi_f|\psi_{\rm in}\,\rangle}\right) e^{-q^2/4\Delta^2} \\
&\qquad \cong \langle\psi_f|\psi_{\rm in}\,\rangle \exp\left(iq\frac{\langle\psi_f|\,A\,|\psi_{\rm in}\,\rangle}{\langle\psi_f|\psi_{\rm in}\,\rangle}\right) e^{-q^2/4\Delta^2}
\end{aligned}
$$

[4] A_w may even be a complex number. The measurement of π gives only the real part $\operatorname{Re} A_w$. In our case, in which the initial state of the measuring device is a Gaussian, we can also find the imaginary part $\operatorname{Im} A_w$ by measuring the canonical variable q itself. Indeed, in the q representation the state of the measuring device is

[5] Y. Aharonov, D. Albert, A. Casher, and L. Vaidman, Phys. Lett. A 124, 199 (1987). [6] The coefficients c_n are derived from the binomial expansion. We can rewrite the left-hand side of (7), the part which multiplies $f(q)$ as

$$
\begin{aligned}
&\sum_{n=N}^{N} \frac{N!}{n!(N-n)!}\left(\frac{1-\alpha^2}{4}\right)^N \left(\frac{1+\alpha}{1-\alpha}\right)^{n/2} e^{iqn/N} \\
&= \left(\frac{1+\alpha}{2}e^{iq/2N} + \frac{1-\alpha}{2}e^{-iq/2N}\right)^{2N} \\
&= [\cos(q/2N) + i\alpha\sin(q/2N)]^{2N} \\
&= \left[1 - \left(1-\alpha^2\right)\sin^2(q/2N)\right]^N e^{i2N\phi}
\end{aligned}
$$

where $\tan\phi = \alpha\tan(q/2N)$. For $f(q) < \exp\left(-\ln\alpha^2|q|\right)$, we obtain

[11] J. von Neumann, Mathematische Gründlagen der Quantemechanik (Springer-Verlag, Berlin, 1932) [English translation: Mathematical Foundations of Quantum Mechanics (Princeton Univ. Press, Princeton, NJ, 1955)].

[2] This Hamiltonian (1) is the effective Hamiltonian of a Stern-Gerlach measuring device as will be explained later [see Eq. (11)].

$$\lim_{N\to\infty} \sum_{n=-N}^{N} c_n e^{iq/2N} f(q)$$
$$= \lim_{N\to\infty} \left[1 - \left(1-\alpha^2\right)\sin^2(q/2N)\right]^N e^{i2N\phi} f(q)$$
$$= e^{iaq} f(q)$$

This proves the statement in the text (7).

20 The Physical Implementation of Quantum Computation by DiVincenzo

Abstract

After a brief introduction to the principles and promise of quantum information processing, the requirements for the physical implementation of quantum computation are discussed. These five requirements, plus two relating to the communication of quantum information, are extensively explored and related to the many schemes in atomic physics, quantum optics, nuclear and electron magnetic resonance spectroscopy, superconducting electronics, and quantum-dot physics, for achieving quantum computing.

20.1 Introduction

[2] The advent of quantum information processing, as an abstract concept, has given birth to a great deal of new thinking, of a very concrete form, about how to create physical computing devices that operate in the hitherto unexplored quantum mechanical regime. The efforts now underway to produce working laboratory devices that perform this profoundly new form of information processing are the subject of this book.

In this chapter I provide an overview of the common objectives of the investigations reported in the remainder of this special issue. The scope of the approaches, proposed and underway, to the implementation of quantum hardware is remarkable, emerging from specialties in atomic physics[1], in quantum optics[2], in nuclear[3] and electron[4] magnetic resonance spectroscopy, in superconducting device physics[5], in electron physics[6], and in mesoscopic and quantum dot research[7]. This amazing variety of approaches has arisen because, as we will see, the principles of quantum computing are posed using the most fundamental ideas of quantum mechanics, ones whose embodiment can be contemplated in virtually every branch of quantum physics.

The interdisciplinary spirit which has been fostered as a result is one of the most pleasant and remarkable features of this field. The excitement and freshness that has been produced bodes well for the prospect for discovery, invention, and innovation in this endeavor.

20.2 Why *quantum* information processing?

The shortest of answers to this question would be, why not? The manipulation and transmission of information is today carried out by physical machines (computers, routers, scanners, etc.), in which the embodiment and transformations of this information can be described using the language of classical mechanics. But the final physical theory of the world is not Newtonian mechanics, and there is no reason to suppose that machines following the laws of quantum

[2]Prepared for Fortschritte der Physik special issue, *Experimental Proposals for Quantum Computation*, eds. H.-K. Lo and S. Braunstein.

mechanics should have the same computational power as classical machines; indeed, since Newtonian mechanics emerges as a special limit of quantum mechanics, quantum machines can only have greater computational power than classical ones. The great pioneers and visionaries who pointed the way towards quantum computers, Deutsch[8], Feynman[9], and others, were stimulated by such thoughts. Of course, by a similar line of reasoning, it may well be asked whether machines embodying the principles of other refined descriptions of nature (perhaps general relativity or string theory) may have even more information processing capabilities; speculations exist about these more exotic possibilities, but they are beyond the scope of the present discussion.

But computing with quantum mechanics really deserves a lot more attention than wormhole computing or quantum-gravity computing; quantum computing, while far in the future from the perspective of CMOS roadmaps and projections of chip fab advances, can certainly be seen as a real prospect from the perspective of research studies in quantum physics. It does not require science fiction to envision a quantum computer; the proposals discussed later in this issue paint a rather definite picture of what a real quantum computer will look like.

So, how much is gained by computing with quantum physics over computing with classical physics? We do not seem to be near to a final answer to this question, which is natural since even the ultimate computing power of classical machines remains unknown. But the answer as we know it today has an unexpected structure; it is not that quantum tools simply speed up all information processing tasks by a uniform amount. By a standard complexity measure (i.e., the way in which the number of computational steps required to complete a task grows with the "size" n of the task), some tasks are not sped up at all[10] by using quantum tools (e.g., obtaining the nth iterate of a function $f(f(...f(x)...))$[11]), some are sped up moderately (locating an entry in a database of n entries[12]), and some are apparently sped up exponentially (Shor's algorithm for factoring an n-digit number[13]).

In other types of information processing tasks, particularly those involving communication[14], both quantitative and qualitative improvements are seen[15]: for certain tasks (choosing a free day for an appointment between two parties from out of n days) there is a quadratic reduction of the amount of communicated data required, if quantum states rather than classical states are transmitted[16]. For some tasks (the "set disjointness problem", related to allocating non-overlapping segments of a shared memory in a distributed computation) the reduction of required communication is exponential[17]. Finally, there are tasks that are doable in the quantum world that have no counterpart classically: quantum cryptography provides an absolute secrecy of communication between parties that is impossible classically[18]. And for some games, winning strategies become possible with the use of quantum resources that are not available otherwise[19, 20].

This issue, and this chapter, are primarily concerned with the "hows" of quantum computing rather than the "whys," so we will leave behind the computer science after this extremely brief mention. There is no shortage of other places to obtain more information about these things; I recommend the recent articles by Aharonov[21] and by Cleve[22]; other general introductions[23] will give the reader pointers to the already vast specialized literature on this subject.

20.3 Realizing quantum computation

Let me proceed with the main topic: the physical realization of quantum information processing. As a guide to the remainder of the special issue, and as a means of reviewing the basic steps required to make quantum computation work, I can think of no better plan than to review a set of basic criteria that my coworkers and I have been discussing over the last few years[24] for the realization of quantum computation (and communication), and to discuss the application of these criteria to the multitude of physical implementations that are found below.

So, without further ado, here are the

Five (plus two) requirements for the implementation of quantum computation

1. A scalable physical system with well characterized qubits

For a start, a physical system containing a collection of qubits is needed. A qubit (or, more precisely, the embodiment of a qubit) is[25] simply a quantum two-level system like the two spin states of a spin 1/2 particle, like the ground and excited states of an atom, or like the vertical and horizontal polarization of a single photon. The generic notation for a qubit state denotes one state as $|0\rangle$ and the other as $|1\rangle$. The essential feature that distinguishes a qubit from a bit is that, according to the laws of quantum mechanics, the permitted states of a single qubit fills up a two-dimensional complex vector space; the general state is written $a|0\rangle + b|1\rangle$, where a and b are complex numbers, and a normalization convention $|a|^2+|b|^2 = 1$ is normally adopted. The general state of two qubits, $a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$, is a four-dimensional vector, one dimension for each distinguishable state of the two systems. These states are generically *entangled*, meaning that they cannot be written as a product of the states of two individual qubits. The general state of n qubits is specified by a 2^n-dimensional complex vector.

A qubit being "well characterized" means several different things. Its physical parameters should be accurately known, including the internal Hamiltonian of the qubit (which determines the energy eigenstates of the qubit, which are often, although not always, taken as the $|0\rangle$ and $|1\rangle$ states), the presence of and couplings to other states of the qubit, the interactions with other qubits, and the couplings to external fields that might be used to manipulate the state of the qubit. If the qubit has third, fourth, etc., levels, the computer's control apparatus should be designed so that the probability of the system ever going into these states is small. The smallness of this and other parameters will be determined by the capabilities of quantum error correction, which will be discussed under requirement 3.

Recognizing a qubit can be trickier than one might think. For example, we might consider a pair of one-electron quantum dots that share a single electron between them as a two-qubit system. It is certainly true that we can denote the presence or absence of an electron on each dot by $|0\rangle$ and $|1\rangle$, and it is well known experimentally how to put this system into the "entangled" state $1/\sqrt{2}(|01\rangle + |10\rangle)$ in which the electron is in a superposition of being on the left dot and the right dot. But it is fallacious to consider this as a two-qubit system; while the states $|00\rangle$ and $|11\rangle$ are other allowed physical states of the dots, superselection principles forbid the creation of entangled states involving different particle numbers such as $1/\sqrt{2}(|00\rangle + |11\rangle)$.

It is therefore false to consider this as a two-qubit system, and, since there are not two qubits, it is nonsense to say that there is entanglement in this system. It is correct to say that the electron is in a superposition of different quantum states living on the two different dots. It is also perfectly correct to consider this system to be the embodiment of a *single* qubit, spanned by the states (in the misleading notation above) $|01\rangle$ ("electron on the right dot") and $|10\rangle$ ("electron on the left dot"). Indeed, several of the viable proposals, including the ones by Schön, Averin, and Tanamoto in this special issue, use exactly this system as a qubit. However, false lines of reasoning like the one outlined here have sunk various proposals before they were properly launched (no such abortive proposals are represented in this book, but they can be found occasionally in the literature).

An amazing variety of realizations of the qubit are represented in this volume. There is a very well developed line of work that began with the proposal of Cirac and Zoller[1] for an ion-trap quantum computer, in which, in its quiescent state, the computer holds the qubits in pairs of energy levels of ions held in a linear electromagnetic trap. Various pairs of energy levels (e.g., Zeeman-degenerate ground states, as are also used in the NMR approach[3] discussed by Cory) have been proposed and investigated experimentally. The many neutral-atom proposals (see chapters by Kimble[2], Deutsch[26], and Briegel[27]) use similar atomic energy levels of

neutral species. These atomic-physics based proposals use other auxiliary qubits such as the position of atoms in a trap or lattice, the presence or absence of a photon in an optical cavity, or the vibrational quanta of trapped electrons, ions or atoms (in the Platzman proposal below[6] this is the primary qubit). Many of the solid-state proposals exploit the fact that impurities or quantum dots have well characterized discrete energy level spectra; these include the spin states of quantum dots (see chapters by Loss[7] and Imamoglu[2]), the spin states of donor impurities (see Kane[4]), and the orbital or charge states of quantum dots (see Tanamoto[7]). Finally, there are a variety of interesting proposals which use the quantized states of superconducting devices, either ones involving the (Cooper-pair) charge (see Schön, Averin), or the flux (see Mooij)[5].

2. The ability to initialize the state of the qubits to a simple fiducial state, such as $|000...\rangle$

This arises first from the straightforward computing requirement that registers should be initialized to a known value before the start of computation. There is a second reason for this initialization requirement: quantum error correction (see requirement 3 below) requires a continuous, fresh supply of qubits in a low-entropy state (like the $|0\rangle$ state). The need for a continuous supply of 0s, rather than just an initial supply, is a real headache for many proposed implementations. But since it is likely that a demonstration of a substantial degree of quantum error correction is still quite some time off, the problem of continuous initialization does not have to be solved very soon; still, experimentalists should be aware that the speed with which a qubit can be zeroed will eventually be a very important issue. If the time it takes to do this initialization is relatively long compared with gate-operation times (see requirement 4), then the quantum computer will have to equipped with some kind of "qubit conveyor belt", on which qubits in need of initialization are carried away from the region in which active computation is taking place, initialized while on the "belt", then brought back to the active place after the initialization is finished. (A similar parade of qubits will be envisioned in requirement 5 for the case of low quantum-efficiency measurements[28].)

There are two main approaches to setting qubits to a standard state: the system can either be "naturally" cooled when the ground state of its Hamiltonian is the state of interest, or the standard state can be achieved by a measurement which projects the system either into the state desired or another state which can be rotated into it. These approaches are not fundamentally different from one another, since the projection procedure is a form of cooling; for instance, the laser cooling techniques used routinely now for the cooling of ion states to near their ground state in a trap[1] are closely connected to the fluorescence techniques used to measure the state of these ions. A more "natural" kind of cooling is advocated in many of the electron spin resonance based techniques (using quantum dots or impurities)[7, 4] in which the spins are placed in a strong magnetic field and allowed to align with it via interaction with their heat bath. In this kind of approach the time scale will be a problem. Since the natural thermalization times are never shorter than the decoherence time of the system, this procedure will be too slow for the needs of error correction and a "conveyor belt" scheme would be required. Cooling by projection, in which the Hamiltonian of the system and its environment are necessarily perturbed strongly, will have a time scale dependent on the details of the setup, but potentially much shorter than the natural relaxation times. One cannot say too much more at this point, as the schemes for measurement have in many cases not been fully implemented (see requirement 5). In the NMR quantum computer implementations to date (see Cory below), cooling of the initial state has been foregone altogether; it is acknowledged[3] that until some of the proposed cooling schemes are implemented (a nontrivial thing to do), NMR can never be a scalable scheme for quantum computing.

3. Long relevant decoherence times, much longer than the gate operation time

Decoherence times characterize the dynamics of a qubit (or any quantum system) in contact with its environment. The (somewhat overly) simplified definition of this time is that it is the

characteristic time for a generic qubit state $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$ to be transformed into the mixture $\rho = |a|^2\,|0\rangle\,\langle 0| + |b|^2\,|1\rangle\,\langle 1|$. A more proper characterization of decoherence, in which the decay can depend on the form of the initial state, in which the state amplitudes may change as well, and in which other quantum states of the qubit can play a role (in a special form of state decay called "leakage" in quantum computing[29, 30]), is rather more technical than I want to get here; but see Refs. [31] and [32] for a good general discussion of all these. Even the simplest discussion of decoherence that I have given here should also be extended to include the possibility that the decoherence of neighboring qubits is correlated. It seems safest to assume that they will be neither completely correlated nor completely uncorrelated, and the thinking about error correction has taken this into account.

Decoherence is very important for the fundamentals of quantum physics, as it is identified as the principal mechanism for the emergence of classical behavior. For the same reason, decoherence is very dangerous for quantum computing, since if it acts for very long, the capability of the quantum computer will not be so different from that of a classical machine. The decoherence time must be long enough that the uniquely quantum features of this style of computation have a chance to come into play. How long is "long enough" is also indicated by the results of quantum error correction, which I will summarize shortly.

I have indicated that the "relevant" decoherence times should be long enough. This emphasizes that a quantum particle can have many decoherence times pertaining to different degrees of freedom of that particle. But many of these can be irrelevant to the functioning of this particle as a qubit. For example, the rapid decoherence of an electron's position state in a solid state environment does not preclude its having a very long spin coherence time, and it can be arranged that this is the only time relevant for quantum computation. Which time is relevant is determined by the choice of the qubit basis states $|0\rangle$ and $|1\rangle$; for example, if these two states correspond to different spin states but identical orbital states, then orbital decoherence will be irrelevant.

One might worry that the decoherence time necessary to do a successful quantum computation will scale with the duration of the computation. This would place incredibly stringent requirements on the physical system implementing the computation. Fortunately, in one of the great discoveries of quantum information theory (in 1995-6), it was found that error correction of quantum states is possible[33] and that this correction procedure can be successfully applied in quantum computation[34], putting much more reasonable (although still daunting) requirements on the needed decoherence times.

In brief, quantum error correction starts with coding; as in binary error correction codes, in which only a subset of all boolean strings are "legal" states, quantum error correction codes consist of legal states confined to a subspace of the vector space of a collection of qubits. Departure from this subspace is caused by decoherence. Codes can be chosen such that, with a suitable sequence of quantum computations and measurements of some ancillary qubits, the error caused by decoherence can be detected and corrected. As noted above, these ancillary qubits have to be continuously refreshed for use. I will not go much farther into the subject here, see [31] for more. It is known that quantum error correction can be made fully fault tolerant, meaning that error correction operations can be successfully intermingled with quantum computation operations, that errors occurring during the act of error correction, if they occur at a sufficiently small rate, do no harm, and that the act of quantum computation does not itself cause an unreasonable proliferation of errors.

These detailed analyses have indicated the magnitude of decoherence time scales that are acceptable for fault-tolerant quantum computation. The result is that, if the decoherence time is $10^4 - 10^5$ times the "clock time" of the quantum computer, that is, the time for the execution of an individual quantum gate (see requirement 4), then error correction can be successful. This is, to tell the truth, a rather stringent condition, quantum systems frequently do not have

such long decoherence times. But sometimes they do, and our search for a successful physical implementation must turn towards these. At least this result says that the required decoherence rate does not become ever smaller as the size and duration of the quantum computation grows. So, once the desired threshold is attainable, decoherence will not be an obstacle to scalable quantum computation.

Having said this, it must be admitted that it will be some time before it is even possible to subject quantum error correction to a reasonable test. Nearly all parts of requirements 1-5 must be in place before such a test is possible. And even the most limited application of quantum error correction has quite a large overhead: roughly 10 ancillary qubits must be added for each individual qubit of the computation. Fortunately, this overhead ratio grows only logarithmically as the the size of the quantum computation is increased.

In the short run, it is at least possible to design and perform experiments which measure the decoherence times and other relevant properties (such as the correlation of decoherence of neighboring qubits) of candidate implementations of qubits. With such initial test experiments, caution must be exercised in interpreting the results, because decoherence is a very system-specific phenomenon, depending on the details of all the qubits' couplings to various environmental degrees of freedom. For example, the decoherence time of the spin of an impurity in the bulk of a perfect semiconductor may not be the same as its decoherence time when it is near the surface of the solid, in the immediate neighborhood of device structures designed to manipulate its quantum state. Test experiments should probe decoherence in as realistic a structure as is possible.

4. A "universal" set of quantum gates

This requirement is of course at the heart of quantum computing. A quantum algorithm is typically specified[8] as a sequence of unitary transformations U_1, U_2, U_3,..., each acting on a small number of qubits, typically no more than three. The most straightforward transcription of this into a physical specification is to identify Hamiltonians which generate these unitary transformations, viz., $U_1 = e^{iH_1 t/\hbar}$, $U_2 = e^{iH_2 t/\hbar}$, $U_3 = e^{iH_3 t/\hbar}$, etc.; then, the physical apparatus should be designed so that H_1 can be turned on from time 0 to time t, then turned off and H_2 turned on from time t to time $2t$, etc.

Would that life were so simple! In reality what can be done is much less, but much less can be sufficient. Understanding exactly how much less is still enough, is the main complication of this requirement. In all the physical implementations discussed in this volume, only particular sorts of Hamiltonians can be turned on and off; in most cases, for example, only two-body (two-qubit) interactions are considered. This immediately poses a problem for a quantum computation specified with three-qubit unitary transformations; fortunately, of course, these can always be re-expressed in terms of sequences of one- and two-body interactions[35], and the two-body interactions can be of just one type[36], the "quantum XOR" or "cNOT". There are some implementations in which multi-qubit gates can be implemented directly[37].

However, this still leaves a lot of work to do. In some systems, notably in NMR (see Cory), there are two-body interactions present which cannot be turned *off*, as well as others which are switchable. This would in general be fatal for quantum computation, but the particular form of the fixed interactions permit their effects to be annulled by particular "refocusing" sequences of the controllable interactions, and it has recently been discovered[38] that these refocusing sequences can be designed and implemented efficiently.

For many other systems, the two-body Hamiltonian needed to generate directly the cNOT unitary transformation is not available. For example, in the quantum-dot proposal described by Loss below[7], the only two-body interaction which should be easily achievable is the exchange interaction between neighboring spins, $H \propto \vec{S}_i \cdot \vec{S}_{i+1}$; in the Imamoglu chapter[2], the attainable interaction is of the XY type, i.e., $H \propto S_{ix}S_{jx} + S_{iy}S_{jy}$. An important observation is that with the appropriate sequence of exchange or XY interactions, in conjunction with particular one-

body interactions (which are assumed to be more easily doable), the cNOT transformation can be synthesized[39]. It is incumbent on each implementation proposal to exhibit such a sequence for producing the cNOT using the interactions that are naturally realizable.

Often there is also some sophisticated thinking required about the time profile of the two-qubit interaction. The naive description above uses a "square pulse" time profile, but often this is completely inappropriate; for instance, if the Hamiltonian can also couple the qubit to other, higher-lying levels of the quantum system, often the only way to get the desired transformation is to turn on and off the interaction smoothly and slowly enough that an adiabatic approximation is accurate[29, 30] (in a solid-state context, see also [40]). The actual duration of the pulse will have to be sufficiently long that any such adiabatic requirement is satisfied; then typically only the time integral $\int dt H(t)$ is relevant for the quantum gate action. The overall time scale of the interaction pulse is also controlled by the attainable maximum size of the matrix elements of $H(t)$, which will be determined by various fundamental considerations, like the requirement that the system remains in the regime of validity of a linear approximation, and practical considerations, like the laser power that can be concentrated on a particular ion. Given these various constraints, the "clock time" of the quantum computer will be determined by the time interval needed such that two consecutive pulses have negligible overlap.

Another consideration, which does not seem to present a problem with any current implementation schemes, but which may be an issue in the future, is the classicality of the control apparatus. We say that the interaction Hamiltonian $H(t)$ has a time profile which is controlled externally by some "classical" means, that is, by the intensity of a laser beam, the value of a gate voltage, or the current level in a wire. But each of these control devices is made up themselves of quantum mechanical parts. When we require that these behave classically, it means that their action should proceed without any entanglement developing between these control devices and the quantum computer. Estimates indicate that this entanglement can indeed be negligible, but this effect needs to be assessed for each individual case.

In many cases it is impossible to turn on the desired interaction between a pair of qubits; for instance, in the ion-trap scheme, no direct interaction is available between the ion-level qubits[1]. In this and in other cases, a special quantum subsystem (sometimes referred to as a "bus qubit") is used which can interact with each of the qubits in turn and mediate the desired interaction: for the ion trap, this is envisioned to be the vibrational state of the ion chain in the trap; in other cases it is a cavity photon whose wavefunction overlaps all the qubits. Unfortunately, this auxiliary quantum system introduces new channels for the environment to couple to the system and cause decoherence, and indeed the decoherence occurring during gate operation is of concern in the ion-trap and cavity-quantum electrodynamics schemes.

Some points about requirement 4 are important to note in relation to the implementation of error correction. Successful error correction requires fully parallel operation, meaning that gate operations involving a finite fraction of all the qubits must be doable simultaneously. This can present a problem with some of the proposals in which the single "bus qubit" is needed to mediate each interaction. On the other hand, the constraint that interactions are only among nearest neighbors in a lattice, as in many of the solid-state proposals, does allow for sufficient parallelism[41].

Quantum gates cannot be implemented perfectly; we must expect both systematic and random errors in the implementation of the necessary Hamiltonians. Both types of errors can be viewed as another source of decoherence and thus error correction techniques are effective for producing reliable computations from unreliable gates, if the unreliability is small enough. The tolerable unreliability due to random errors is in the same vicinity as the decoherence threshold, that is, the magnitude of random errors should be $10^{-4} - 10^{-5}$ per gate operation or so. It might be hoped that systematic errors could be virtually eliminated by careful calibration; but this will surely not always be the case. It seems harder to give a good rule for how much

systematic error is tolerable, the conservative estimates give a very, very small number (the square of the above)[31], but on the other hand there seems to be some evidence that certain important quantum computations (e.g., the quantum Fourier transform) can tolerate a very high level of systematic error (over- or under-rotation). Some types of very large errors may be tolerable if their presence can be detected and accounted for on the fly (we are thinking, for example, about charge switching in semiconductors or superconductors).

Error correction requires that gate operations be done on coded qubits, and one might worry that such operations would require a new repertoire of elementary gate operations for the base-level qubits which make up the code. For the most important error correction techniques, using the so called "stabilizer" codes, this is not the case. The base-level toolkit is exactly the same as for the unencoded case: one-bit gates and cNOTs, or any gate repertoire that can produce these, are adequate. Sometimes the use of coding can actually *reduce* the gate repertoire required: in the work on decoherence free subspaces and subsystems, codes are introduced using blocks of three and four qubits for which two-qubit exchange interactions alone are enough to implement general quantum computation[42, 43]. This simplification could be very useful in the quantum-dot[7] or semiconductor-impurity[4] implementations.

5. A qubit-specific measurement capability

Finally, the result of a computation must be read out, and this requires the ability to measure specific qubits. In an ideal measurement, if a qubit's density matrix is $\rho = p\,|0\rangle\langle 0| + (1-p)\,|1\rangle\langle 1| + \alpha\,|0\rangle\langle 1| + \alpha^*\,|1\rangle\langle 0|$, the measurement should give outcome "0" with probability p and "1" with probability $1-p$ independent of α and of any other parameters of the system, including the state of nearby qubits, and without changing the state of the rest of the quantum computer. If the measurement is "non-demolition", that is, if in addition to reporting outcome "0" the measurement leaves the qubit in state $|0\rangle\langle 0|$, then it can also be used for the state preparation of requirement 2; but requirement 2 can be fulfilled in other ways.

Such an ideal measurement as I have described is said to have 100% quantum efficiency; real measurements always have less. While the fidelity of a quantum measurement is not captured by a single number, the single quantum-efficiency parameter is often a very useful way to summarize it, just as the decoherence time is a useful if incomplete summary of the damage caused to a quantum state by the environment.

While quantum efficiency of 100% is desirable, much less is needed for quantum computation; there is, in fact, a tradeoff possible between quantum efficiency and other resources which results in reliable computation. As a simple example, if the quantum efficiency is 90%, then, in the absence of any other imperfections, a computation with a single-bit output (a so-called "decision problem", common in computer science) will have 90% reliability. If 97% reliability is needed, this can just be achieved by rerunning the calculation three times. Much better, actually, is to "copy" the single output qubit to three, by applying two cNOT gates involving the output qubit and two other qubits set to $|0\rangle$, and measuring those three. (Of course, qubits cannot be "copied", but their value in a particular basis can.) In general, if quantum efficiency q is available, then copying to somewhat more than $1/q$ qubits and measuring all of these will result in a reliable outcome. So, a quantum efficiency of 1% would be usable for quantum computation, at the expense of hundreds of copies/remeasures of the same output qubit. (This assumes that the measurement does not otherwise disturb the quantum computer. If it does, the possibilities are much more limited.)

Even quantum efficiencies much, much lower than 1% can be and are used for successful quantum computation: this is the "bulk" model of NMR (see Cory and [3]), where macroscopic numbers of copies of the same quantum computer (different molecules in solution) run simultaneously, with the final measurement done as an ensemble average over the whole sample. These kinds of weak measurements, in which each individual qubit is hardly disturbed, are quite common and well understood in condensed-matter physics.

If a measurement can be completed quickly, on the timescale of 10^{-4} of the decoherence time, say, then its repeated application during the course of quantum computation is valuable for simplifying the process of quantum error correction. On the other hand, if this fast measurement capability is not available, quantum error correction is still possible, but it then requires a greater number of quantum gates to implement.

Other tradeoffs between the complexity and reliability of quantum measurement vs. those of quantum computation have recently been explored. It has been shown that if qubits can be initialized into pairs of maximally entangled states, and two-qubit measurements in the so-called Bell basis ($\Psi^{\pm} = |01\rangle \pm |10\rangle$, $\Phi^{\pm} = |00\rangle \pm |11\rangle$) are possible, then no two-qubit quantum gates are needed, one-bit gates alone suffice[44]. Now, often this tradeoff will not be useful, as in many schemes a Bell measurement would require two-bit quantum gates.

But the overall message, seen in many of our requirements, is that more and more, the theoretical study of quantum computation has offered a great variety of tradeoffs for the potential implementations: if X is very hard, it can be substituted with more of Y. Of course, in many cases both X and Y are beyond the present experimental state of the art; but a thorough knowledge of these tradeoffs should be very useful for devising a rational plan for the pursuit of future experiments.

20.4 Desiderata for quantum communication

For computation alone, the five requirements above suffice. But the advantages of quantum information processing are not manifest solely, or perhaps even principally, for straightforward computation only. There are many kinds of information-processing tasks, reviewed briefly at the beginning, that involve more than just computation, and for which quantum tools provide a unique advantage.

The tasks we have in mind here all involve not only computation but also communication. The list of these tasks that have been considered in the light of quantum capabilities, and for which some advantage has been found in using quantum tools, is fairly long and diverse: it includes secret key distribution, multiparty function evaluation as in appointment scheduling, secret sharing, and game playing[14].

When we say communication we mean quantum communication: the transmission of intact qubits from place to place. This obviously adds more features that the physical apparatus must have to carry out this information processing. We formalize these by adding two more items to the list of requirements:

6. The ability to interconvert stationary and flying qubits

7. The ability faithfully to transmit flying qubits between specified locations

These two requirements are obviously closely related, but it is worthwhile to consider them separately, because some tasks need one but not the other. For instance, quantum cryptography[18] involves only requirement 7; it is sufficient to create and detect flying qubits directly.

I have used the jargon "flying qubits"[2], which has become current in the discussions of quantum communication. Using this term emphasizes that the optimal embodiment of qubits that are readily transmitted from place to place is likely to be very different from the optimal qubits for reliable local computation. Indeed, almost all proposals assume that photon states, with the qubit encoded either in the polarization or in the spatial wavefunction of the photon, will be the flying qubit of choice, and indeed, the well developed technology of light transmission through optical fibers provides a very promising system for the transmission of qubits. I would note, though, that my colleagues and I have raised the possibility that electrons traveling though solids could provide another realization of the flying qubit[14, 45].

Only a few completely developed proposals exist which incorporate requirements 6 and 7. Of course, there are a number of quite detailed studies of 7, in the sense that experiments on quantum cryptography have been very concerned with the preservation of the photon quantum state during transmission through optical fibers or through the atmosphere. However, these studies are rather disconnected from the other concerns of quantum computing. Requirement 6 is the really hard one; to date the only theoretical proposal sufficiently concrete that experiments addressing it have been planned is the scheme produced by Kimble and coworkers[46] for unloading a cavity photon into a traveling mode via atomic spectroscopy, and loading it by the time-reversed process. Other promising concepts, like the launching of electrons from quantum dots into quantum wires such that the spin coherence of the electrons is preserved, need to be worked out more fully.

20.5 Summary

So, what is the "winning" technology going to be? I don't think that any living mortal has an answer to this question, and at this point it may be counterproductive even to ask it. Even though we have lived with quantum mechanics for a century, our study of quantum effects in complex artificial systems like those we have in mind for quantum computing is in its infancy. No one can see how or whether all the requirements above can be fulfilled, or whether there are new tradeoffs, not envisioned in our present theoretical discussions but suggested by further experiments, that might take our investigations in an entirely new path.

Indeed, the above discussion, and the other chapters of this special issue, really do not cover all the foreseeable approaches. I will mention two of which I am aware: first, another computational paradigm, that of the cellular automaton, is potentially available for exploitation. This is distinguished from the above "general purpose" approach in that it assumes that every bit pattern throughout the computer will be subjected to the same evolution rule. It is known that general-purpose computation is performable, although with considerable overhead, by a cellular automaton. This is true as well for the quantum version of the cellular automaton, as Lloyd[47] indicated in his original work. New theoretical work by Benjamin[48] shows very explicitly how relatively simple local rules would permit the implementation of some quantum computations. This could point us perhaps towards some sort of polymer with a string of qubits on its backbone that can be addressed globally in a spectroscopic fashion. Experiments are not oriented towards this at the moment, but the tradeoffs are very different, and I don't believe it should be excluded in the future.

Second, even more speculative, but very elegant, is the proposal of Kitaev[49] to use quantum systems with particular kinds of topological excitations, for example nonabelian anyons, for quantum computing. It is hard to see at the moment how to turn this exciting proposal into an experimental program, as no known physical system is agreed to have the appropriate topological excitations. But further research in, for example, the quantum Hall effect might reveal such a system; more likely, perhaps, is that further understanding of this approach, and that of Freedman and his colleagues[50], will shed more light on doing quantum computing using the "standard" approach being considered in this book.

I am convinced of one thing: the ideas of quantum information theory will continue to exert a decisive influence on the further investigation of the fundamental quantum properties of complex quantum systems, and will stimulate many creative and exciting developments for many years to come.

21 Decoherence, Einselection, and the Quantum Origins of the Classical by Zurek

Decoherence is caused by the interaction with the environment which in effect monitors certain observables of the system, destroying coherence between the *pointer states* corresponding to their eigenvalues. This leads to *environment-induced superselection* or *einselection*, a quantum process associated with selective loss of information. Einselected pointer states are stable. They can retain correlations with the rest of the Universe in spite of the environment. Einselection enforces classicality by imposing an effective ban on the vast majority of the Hilbert space, eliminating especially the flagrantly non-local "Schrödinger cat" states. Classical structure of phase space emerges from the quantum Hilbert space in the appropriate macroscopic limit: Combination of einselection with dynamics leads to the idealizations of a point and of a classical trajectory. In measurements, einselection replaces quantum entanglement between the apparatus and the measured system with the classical correlation. Only the preferred pointer observable of the apparatus can store information that has predictive power. When the measured quantum system is microscopic and isolated, this restriction on the predictive utility of its correlations with the macroscopic apparatus results in the effective "collapse of the wavepacket". *Existential interpretation* implied by einselection regards observers as open quantum systems, distinguished only by their ability to acquire, store, and process information. Spreading of the correlations with the effectively classical pointer states throughout the environment allows one to understand 'classical reality' as a property based on the *relatively objective existence* of the einselected states: They can be "found out" without being re-prepared, e.g, by intercepting the information already present in the environment. The redundancy of the records of pointer states in the environment (which can be thought of as their 'fitness' in the Darwinian sense) is a measure of their classicality. A new symmetry appears in this setting: Environment - assisted invariance or *envariance* sheds a new light on the nature of ignorance of the state of the system due to quantum correlations with the environment, and leads to Born's rules and to the reduced density matrices, ultimately justifying basic principles of the program of decoherence and einselection.

21.1 Introduction

The issue of interpretation is as old as quantum theory. It dates back to the discussions of Niels Bohr, Werner Heisenberg, Erwin Schrödinger, (Bohr, 1928; 1949; Heisenberg, 1927; Schrödinger, 1926; 1935a,b; see also Jammer, 1974; Wheeler and Zurek, 1983). Perhaps the most incisive critique of the (then new) theory was due to Albert Einstein, who, searching for inconsistencies, distilled the essence of the conceptual difficulties of quantum mechanics through ingenious "gedankenexperiments". We owe him and Bohr clarification of the significance of the quantum indeterminacy in course of the Solvay congress debates (see Bohr, 1949) and elucidation of the nature of quantum entanglement (Einstein, Podolsky, and Rosen, 1935; Bohr, 1935, Schrödinger, 1935a,b). Issues identified then are still a part of the subject.

Within the past two decades the focus of the research on the fundamental aspects of quantum theory has shifted from esoteric and philosophical to more "down to earth" as a result of three developments. To begin with, many of the old *gedankenexperiments* (such as the EPR "paradox") became compelling demonstrations of quantum physics. More or less simultaneously the role of decoherence begun to be appreciated and einselection was recognized as key in the emergence of classicality. Last not least, various developments have led to a new view of the role of information in physics. This paper reviews progress with a focus on decoherence, einselection and the emergence of classicality, but also attempts a "preview" of the future of this exciting and fundamental area.

21.1.1 The problem: Hilbert space is big

The interpretation problem stems from the vastness of the Hilbert space, which, by the principle of superposition, admits arbitrary linear combinations of any states as a possible quantum state. This law, thoroughly tested in the microscopic domain, bears consequences that defy classical intuition: It appears to imply that the familiar classical states should be an exceedingly rare exception. And, naively, one may guess that superposition principle should always apply literally: Everything is ultimately made out of quantum "stuff". Therefore, there is no *a priori* reason for macroscopic objects to have definite position or momentum. As Einstein noted[3] localization with respect to macrocoordinates is not just *independent*, but *incompatible* with quantum theory. How can one then establish correspondence between the quantum and the familiar classical reality?

Copenhagen Interpretation

Bohr's solution was to draw a border between the quantum and the classical and to keep certain objects – especially measuring devices and observers – on the classical side (Bohr, 1928; 1949). The principle of superposition was suspended "by decree" in the classical domain. The exact location of this border was difficult to pinpoint, but measurements "brought to a close" quantum events. Indeed, in Bohr's view the classical domain was more fundamental: Its laws were self-contained (they could be confirmed from within) and established the framework necessary to define the quantum.

The first breach in the quantum-classical border appeared early: In the famous Bohr – Einstein double-slit debate, quantum Heisenberg uncertainty was invoked by Bohr at the macroscopic level to preserve wave-particle duality. Indeed, as the ultimate components of classical objects are quantum, Bohr emphasized that the boundary must be moveable, so that even the human nervous system could be regarded as quantum provided that suitable classical devices to detect its quantum features were available. In the words of John Archibald Wheeler (1978; 1983) who has elucidated Bohr's position and decisively contributed to the revival of interest in these matters, "No [quantum] phenomenon is a phenomenon until it is a recorded (observed) phenomenon".

This is a pithy summary of a point of view – known as the Copenhagen Interpretation (CI) – that has kept many a physicist out of despair. On the other hand, as long as a compelling reason for the quantum-classical border could not be found, the CI Universe would be governed by two sets of laws, with poorly defined domains of jurisdiction. This fact has kept many a student, not to mention their teachers, in despair (Mermin 1990a; b; 1994).

Many Worlds Interpretation

The approach proposed by Hugh Everett (1957a, b) and elucidated by Wheeler (1957), Bryce DeWitt (1970) and others (see DeWitt and Graham, 1973; Zeh, 1970; 1973; Geroch, 1984; Deutsch, 1985, 1997, 2001) was to enlarge the quantum domain. Everything is now represented by a unitarily evolving state vector, a gigantic superposition splitting to accommodate all the alternatives consistent with the initial conditions. This is the essence of the Many Worlds Interpretation (MWI). It does not suffer from the dual nature of CI. However, it also does not explain the emergence of classical reality.

[3] In a letter dated 1954, Albert Einstein wrote to Max Born "Let ψ_1 and ψ_2 be solutions of the same Schrödinger equation.... When the system is a macrosystem and when ψ_1 and ψ_2 are 'narrow' with respect to the macrocoordinates, then in by far the greater number of cases this is no longer true for $\psi = \psi_1 + \psi_2$. Narrowness with respect to macrocoordinates is not only independent of the principles of quantum mechanics, but, moreover, incompatible with them." (The translation from Born (1969) quoted here is due to Joos (1986).)

The difficulty many have in accepting MWI stems from its violation of the intuitively obvious "conservation law" – that there is just one Universe, the one we perceive. But even after this question is dealt with, , many a convert from CI (which claims allegiance of a majority of physicists) to MWI (which has steadily gained popularity; see Tegmark and Wheeler, 2001, for an assessment) eventually realizes that the original MWI does not address the "preferred basis question" posed by Einstein[1] (see Wheeler, 1983; Stein, 1984; Bell 1981, 1987; Kent, 1990; for critical assessments of MWI). And as long as it is unclear what singles out preferred states, perception of a unique outcome of a measurement and, hence, of a single Universe cannot be explained either[4].

In essence, Many Worlds Interpretation does not address but only postpones the key question. The quantum - classical boundary is pushed all the way towards the observer, right against the border between the material Universe and the "consciousness", leaving it at a very uncomfortable place to do physics. MWI is incomplete: It does not explain what is effectively classical and why. Nevertheless, it was a crucial conceptual breakthrough: Everett reinstated quantum mechanics as a basic tool in the search for its interpretation.

21.1.2 Decoherence and einselection

Decoherence and einselection are two complementary views of the consequences of the same process of environmental monitoring. Decoherence is the destruction of quantum coherence between preferred states associated with the observables monitored by the environment. Einselection is its consequence – the *de facto* exclusion of all but a small set, a *classical domain* consisting of pointer states – from within a much larger Hilbert space. Einselected states are distinguished by their resilience – stability in spite of the monitoring environment.

The idea that "openness" of quantum systems may have anything to do with the transition from quantum to classical was resolutely ignored for a very long time, probably because in classical physics problems of fundamental importance were always settled in isolated systems. In the context of measurements Gottfried (1967) anticipated some of the latter developments. The fragility of energy levels of quantum systems was emphasized by seminal papers of Dieter Zeh (1970; 1973), who argued (inspired by remarks relevant to what would be called today "deterministic chaos" (Borel, 1914)) that macroscopic quantum systems are in effect impossible to isolate.

The understanding of how the environment distills the classical essence from quantum systems is more recent (Zurek, 1981; 1982; 1993a). It combines two observations: (1) In quantum physics "reality" can be attributed to the measured states. (2) Information transfer usually associated with measurements is a common result of almost any interaction with the environment of a system.

Some quantum states are resilient to decoherence. This is the basis of einselection. Using Darwinian analogy, one might say that pointer states are most 'fit'. They survive monitoring by the environment to leave 'descendants' that inherit their properties. Classical domain of pointer states offers a static summary of the result of quantum decoherence. Save for classical dynamics, (almost) nothing happens to these einselected states, even though they are immersed in the environment.

[4]DeWitt, in the Many Worlds re-analysis of quantum measurements makes this clear: in DeWitt and Graham (1973), last paragraph of p. 189 he writes about the key 'remaining problem': "Why is it so easy to find apparata in states [with a well defined value of the pointer observable]? In the case of macroscopic apparata it is well known that a small value for the mean square deviation of a macroscopic observable is a fairly stable property of the apparatus. But how does the mean square deviation become so small in the first place? Why is a large value of the mean square deviation of a macroscopic observable virtually never, in fact, encountered in practice? ... a proof of this does not yet exist. It remains a program for the future."

It is difficult to catch einselection "in action": Environment has little effect on the pointer states, as they are already classical. Therefore, it was easy to miss decoherence - driven dynamics of einselection by taking for granted its result – existence of the classical domain, and a ban on arbitrary quantum superpositions. Macroscopic superpositions of einselected states disappear rapidly. Einselection creates effective superselection rules (Wick, Wightman and Wigner, 1952; 1970; Wightman, 1995). However, in the microscopic, decoherence can be slow in comparison with the dynamics.

Einselection is a quantum phenomenon. Its essence cannot be even motivated classically: In classical physics arbitrarily accurate measurements (also by the environment) can be in principle carried out without disturbing the system. Only in quantum mechanics acquisition of information inevitably alters the state of the system – the fact that becomes apparent in double-slit and related experiments (Wootters and Zurek, 1979; Zurek, 1983).

Quantum nature of decoherence and the absence of classical analogues are a source of misconceptions. For instance, decoherence is sometimes equated with relaxation or classical noise that can be also introduced by the environment. Indeed, *all* of these effects often appear together and as a consequence of the "openness". The distinction between them can be briefly summed up: *Relaxation and noise are caused by the environment perturbing the system*, while *decoherence and einselection are caused by the system perturbing the environment.*

Within the past few years decoherence and einselection became familiar to many. This does not mean that their implications are universally accepted (see comments in the April 1993 issue of *Physics Today*; d'Espagnat, 1989 and 1995; Bub, 1997; Leggett, 1998 and 2002; Stapp, 2001; exchange of views between Anderson, 2001, and Adler, 2001). In a field where controversy reigned for so long this resistance to a new paradigm is no surprise.

21.1.3 The nature of the resolution and the role of envariance

Our aim is to explain why does the quantum Universe appear classical. This question can be motivated only in the context of the Universe divided into systems, and must be phrased in the language of the correlations between them. In the absence of systems Schrödinger equation dictates deterministic evolution;

$$|\Psi(t)\rangle \;=\; \exp(-iHt/\hbar)\;|\Psi(0)\rangle\;, \tag{1.1}$$

and the problem of interpretation seems to disappear.

There is no need for "collapse" in a Universe with no systems. Yet, the division into systems is imperfect. As a consequence, the Universe is a collection of open (interacting) quantum systems. As the interpretation problem does not arise in quantum theory unless interacting systems exist, we shall also feel free to assume that an environment exists when looking for a resolution.

Decoherence and einselection fit comfortably in the context of the Many Worlds Interpretation where they define the "branches" of the universal state vector. Decoherence makes MWI complete: It allows one to analyze the Universe as it is seen by an observer, who is also subject to decoherence. Einselection justifies elements of Bohr's CI by drawing the border between the quantum and the classical. This natural boundary can be sometimes shifted: Its effectiveness depends on the degree of isolation and on the manner in which the system is probed, but it is a very effective quantum - classical border nevertheless.

Einselection fits either MWI or CI framework: It supplies a statute of limitations, putting an end to the quantum jurisdiction. . It delineates how much of the Universe will appear classical to observers who monitor it from within, using their limited capacity to acquire, store, and process information. It allows one to understand classicality as an idealization that holds in the limit of macroscopic open quantum systems.

Environment imposes superselection rules by preserving part of the information that resides in the correlations between the system and the measuring apparatus (Zurek, 1981, 1982). The observer and the environment compete for the information about the system. Environment – because of its size and its incessant interaction with the system – wins that competition, acquiring information faster and more completely than the observer. Thus, a record useful for the purpose of prediction must be restricted to the observables that are already monitored by the environment. In that case, the observer and the environment no longer compete and decoherence becomes unnoticeable. Indeed, typically *observers use environment as a "communication channel", and monitor it to find out about the system.*

Spreading of the information about the system through the environment is ultimately responsible for the emergence of the "objective reality". Objectivity of a state can be quantified by the redundancy with which it is recorded throughout Universe. Intercepting fragments of the environment allows observers to find out (pointer) state of the system without perturbing it (Zurek, 1993a, 1998a, and 2000; see especially section VII of this paper for a preview of this new "environment as a witness" approach to the interpretation of quantum theory).

When an effect of a transformation acting on a system can be undone by a suitable transformation acting on the environment, so that the joint state of the two remains unchanged, the transformed property of the system is said to exhibit "environment assisted invariance" or *envariance* (Zurek, 2002b). Observer must be obviously ignorant of the envariant properties of the system. Pure entangled states exhibit envariance. Thus, in quantum physics perfect information about the joint state of the system-environment pair can be used to prove ignorance of the state of the system.

Envariance offers a new fundamental view of what is information and what is ignorance in the quantum world. It leads to Born's rule for the probabilities and justifies the use of reduced density matrices as a description of a part of a larger combined system. Decoherence and einselection rely on reduced density matrices. Envariance provides a fundamental resolution of many of the interpretational issues. It will be discussed in section VI D.

21.1.4 Existential Interpretation and 'Quantum Darwinism'

What the observer knows is inseparable from what the observer is: The physical state of his memory implies his information about the Universe. Its reliability depends on the stability of the correlations with the external observables. In this very immediate sense decoherence enforces the apparent "collapse of the wavepacket": After a decoherence timescale, only the einselected memory states will exist and retain useful correlations (Zurek, 1991; 1998a,b; Tegmark, 2000). The observer described by some specific einselected state (including a configuration of memory bits) will be able to access ("recall") only that state. The collapse is a consequence of einselection and of the one-to-one correspondence between the state of his memory and of the information encoded in it. Memory is simultaneously a description of the recorded information and a part of the "identity tag", defining observer as a physical system. It is as inconsistent to imagine observer perceiving something else than what is implied by the stable (einselected) records in his possession as it is impossible to imagine the same person with a different DNA: Both cases involve information encoded in a state of a system inextricably linked with the physical identity of an individual.

Distinct memory/identity states of the observer (that are also his "states of knowledge") cannot be superposed: This censorship is strictly enforced by decoherence and the resulting einselection. Distinct memory states label and "inhabit" different branches of the Everett's "Many Worlds" Universe. Persistence of *correlations* is all that is needed to recover "familiar reality". In this manner, the distinction between epistemology and ontology is washed away: To put it succinctly (Zurek, 1994) there can be *no information without representation* in physical

states.

There is usually no need to trace the collapse all the way to observer's memory. It suffices that the states of a decohering system quickly evolve into mixtures of the preferred (pointer) states. All that can be known in principle about a system (or about an observer, also introspectively, e.g., by the observer himself) is its decoherence-resistant 'identity tag' – a description of its einselected state.

Apart from this essentially negative function of a censor the environment plays also a very different role of a "broadcasting agent", relentlessly cloning the information about the einselected pointer states. This role of the environment as a witness in determining what exists was not appreciated until now: Throughout the past two decades, study of decoherence focused on the effect of the environment on the system. This has led to a multitude of technical advances we shall review, but it has also missed one crucial point of paramount conceptual importance: Observers monitor systems indirectly, by intercepting small fractions of their environments (e.g., a fraction of the photons that have been reflected or emitted by the object of interest). Thus, if the understanding of why we perceive quantum Universe as classical is the principal aim, study of the nature of accessibility of information spread throughout the environment should be the focus of attention. This leads one away from the models of measurement inspired by the "von Neumann chain" (1932) to studies of information transfer involving branching out conditional dynamics and the resulting "fan-out" of the information throughout environment (Zurek, 1983, 1998a, 2000). This new 'quantum Darwinism' view of environment selectively amplifying einselected pointer observables of the systems of interest is complementary to the usual image of the environment as the source of perturbations that destroy quantum coherence of the system. It suggests the redundancy of the imprint of the system in the environment may be a quantitative measure of relative *objectivity* and hence of classicality of quantum states. It is introduced in Sections VI and VII of this review.

Benefits of recognition of the role of environment include not just operational definition of the objective existence of the einselected states, but – as is also detailed in Section VI – a clarification of the connection between the quantum amplitudes and probabilities. Einselection converts arbitrary states into mixtures of well defined possibilities. Phases are envariant: Appreciation of envariance as a symmetry tied to the ignorance about the state of the system was the missing ingredient in the attempts of 'no collapse' derivations of Born's rule and in the probability interpretation. While both envariance and the "environment as a witness" point of view are only beginning to be investigated, the extension of the program of einselection they offer allowes one to understand emergence of "classical reality" form the quantum substrate as a consequence of quantum laws.

21.2 Quantum Measurements

The need for a transition from quantum determinism of the global state vector to classical definiteness of states of individual systems is traditionally illustrated by the example of quantum measurements. An outcome of a "generic" measurement of the state of a quantum system is *not* deterministic. In the textbook discussions this random element is blamed on the "collapse of the wavepacket", invoked whenever a quantum system comes into contact with a classical apparatus. In a fully quantum discussion this issue still arises, in spite (or rather because) of the overall deterministic quantum evolution of the state vector of the Universe: As pointed out by von Neumann (1932), there is no room for a 'real collapse' in the purely unitary models of measurements.

21.2.1 Quantum conditional dynamics

To illustrate the ensuing difficulties, consider a quantum system $\mathcal{S}$ initially in a state $|\psi\rangle$ interacting with a quantum apparatus $\mathcal{A}$ initially in a state $|A_0\rangle$:

$$|\Psi_0\rangle = |\psi\rangle|A_0\rangle = \big(\sum_i a_i|s_i\rangle\big)|A_0\rangle$$
$$\longrightarrow \sum_i a_i|s_i\rangle|A_i\rangle = |\Psi_t\rangle \ . \qquad 2.1 \tag{21.1}$$

Above, $\{|A_i\rangle\}$ and $\{|s_i\rangle\}$ are states in the Hilbert spaces of the apparatus and of the system, respectively, and a_i are complex coefficients. Conditional dynamics of such premeasurement (as the step achieved by Eq. (2.1) is often called) can be accomplished by means of a unitary Schrödinger evolution. Yet it is not enough to claim that a measurement has been achieved: Equation (2.1) leads to an uncomfortable conclusion: $|\Psi_t\rangle$ is an EPR-like *entangled state*. Operationally, this EPR nature of the state emerging from the premeasurement can be made more explicit by re-writing the sum in a different basis:

$$|\Psi_t\rangle \ = \sum_i a_i|s_i\rangle|A_i\rangle = \sum_i b_i|r_i\rangle|B_i\rangle \ . \qquad 2.2 \tag{21.2}$$

This freedom of basis choice – basis ambiguity – is guaranteed by the principle of superposition. Therefore, if one were to associate states of the apparatus (or the observer) with decompositions of $|\Psi_t\rangle$, then even before enquiring about the specific outcome of the measurement one would have to decide on the decomposition of $|\Psi_t\rangle$; the change of the basis redefines the measured quantity.

Controlled not and a bit-by-bit measurement

The interaction required to entangle the measured system and the apparatus, Eq. (2.1), is a generalization of the basic logical operation known as a "controlled not" or a `c-not`. Classical, `c-not` changes the state a_t of the target when the control is 1, and does nothing otherwise:

$$0_{\mathtt{c}}\ a_{\mathtt{t}} \ \longrightarrow \ 0_{\mathtt{c}}\ a_{\mathtt{t}} \ ; \quad 1_{\mathtt{c}}\ a_{\mathtt{t}} \ \longrightarrow \ 1_{\mathtt{c}}\ \neg a_{\mathtt{t}} \tag{2.3}$$

Quantum `c-not` is a straightforward quantum version of Eq. (2.3). It was known as a "bit by bit measurement" (Zurek, 1981; 1983) and used to elucidate the connection between entanglement and premeasurement already before it acquired its present name and significance in the context of quantum computation (see e.g. Nielsen and Chuang, 2000). Arbitrary superpositions of the control bit and of the target bit states are allowed:

$$(\alpha|0_{\mathtt{c}}\rangle \ + \ \beta|1_{\mathtt{c}}\rangle)|a_{\mathtt{t}}\rangle$$
$$\longrightarrow \ \alpha|0_{\mathtt{c}}\rangle|a_{\mathtt{t}}\rangle \ + \ \beta|1_{\mathtt{c}}\rangle|\neg a_{\mathtt{t}}\rangle \qquad 2.4 \tag{21.3}$$

Above "negation" $|\neg a_{\mathtt{t}}\rangle$ of a state is basis dependent;

$$\neg(\gamma|0_{\mathtt{t}}\rangle + \delta|1_{\mathtt{t}}\rangle) = \gamma|1_{\mathtt{t}}\rangle + \delta|0_{\mathtt{t}}\rangle \tag{2.5}$$

With $|A_0\rangle = |0_{\mathtt{t}}\rangle$, $|A_1\rangle = |1_{\mathtt{t}}\rangle$ we have an obvious analogy between the `c-not` and a premeasurement.

In the classical controlled not the direction of information transfer is consistent with the designations of the two bits: The state of the control remains unchanged while it influences the target, Eq. (2.3). Classical measurement need not influence the system. Written in the logical

basis $\{|0\rangle, |1\rangle\}$, the truth table of the quantum `c-not` is essentially – that is, save for the possibility of superpositions – the same as Eq. (2.3). One might have anticipated that the direction of information transfer and the designations ("control/system" and "target/apparatus") of the two qubits will be also unambiguous, as in the classical case. This expectation is incorrect. In the conjugate basis $\{|+\rangle, |-\rangle\}$ defined by:

$$|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2} \ , \tag{2.6}$$

the truth table of Eq. (2.3) along with Eq. (2.6) lead to a new complementary truth table:

$$|\pm\rangle|+\rangle \longrightarrow |\pm\rangle|+\rangle; \quad |\pm\rangle|-\rangle \longrightarrow |\mp\rangle|-\rangle \ . \qquad 2.7,\ 2.8 \tag{21.4}$$

In the complementary basis $\{|+\rangle, |-\rangle\}$ roles of the control and of the target are reversed: The former (basis $\{|0\rangle, |1\rangle\}$) target – represented by the second ket above – remains unaffected, while the state of the former control (the first ket) is conditionally "flipped".

In the bit-by-bit case the measurement interaction is:

$$\begin{aligned} H_{int} \ &= \ g|1\rangle\langle 1|_{\mathcal{S}}|-\rangle\langle -|_{\mathcal{A}} \ = \\ \frac{g}{2}|1\rangle\langle 1|_{\mathcal{S}} \otimes (\mathbf{1} - (|0\rangle\langle 1| + |1\rangle\langle 0|))_{\mathcal{A}} \qquad & 2.9 \end{aligned} \tag{21.5}$$

Above, g is a coupling constant, and the two operators refer to the system (i.e., to the former control), and to the apparatus pointer (the former target), respectively. It is easy to see that the states $\{|0\rangle, |1\rangle\}_{\mathcal{S}}$ of the system are unaffected by H_{int}, since;

$$[H_{int}, e_0|0\rangle\langle 0|_{\mathcal{S}} + e_1|1\rangle\langle 1|_{\mathcal{S}}] = 0 \tag{2.10}$$

The measured (control) observable $\hat{\epsilon} = e_0|0\rangle\langle 0| + e_1|1\rangle\langle 1|$ is a constant of motion under H_{int}. `c-not` requires interaction time t such that $gt = \pi/2$.

The states $\{|+\rangle, |-\rangle\}_{\mathcal{A}}$ of the apparatus encode the information about phase between the logical states. They have exactly the same "immunity":

$$[H_{int}, f_+|+\rangle\langle +|_{\mathcal{A}} + f_-|-\rangle\langle -|_{\mathcal{A}}] = 0 \tag{2.11}$$

Hence, when the apparatus is prepared in a definite phase state (rather than in a definite pointer/logical state), it will pass on its phase onto the system, as Eqs. (2.7) - (2.8), show. Indeed, H_{int} can be written as:

$$\begin{aligned} H_{int} \ &= \ g|1\rangle\langle 1|_{\mathcal{S}}|-\rangle\langle -|_{\mathcal{A}} \\ = \tfrac{g}{2}(\mathbf{1} - (|-\rangle\langle +| + |+\rangle\langle -|))_{\mathcal{S}} \otimes |-\rangle\langle -|_{\mathcal{A}} \qquad & 2.12 \end{aligned} \tag{21.6}$$

making this "immunity" obvious.

This basis-dependent direction of information flow in a quantum `c-not` (or in a premeasurement) is a consequence of complementarity. While the information about the observable with the eigenstates $\{|0\rangle, |1\rangle\}$ travels from the system to the apparatus, in the complementary $\{|+\rangle, |-\rangle\}$ basis it seems that the apparatus is measured by the system. This remark (Zurek 1998a, b; see also Beckman, Gottesman, and Nielsen, 2001) clarifies the sense in which phases are inevitably "disturbed" in measurements. They are not really destroyed, but, rather, as the apparatus measures a certain observable of the system, the system simultaneously "measures" phases between the possible outcome states of the apparatus. This leads to loss of phase coherence: Phases become "shared property" as we shall see in more detail in the discussion of envariance.

The question "what measures what?" (decided by the direction of the information flow) depends on the initial states. In "the classical practice" this ambiguity does not arise. Einselection limits the set of possible states of the apparatus to a small subset.

Measurements and controlled shifts.

The truth table of a whole class of `c-not` like transformations that includes general premeasurement, Eq. (2.1), can be written as:

$$|s_j\rangle|A_k\rangle \longrightarrow |s_j\rangle|A_{k+j}\rangle \tag{2.13}$$

Equation (2.1) follows when $k = 0$. One can therefore model measurements as controlled shifts – `c-shifts` – generalizations of the `c-not`. In the bases $\{|s_j\rangle\}$ and $\{|A_k\rangle\}$, the direction of the information flow appears to be unambiguous – from the system $\mathcal{S}$ to the apparatus $\mathcal{A}$. However, a complementary basis can be readily defined (Ivanovic, 1981; Wootters and Fields, 1989);

$$|B_k\rangle \;=\; N^{-\frac{1}{2}} \sum_{l=0}^{N-1} \exp\left(\frac{2\pi i}{N} kl\right) |A_l\rangle \ . \tag{2.14a}$$

Above N is the dimensionality of the Hilbert space. Analogous transformation can be carried out on the basis $\{|s_i\rangle\}$ of the system, yielding states $\{|r_j\rangle\}$.

Orthogonality of $\{|A_k\rangle\}$ implies:

$$\langle B_l|B_m\rangle = \delta_{lm} \ . \tag{2.15}$$

$$|A_k\rangle \;=\; N^{-\frac{1}{2}} \sum_{l=0}^{N-1} \exp\left(-\frac{2\pi i}{N} kl\right) |B_l\rangle \tag{2.14b}$$

inverts of the transformtion of Eq. (2.14a). Hence:

$$|\psi\rangle = \sum_l \alpha_l |A_l\rangle = \sum_k \beta_k |B_k\rangle \ , \tag{2.16}$$

where the coefficients β_k are:

$$\beta_k = N^{-\frac{1}{2}} \sum_{l=0}^{N-1} \exp\left(-\frac{2\pi i}{N} kl\right) \alpha_l \ . \tag{2.17}$$

Hadamard transform of Eq. (2.6) is a special case of the more general transformation considered here.

To implement the truth tables involved in premeasurements we define observable $\hat{A}$ and its conjugate:

$$\hat{A} = \sum_{k=0}^{N-1} k|A_k\rangle\langle A_k|; \ \ \hat{B} = \sum_{l=0}^{N-1} l|B_l\rangle\langle B_l| \ . \tag{2.18a, b}$$

The interaction Hamiltonian:

$$H_{int} = g\hat{s}\hat{B} \tag{2.19}$$

is an obvious generalization of Eqs. (2.9) and (2.12), with g the coupling strength and $\hat{s}$:

$$\hat{s} = \sum_{l=0}^{N-1} l|s_l\rangle\langle s_l| \tag{2.20}$$

In the $\{|A_k\rangle\}$ basis $\hat{B}$ is a shift operator,

$$\hat{B} = \frac{iN}{2\pi} \frac{\partial}{\partial \hat{A}} \ . \tag{2.21}$$

To show how H_{int} works, we compute:

$$\exp(-iH_{int}t/\hbar)|s_j\rangle|A_k\rangle = |s_j\rangle N^{-\frac{1}{2}} \sum_{l=0}^{N-1} \exp[-i(jgt/\hbar + 2\pi k/N)l]|B_l\rangle \qquad 2.22 \tag{21.7}$$

We now adjust the coupling g and the duration of the interaction t so that the action ι expressed in Planck units $2\pi\hbar$ is a multiple of $1/N$;

$$\iota = gt/\hbar = G * 2\pi/N \ . \tag{2.23a}$$

For an integer G, Eq. (2.22) can be readily evaluated:

$$\exp(-iH_{int}t/\hbar)|s_j\rangle|A_k\rangle = |s_j\rangle|A_{\{k+G*j\}_N}\rangle. \qquad 2.24 \tag{21.8}$$

This is a shift of the apparatus state by an amount $G * j$ proportional to the eigenvalue j of the state of the system. G plays the role of gain. The index $\{k + G * j\}_N$ is evaluated modulo N, where N is the number of the possible outcomes, that is, the dimensionality of the Hilbert space of the apparatus pointer $\mathcal{A}$: When $G * j > N$, the pointer will just rotate through the initial "zero". The truth table for $G = 1$ defines a `c-shift`, Eq. (2.13), and with $k = 0$ leads to a premeasurement, Eq. (2.1).

The form of the interaction, Eq. (2.19), in conjunction with the initial state decide the direction of information transfer. Note that – as was the case with the `c-not`s – the observable that commutes with the interaction Hamiltonian will not be perturbed:

$$[H_{int}, \hat{s}] = 0 \tag{2.25}$$

$\hat{s}$ commutes with H_{int}, and is therefore a non-demolition observable (Braginsky, Vorontsov and Thorne, 1980; Caves et al, 1980; Bocko and Onofrio, 1996).

Amplification

Amplification was often regarded as the process forcing quantum potentialities to become classical reality. Its example is an extension of the model of measurement described above.

Assume the Hilbert space of the apparatus pointer is large compared with the space spanned by the eigenstates of the measured observable $\hat{s}$:

$$N = Dim(\mathcal{H}_\mathcal{A}) \gg Dim(\mathcal{H}_\mathcal{S}) = n \tag{2.26}$$

Then one can increase ι to an integer multiple G of $2\pi/N$. This was implicit in Eqs. (2.23a) and (2.24). However, larger ι will lead to redundancy only when the apparatus the Hilbert space has many more dimensions in then there are possible outcomes. Otherwise, only "wrapping" of the same record will ensue. The simplest example of such wrapping: $(\texttt{c-not})^2$ is the identity. For $N \gg n$, however, one can attain gain:

$$G = Ngt/2\pi\hbar \ . \tag{2.23b}$$

The outcomes are now separated by $G-1$ "empty" eigenstates of the record observable. In this sense $G \gg 1$ achieves redundancy, providing that wrapping of the record is avoided, which is guaranteed when:

$$nG < N \ . \tag{2.27}$$

Amplification is useful in presence of noise. For example, it may be difficult to initiate the apparatus in $|A_0\rangle$, so the initial state may be a superposition;

$$|a_l\rangle = \sum_k \alpha_l(k)|A_k\rangle \ . \tag{2.28a}$$

Indeed, typically a mixture of such superpositions;

$$\rho^0_{\mathcal{A}} = \sum_i w_i |a_i\rangle\langle a_i| \tag{2.28b}$$

may be the starting point for a premeasurement. Then:

$$|s_k\rangle\langle s_{k'}|\rho_{\mathcal{A}} = |s_k\rangle\langle s_{k'}| \sum_l w_l |a_l\rangle\langle a_l|$$

$$\longrightarrow |s_k\rangle\langle s_{k'}| \sum_l w_l |a_{l+Gk}\rangle\langle a_{l+Gk'}| \qquad 2.29 \tag{21.9}$$

where $|a_{l+Gk}\rangle$ obtains from $|a_l\rangle$, Eq. (2.28a), through:

$$|a_{l+Gk}\rangle \;=\; \sum_j \alpha_l(j) |A_{j+Gk}\rangle \;, \tag{2.30}$$

and the simplifying assumption about the coefficients;

$$\alpha_l(j) = \alpha(j-l) \tag{2.31}$$

has been made. Its aim to focus on the case when the apparatus states are peaked around a certain value l (e.g., $\alpha_l(j) \sim \exp(-(j-l)^2/2\Delta^2)$, and where the form of their distribution over $\{|A_k\rangle\}$ does not depend on l.

A good measurement allows one to distinguish states of the system. Hence, it must satisfy:

$$|\langle a_{l+Gk}|a_{l+Gk'}\rangle|^2$$

$$= |\textstyle\sum_j \alpha(j+G(k-k'))\alpha^*(j)|^2 \approx \delta_{k',k} \;. \qquad 2.32 \tag{21.10}$$

States of the system that need to be distinguished should rotate the pointer of the apparatus to the correlated outcome states that are approximately orthogonal. When the coefficients $\alpha(k)$ are peaked around $k=0$ with dispersion Δ, this implies:

$$\Delta \ll G \;. \tag{2.33}$$

In the general case of an initial mixture, Eq. (2.29), one can evaluate the dispersion of the expectation value of the record observable $\hat{A}$ as:

$$\langle \hat{A}^2\rangle - \langle \hat{A}\rangle^2 \;=\; Tr\rho^0_{\mathcal{A}}\hat{A}^2 \;-\; (Tr\rho^0_{\mathcal{A}}\hat{A})^2 \tag{2.34}$$

The outcomes are distinguishable when:

$$\langle \hat{A}^2\rangle - \langle \hat{A}\rangle^2 \ll G \tag{2.35}$$

Interaction with the environment yields a mixture of the form of Eq. (2.29). Amplification can protect measurement outcomes from noise through redundancy.[5]

[5]The above model of amplification is unitary. Yet, it contains seeds of irreversibility. Reversibility of `c-shift` is evident: As the interaction continues, the two systems will eventually disentangle. For instance, it takes $t_e = 2\pi\hbar/(gN)$ (see Eq. (2.23b) with $G=1$) to entangle $\mathcal{S}$ ($Dim(\mathcal{H}_{\mathcal{S}}) = n$) with an $\mathcal{A}$ with $Dim(\mathcal{H}_{\mathcal{A}}) = N \geq n$ pointer states. However, as the interaction continues, $\mathcal{A}$ and $\mathcal{S}$ disentangle. For a `c-shift` this recurrence timescale is: $t_{Rec} = Nt_e = 2\pi\hbar/g$. It corresponds to gain $G = N$. Thus, for an instant of less than t_e at $t = t_{Rec}$ the apparatus disentangles from the system, as $\{k + N * j\}_N = k$. Reversibility results in recurrences of the initial state, but for $N \gg 1$, they are rare.
For less regular interactions (e.g, involving environment) recurrence time is much longer. In that case, t_{Rec} is,

21.2.2 Information transfer in measurements

Information transfer is the objective of the measurement process. Yet, quantum measurements were only rarely analyzed from that point of view. As a result of the interaction of the system $\mathcal{S}$ with the apparatus $\mathcal{A}$, their joint state is still pure $|\Psi_t\rangle$, Eq. (2.1), but each of the subsystems is in a mixture:

$$\rho_{\mathcal{S}} \;=\; Tr_{\mathcal{A}}|\Psi_t\rangle\langle\Psi_t| \;=\; \sum_{i=0}^{N-1} |a_i|^2 |s_i\rangle\langle s_i| \;; \qquad \text{2.36a} \tag{21.11}$$

$$\rho_{\mathcal{A}} \;=\; Tr_{\mathcal{S}}|\Psi_t\rangle\langle\Psi_t| \;=\; \sum_{i=0}^{N-1} |a_i|^2 |A_i\rangle\langle A_i| \;. \qquad \text{2.36b} \tag{21.12}$$

Partial trace leads to *reduced density matrices*, here $\rho_{\mathcal{S}}$ and $\rho_{\mathcal{A}}$, important for what follows. They describe subsystems to the observer who, before the premeasurement, knew pure states of the system and of the apparatus, but who has access to only one of them afterwards.

Reduced density matrix is a technical tool of paramount importance. It was introduced by Landau (1927) as the only density matrix that gives rise to the correct measurement statistics given the usual formalism that includes Born's rule for calculating probabilities (see e.g. p. 107 of Nielsen and Chuang, 2000, for an insightful discussion). This remark will come to haunt us later when in Section VI we shall consider the relation between decoherence and probabilities: In order to derive Born's rule it will be important not to assume it in some guise!

Following premeasurement, the information about the subsystems available to the observer locally decreases. This is quantified by the increase of the entropies:

$$\begin{aligned} H_{\mathcal{S}} \;&=\; -Tr\rho_{\mathcal{S}} \log \rho_{\mathcal{S}} = -\sum_{i=0}^{N-1} |a_i|^2 \log |a_i|^2 \\ &=\; -Tr\rho_{\mathcal{A}} \log \rho_{\mathcal{A}} = H_{\mathcal{A}} \qquad \text{2.37} \end{aligned} \tag{21.13}$$

As the evolution of the whole $\mathcal{SA}$ is unitary, the increase of entropies in the subsystems is

---

in effect, a Poincaré time: $t_{Rec} \sim t_{Poincaré} \approx N! t_e$. In any case $t_{Rec} \gg t_e$ for large N. Undoing entanglement in this manner would be exceedingly difficult because one would need to know precisely when to look, and because one would need to isolate the apparatus or the immediate environment from other degrees of freedom – their environments.

The price of letting the entanglement undo itself by waiting for an appropriate time interval is at the very least given by the cost of storing the information on how long is it necessary to wait. In the special `c-shift` case this is $\sim \log N$ memory bits. In situations when eigenvalues of the interaction Hamiltonian are not commensurate, it will be more like $\sim \log N! \approx N \log N$, as the entanglement will get undone only after a Poincaré time. Both classical and quantum case can be analyzed using algorithmic information . For related discussions see Zurek, (1989), Caves, (1994); Schack and Caves (1996) and Zurek (1998b).

Amplified correlations are hard to contain. The return to purity after t_{Rec} in the manner described above can be hoped for only when either the apparatus or the immediate environment $\mathcal{E}$ (i.e., the environment directly interacting with the system) cannot "pass on" the information to their more remote environments $\mathcal{E}'$. The degree of isolation required puts a stringent limit on the coupling $g_{\mathcal{E}\mathcal{E}'}$ between the two environments: Return to purity can be accomplished in this manner only if $t_{Rec} < t_{e'} = 2\pi\hbar/(N' g_{\mathcal{E}\mathcal{E}'})$, where N' is the dimension of the Hilbert space of the environment $\mathcal{E}'$. Hence, the two estimates of t_{Rec} translate into: $g_{\mathcal{E}\mathcal{E}'} < g/N'$ for the regular spectrum, and the much tighter; $g_{\mathcal{E}\mathcal{E}'} < g/N!N'$ for the random case more relevant for decoherence.

In short, once information "leaks" into the correlations between the system and the apparatus or the environment, keeping it from spreading further ranges between very hard and next to impossible. With the exception of very special cases (small N, regular spectrum), the strategy of "enlarging the system, so that it includes the environment" – occasionally mentioned as an argument against decoherence – is doomed to fail, unless the Universe as a whole is included. This is a questionable setting (as the observers are *inside* this "isolated" system) and in any case makes the relevant Poincaré time absurdly long!

compensated by the increase of the mutual information:

$$\mathcal{I}(\mathcal{S}:\mathcal{A}) = H_{\mathcal{S}} + H_{\mathcal{A}} - H_{\mathcal{SA}} = -2\sum_{i=0}^{N-1} |a_i|^2 \log |a_i|^2 \qquad 2.38 \tag{21.14}$$

It was used in quantum theory as a measure of entanglement (Zurek, 1983; Barnett and Phoenix, 1989).

Action per bit

An often raised question concerns the price of information in units of some other "physical currency", (Brillouin, 1962; 1964; Landauer, 1991). Here we shall establish that the least action necessary to transfer one bit is of the order of a fraction of $\hbar$ for quantum systems with two-dimensional Hilbert spaces. Information transfer can be made cheaper on the "wholesale" level, when the systems involved have large Hilbert spaces.

Consider Eq. (2.1). It evolves initial product state of the two subsystems into a superposition of product states, $(\sum_j \alpha_j|s_j\rangle)|A_0\rangle \longrightarrow \sum_j \alpha_j|s_j\rangle|A_j\rangle$. The expectation value of the action involved is no less than:

$$I = \sum_{j=0}^{N-1} |\alpha_j|^2 \arccos |\langle A_0|A_j\rangle| \tag{2.39}$$

When $\{|A_j\rangle\}$ are mutually orthogonal, the action is:

$$I = \pi/2 \tag{2.40}$$

in Planck ($\hbar$) units. This estimate can be lowered by using the initial $|A_0\rangle$, a superposition of the outcomes $|A_j\rangle$. In general, interaction of the form:

$$H_{\mathcal{SA}} = ig \sum_{k=0}^{N-1} |s_k\rangle\langle s_k| \sum_{l=0}^{N-1} (|A_k\rangle\langle A_l| - h.c.) \qquad 2.41 \tag{21.15}$$

saturates the lower bound given by:

$$I = \arcsin \sqrt{1 - 1/N}\ , \tag{2.42}$$

For a two-dimensional Hilbert space the average action can be thus brought down to $\pi\hbar/4$ (Zurek, 1981; 1983).

As the size of the Hilbert space increases, action involved approaches the asymptotic estimate of Eq. (2.40). The entropy of entanglement can be as large as $\log N$ where N is the dimension of the Hilbert space of the smaller of the two systems. Thus, the least action per bit of information decreases with the increase of N:

$$\iota = \frac{I}{\log_2 N} \approx \frac{\pi}{2\log_2 N} \tag{2.43}$$

This may be one reason why information appears "free" in the macroscopic domain, but expensive (close to $\hbar$/bit) in the quantum case of small Hilbert spaces.

21.2.3 "Collapse" analogue in a classical measurement

Definite outcomes we perceive appear to be at odds with the principle of superposition. They can nevertheless occur also in quantum physics when the initial state of the measured system is – already before the measurement – in one of the eigenstates of the measured observable. Then

Eq. (2.1) will deterministically rotate the pointer of the apparatus to the appropriate record state. The result of such a measurement can be predicted by an *insider* – an observer aware of the initial state of the system. This *a priori* knowledge can be represented by the preexisting record $|A_i\rangle$, which is only corroborated by an additional measurement:

$$|A_i\rangle|A_0\rangle|\sigma_i\rangle \longrightarrow |A_i\rangle|A_i\rangle|\sigma_i\rangle \ . \qquad (2.44a)$$

In classical physics complete information about the initial state of an isolated system always allows for an exact prediction of its future state: A well-informed observer will be even able to predict future of the classical Universe as a whole ("Laplace's demon").

Any element of surprise (any use of probabilities) must be therefore blamed on partial ignorance. Thus, when the information available initially does not include the exact initial state of the system, observer can use an ensemble described by $\rho_{\mathcal{S}}$ – by a list of possible initial states $\{|\sigma_i\rangle\}$ and their probabilities p_i. This is the *ignorance interpretation* of probabilities. We shall see in section VI that – using quantum envariance – one can justify ignorance about a part of the system by relying on perfect knowledge of the whole.

Through measurement observer finds out which of the potential outcomes consistent with his prior (lack of) information actually happens. This act of acquisition of information changes physical state of the observer – the state of his memory: The initial memory state containing description A_{ρ_S} of an ensemble and a "blank" A_0, $|A_{\rho_S}\rangle\langle A_{\rho_S}| \ |A_0\rangle\langle A_0|$, is transformed into record of a specific outcome: $|A_{\rho_S}\rangle\langle A_{\rho_S}| \ |A_i\rangle\langle A_i|$. In quantum notation this process will be described by such a *discoverer* as a random "collapse":

$$|A_{\rho_S}\rangle\langle A_{\rho_S}| \ |A_0\rangle\langle A_0| \ \sum_i p_i|\sigma_i\rangle\langle\sigma_i|$$
$$\longrightarrow |A_{\rho_S}\rangle\langle A_{\rho_S}| \ |A_i\rangle\langle A_i| \ |\sigma_i\rangle\langle\sigma_i| \ . \qquad 2.44\text{b} \qquad (21.16)$$

This is only the description of what happens "as reported by the discoverer". Deterministic representation of this very same process by Eq. (2.44a) is still possible. In other words, in classical physics discoverer can be always convinced that the system was in a state $|\sigma_i\rangle$ already before the record is made in accord with Eq. (2.44b).

This sequence of events as seen by the discoverer looks like a "collapse" (see also Zurek, 1998a,b): For instance, insider who knew the state of the system before discoverer carried out his measurement need not notice any change of that state when he makes further "confirmatory" measurements. This property is the cornerstone of the "reality" of classical states – they need not ever change as a consequence of measurements. We emphasize, however, that while the state of the system may remain unchanged, the state of the observer must change to reflect the acquired information.

Last not least, an *outsider* – someone who knows about the measurement, but (in contrast to the insider) not about the initial state of the system nor (in contrast to the discoverer) about the measurement outcome, will describe the same process still differently:

$$|A_{\rho_S}\rangle\langle A_{\rho_S}| \ |A_0\rangle\langle A_0| \ \sum_i p_i|\sigma_i\rangle\langle\sigma_i| \longrightarrow$$
$$\longrightarrow |A_{\rho_S}\rangle\langle A_{\rho_S}|(\sum_i p_i|A_i\rangle\langle A_i| \ |\sigma_i\rangle\langle\sigma_i|) \ . \qquad 2.44\text{c} \qquad (21.17)$$

This view of the outsider, Eq. (2.44c), combines one-to-one classical correlation of the states of the system and the records with the indefiniteness of the outcome.

We have just seen three distinct quantum-looking descriptions of the very same *classical* process (see Zurek, 1989, and Caves, 1994 for previous studies of the insider - outsider theme). They differ only in the information available *ab initio* to the observer. The information in

possession of the observer prior to the measurement determines in turn whether – to the observer – the evolution appears to be (a) a confirmation of the preexisting data, Eq. (2.44a), (b) a "collapse" associated with the information gain, Eq. (2.44b) – and with the entropy decrease translated into algorithmic randomness of the acquired data (Zurek, 1989; 1998b) – or (c) an entropy-preserving establishment of a correlation, Eq. (2.44c). All three descriptions are classically compatible, and can be implemented by the same (deterministic and reversible) dynamics.

In classical physics the insider view always exists in principle. In quantum physics it does not. Every observer in a classical Universe could in principle aspire to be an ultimate insider. The fundamental contradiction between every observer knowing precisely the state of the rest of the Universe (including the other observers) can be swept under the rug (if not really resolved) in the Universe where the states are infinitely precisely determined and the observer's records (as a consequence of the $\hbar \to 0$ limit) may have an infinite capacity for information storage. However – given a set value of $\hbar$ – information storage resources of any finite physical system are finite. Hence, in quantum physics observers remain largely ignorant of the detailed state of the Universe as there can be *no information without representation* (Zurek, 1994).

Classical "collapse" is described by Eq. (2.44b): The observer discovers the state of the system. From then on, the state of the system will remain correlated with his record, so that all the future outcomes can be predicted, in effect by iterating Eq. (2.44a). This disappearance of all the potential alternatives save for one that becomes a "reality" is the essence of the collapse. There need not be anything quantum about it.

Einselection in observers memory provides many of the ingredients of the "classical collapse" in the quantum context. In presence of einselection, one-to-one correspondence between the state of the observer and his knowledge about the rest of the Universe can be firmly established, and (at least in principle) operationally verified: One could measure bits in observers memory and determine what he knows without altering his records – without altering his state. After all, one can do so with a classical computer. Existential interpretation recognizes that the information possessed by the observer is reflected in his einselected state, explaining his perception of a single "branch" – "his" classical Universe.

21.3 Chaos and Loss of Coherence

The study of the relationship between the quantum and the classical has been – for a long time – focused almost entirely on measurements. However, the problem of measurement is difficult to discuss without observers. And once observer enters, it is often hard to avoid its ill-understood anthropic attributes such as consciousness, awareness, and the ability to perceive.

We shall sidestep these presently "metaphysical" problems and focus on the information-processing underpinnings of the "observership". It is nevertheless fortunate that there is another problem with the quantum - classical correspondence that leads to interesting questions not motivated by measurements. As was anticipated by Einstein (1917) before the advent of modern quantum theory, chaotic motion presents such a challenge. Full implications of classical dynamical chaos were understood much later. The concern about the quantum-classical correspondence in this modern context dates to Berman and Zaslavsky (1978) and Berry and Balazs (1979) (see Haake, 1991 and Casati and Chirikov, 1995a, for references). It has even led some to question validity of quantum theory (Ford and Mantica, 1992).

21.3.1 Loss of the quantum-classical correspondence

The interplay between quantum interference and chaotic exponential instability leads to the rapid loss of the quantum-classical correspondence. Chaos in dynamics is characterized by the

exponential divergence of the classical trajectories. As a consequence, a small patch representing the probability density in phase space is exponentially stretching in unstable directions and to exponentially compressing in the stable directions. The rates of stretching and compression are given by positive and negative Lyapunov exponents Λ_i. Hamiltonian evolution demands that the sum of all the Lyapunov exponents be zero. In fact, they appear in $\pm\Lambda_i$ pairs.

Loss of the correspondence in chaotic systems is a consequence of the exponential stretching of the effective support of the probability distribution in the unstable direction (say, x) and its exponential narrowing in the complementary direction (Zurek and Paz, 1994; Zurek, 1998b). As a consequence, classical probability distribution will develop structures on the scale:

$$\Delta p \sim \Delta p_0 \ \exp(-\Lambda t) \ . \tag{3.1}$$

Above, Δp_0 is the measure of the initial momentum spread. Λ is the net rate of contraction in the direction of momentum given by the Lyapunov exponents (but see Boccaletti, Farini, and Arecchi, 1997). In the real chaotic system stretching and narrowing of the probability distribution in both x and p occur simultaneously, as the initial patch is rotated and folded. Eventually, the envelope of its effective support will swell to fill in the available phase space, resulting in the wavepacket coherently spread over the spatial region of no less than;

$$\Delta x \sim (\hbar/\Delta p_0) \ \exp(\Lambda t) \tag{3.2}$$

until it becomes confined by the potential, while the small-scale structure will continue to descend to ever smaller scales (Fig. 1). Breakdown of the quantum-classical correspondence can be understood in two complementary ways, either as a consequence of small Δp (see the discussion of Moyal bracket below), or as a result of large Δx.

Coherent exponential spreading of the wavepacket – large Δx – must cause problems with correspondence. This is inevitable, as classical evolution appeals to the idealization of a point in phase space acted upon by a force given by the gradient $\partial_x V$ of the potential $V(x)$ evaluated at that point. But quantum wavefunction can be coherent over a region larger than the nonlinearity scale χ over which the gradient of the potential changes significantly. χ can be usually estimated by:

$$\chi \simeq \sqrt{\partial_x V/\partial_{xxx} V} \ , \tag{3.3}$$

and is typically of the order of the size L of the system:

$$L \sim \chi \ . \tag{3.4}$$

An initially localized state evolving in accord with Eqs. (3.1) and (3.2) will spread over such scales after:

$$t_\hbar \simeq \Lambda^{-1} \ln \frac{\Delta p_0 \chi}{\hbar} \ . \tag{3.5}$$

It is then impossible to tell what is the force acting on the system, as it is not located in any specific x. This estimate of what can be thought of as Ehrenfest time – the time over which a quantum system that has started in a localized state will continue to be sufficiently localized for the quantum corrections to the equations of motion obeyed by its expectation values to be negligible (Gottfried, 1966) – is valid for chaotic systems. Logarithmic dependence is the result of inverting of the exponential sensitivity. In the absence of the exponential instability ($\Lambda = 0$) divergence of trajectories is typically polynomial, and leads to a power law dependence, $t_\hbar \sim (I/\hbar)^\alpha$, where I is the classical action. Thus, macroscopic (large I) integrable systems can follow classical dynamics for a very long time, providing they were initiated in a localized state. For chaotic systems $t_\hbar$ also becomes infinite in the limit $\hbar \to 0$, but that happens only logarithmically slowly. As we shall see below, in the context of quantum-classical correspondence this is too slow for comfort.

Another way of describing the "root cause" of the correspondence breakdown is to note that after the timescale of the order of $t_\hbar$ quantum wave function of the system would have spread over all of the available space, and is being forced to "fold" onto itself. Fragments of the wavepacket arrive at the same location (although with different momenta, and having followed different paths). The ensuing evolution critically depends on whether they have retained phase coherence. When coherence persists, a complicated interference event decides the subsequent evolution. And – as can be anticipated from the double slit experiment – there is a big difference between coherent and incoherent folding in the configuration space. This translates into the loss of correspondence, which sets in surprisingly quickly, at $t_\hbar$.

To find out how quickly, we estimate $t_\hbar$ for an obviously macroscopic Hyperion, chaotically tumbling moon of Saturn (Wisdom, 1985). Hyperion has a prolate shape of a potato and moves on an eccentric orbit with a period t_O =21 days. Interaction between its gravitational quadrupole and the tidal field of Saturn leads to chaotic tumbling with Lyapunov time $\Lambda^{-1} \simeq$42 days.

To estimate the time over which orientation of Hyperion becomes delocalized, we use a formula (Berman and Zaslavsky, 1978, Berry and Balazs, 1979):

$$t_r = \Lambda^{-1} \ln \frac{LP}{\hbar} = \Lambda^{-1} \ln \frac{I}{\hbar} \tag{3.6}$$

Above L and P give the range of values of the coordinate and momentum in phase space of the system. Since $L \simeq \chi$ and $P > \Delta p_0$, it follows that $t_r \geq t_\hbar$. On the other hand, $LP \simeq I$, the action of the system.

The advantage of Eq. (3.6) is its insensitivity to initial conditions, and the ease with which the estimate can be obtained. For Hyperion, a generous overestimate of the classical action I can be obtained from its binding energy E_B and its orbital time t_O:

$$I/\hbar \simeq E_B t_O/\hbar \simeq 10^{77} \tag{3.7}$$

The above estimate (Zurek, 1998b) is "astronomically" large. However, in the calculation of the loss of correspondence, Eq. (3.6), only its logarithm enters. Thus,

$$t_r^{Hyperion} \simeq 42[\text{days}] \ln 10^{77} \simeq 20[\text{yrs}] \tag{3.8}$$

After approximately 20 years Hyperion would be in a coherent superposition of orientations that differ by 2π!

We conclude that after a relatively short time an obviously macroscopic chaotic system becomes forced into a flagrantly non-local "Schrödinger cat" state. In the original discussion (Schrödinger, 1935a,b) an intermediate step in which decay products of the nucleus were *measured* to determine the fate of the cat was essential. Thus, it was possible to maintain that the preposterous superposition of the dead and alive cat could be avoided providing that quantum measurement (with the "collapse" it presumably induces) was properly understood.

This cannot be the resolution for chaotic quantum systems. They can evolve – as the example of Hyperion demonstrates – into states that are non-local, and, therefore, extravagantly quantum, simply as a result of the exponentially unstable dynamics. Moreover, this happens surprisingly quickly, even for very macroscopic examples. Hyperion is not the only chaotic system. There are asteroids that have chaotically unstable orbits (e.g., Chiron), and even indications that the solar system as a whole is chaotic (Laskar, 1989; Sussman and Wisdom, 1992). In all of these cases straightforward estimates of $t_\hbar$ yield answers much smaller than the age of the solar system. Thus, if unitary evolution of closed subsystems was a complete description of planetary dynamics, planets would be delocalized along their orbits.

21.3.2 Moyal bracket and Liouville flow

Heuristic argument about breakdown of the quantum-classical correspondence can be made more rigorous with the help of the Wigner function. We start with the von Neumann equation:

$$i\hbar\dot{\rho} = [H, \rho] \ . \tag{3.9}$$

It can be transformed into the equation for Wigner function W, which is defined in phase space:

$$W(x,p) = \frac{1}{2\pi\hbar}\int \exp\left(\frac{ipy}{\hbar}\right)\rho(x-\frac{y}{2}, x+\frac{y}{2})dy \ . \tag{3.10}$$

The result is:

$$\dot{W} = \{H, W\}_{MB} \ . \tag{3.11}$$

Here $\{...,...\}_{MB}$ stands for Moyal bracket, the Wigner transform of the von Neumann bracket (Moyal, 1949).

Moyal bracket can be expressed in terms of the Poisson bracket $\{...,...\}$, which generates Liouville flow in the classical phase space, by the formula:

$$i\hbar\{...,...\}_{MB} = \sin(i\hbar\{...,...\}) \ . \tag{3.12}$$

When the potential $V(x)$ is analytic, Moyal bracket can be expanded (Hillery et al, 1984) in powers of $\hbar$:

$$\dot{W} = \{H, W\} + \sum_{n\geq 1} \frac{\hbar^{2n}(-)^n}{2^{2n}(2n+1)!}\partial_x^{2n+1}V\partial_p^{2n+1}W \ . \qquad 3.13 \tag{21.18}$$

The first term is just the Poisson bracket. Alone, it would generate classical motion in phase space. However, when the evolution is chaotic, quantum corrections (proportional to the odd order momentum derivatives of the Wigner function) will eventually dominate the right hand side of Eq. (3.10). This is because the exponential squeezing of the initially regular patch in phase space (which begins its evolution in the classical regime, where the Poisson bracket dominates) leads to an exponential explosion of the momentum derivatives. Consequently, after a time logarithmic in $\hbar$, (Eqs. (3.5), (3.6)) the Poisson bracket will cease to be a good estimate of the right hand side of Eq. (3.13).

The physical reason for the ensuing breakdown of the quantum-classical correspondence was already explained before: Exponential instability of the chaotic evolution delocalizes the wavepacket. As a result, the force acting on the system is no longer given by the gradient of the potential evaluated at the location of the system: It is not even possible to say where the system is, since it is in a superposition of many distinct locations. Consequently, phase space distribution and even the typical observables of the system noticeably differ when evaluated classically and quantum mechanically (Haake, Kuś and Sharf, 1987; Habib, Shizume and Zurek, 1998; Karkuszewski, Zakrzewski, and Zurek, 2002). Moreover, this will happen after an uncomfortably short time $t_\hbar$.

21.3.3 Symptoms of correspondence loss

Wavepacket becomes rapidly delocalized in a chaotic system, and the correspondence between classical and quantum is quickly lost. Schrödinger cat states appear after $t_\hbar$ and this is the overarching interpretational as well as physical problem: In the familiar real world we never seem to encounter such smearing of the wavefunction even in the examples of chaotic dynamics it is predicted by quantum theory.

Expectation values

Measurements often average out fine phase space structures, which may be striking, but experimentally inaccessible symptom of breakdown of the correspondence. Thus, one might hope that when interference patterns in the Wigner function are ignored by looking at the coarse-grained distribution, the quantum results should be in accord with the classical. This would not exorcise the 'chaotic cat' problem. Moreover, breakdown of correspondence can be also seen in the expectation values of quantities that are smooth in phase space.

Trajectories diverge exponentially in a chaotic system. A comparison between expectation values for a single trajectory and for a delocalized quantum state (which is how the Ehrenfest theorem mentioned above is usually stated) would clearly lead to a rapid loss of correspondence. One may object to the use of a single trajectory and argue that both quantum and classical state be prepared and accessed only through measurements that are subject to the Heisenberg indeterminacy. Thus, it should be fair to compare averages over an evolving Wigner function with an initially identical classical probability distribution (Ballentine, Yang, and Zibin, 1994; Haake, Kuś & Sharf, 1987; Fox and Elston, 1994; Miller, Sarkar and Zarum, 1998). These are shown in Fig. 2 for an example of a driven chaotic system. Clearly, there is reason for concern: Fig. 2 (corroborated by other studies, see e.g. Karkuszewski, Zakrzewski, and Zurek, 2002, for references) demonstrates that not just phase space portrait but also averages diverge at a time $\sim t_\hbar$.

In integrable systems rapid breakdown of correspondence may still occur, but only for very special initial conditions. It is due to the local instability in phase space. Indeed, a double - slit experiment is an example of a regular system in which a local instability (splitting of the paths) leads to correspondence loss, but only for judiciously selected initial conditions. Thus, one may dismiss it as a consequence of a rare pathological starting point, and argue that the conditions that lead to discrepancies between classical and quantum behavior exist, but are of measure zero in the classical limit.

In the chaotic case the loss of correspondence is typical. As shown in Fig. 2, it happens after a disturbingly short $t_\hbar$ for generic initial conditions. The time at which the quantum and classical expectation values diverge in the example studied here is consistent with the estimates of $t_\hbar$, Eq. (3.5), but exhibits a significant scatter. This is not too surprising – exponents characterizing local instability vary noticeably with the location in phase space. Hence, stretching and contraction in phase space will occur at a rate that depends on the specific trajectory. Dependence of its typical magnitude as a function of $\hbar$ is still not clear. Emerson and Ballentine (2001a&b) study coupled spins and argue that it is of order of $\hbar$, but Fig. 2 suggests it decreases more slowly than that, and that it may be only logarithmic in $\hbar$ (Karkuszewski et al. 2002).

Structure saturation

Evolution of the Wigner function exhibits rapid buildup of interference fringes. These fringes become progressively smaller, until saturation when the wavepacket is spread over the available phase space. At that time their scales in momentum and position are typically:

$$dp = \hbar/L \quad ; \quad dx = \hbar/P \tag{3.14, 3.15}$$

where L (P) defines the range of positions (momenta) of the effective support of W in phase space.

Hence, smallest structures in the Wigner function occur (Zurek, 2001) on scales corresponding to action:

$$a \;=\; dx\; dp \;=\; \hbar \times \hbar/LP \;=\; \hbar^2/I \;, \tag{3.16}$$

where $I \simeq LP$ is the classical action of the system. Action $a \ll \hbar$ for macroscopic I.

Sub-Planck structure is a kinematic property of quantum states. It limits their sensitivity to perturbations, and has applications outside quantum chaos or decoherene. For instance, Schrödinger cat state can be used as a weak force detector (Zurek, 2001), and its sensitivity is determined by Eqs. (3.14)-(3.16).

Structure saturation on scale a is an important distinction between quantum and classical. In chaotic systems smallest structures in the classical probability density exponentially shrink with time, in accord with Eq. (3.1) (see Fig. 1). Equation (3.16) has implications for decoherence, as a controls sensitivity of the systems as well as environments (Zurek, 2001; Karkuszewski, Jarzynski, and Zurek, 2002): As a result of smallness of a, Eq. (3.16), and as anticipated by Peres (1993), quantum systems are more sensitive to perturbations when their classical counterparts are chaotic (see also Jalabert and Pastawski, 2001). But – in contrast to classical chaotic systems – they are not exponentially sensitive to infinitesimally small perturbations: Rather, the smallest perturbations that can effective are set by Eq. (3.16).

Emergence of Schrödinger cats through dynamics is a challenge to quantum - classical correspondence. It is not yet clear to what extent one should be concerned about the discrepancies between quantum and classical averages: The size of this discrepancy may or may not be negligible. But in the original Schrödinger cat problem quantum and classical expectation values (for the survival of the cat) were also in accord. In both cases it is ultimately the state of the cat which is most worrisome.

Note that we have not dealt with dynamical localization (Casati and Chirikov, 1995a). This is because it appears after too long a time ($\sim \hbar^{-1}$) to be a primary concern in the macroscopic limit, and is quite sensitive to small perturbations of the potential (Karkuszewski, Zakrzewski, and Zurek, 2002).

21.4 Environment-Induced Superselection

The principle of superposition applies only when the quantum system is closed. When the system is open, interaction with the environment results in an incessant monitoring of some of its observables. As a result, pure states turn into mixtures that rapidly diagonalize in the einselected states. These pointer states are chosen with the help of the interaction Hamiltonian and are independent of the initial state of the system. Their predictability is key to the effective classicality (Zurek, 1993a; Zurek, Habib, and Paz, 1993).

Environments can be external (such as particles of the air or photons that scatter off, say, the apparatus pointer) or internal (collections of phonons or other internal excitations). Often, environmental degrees of freedom emerge from the split of the original set of degrees of freedom into the "system of interest" which may be a collective observable (e.g., an order parameter in a phase transition), and the "microscopic remainder".

The set of einselected states is called *the pointer basis* (Zurek, 1981) in recognition of its role in measurements. The criterion for the einselection of states goes well beyond the often repeated characterizations based on the instantaneous eigenstates of the density matrix. What is of the essence is the ability of the einselected states to survive monitoring by the environment. This heuristic criterion can be made rigorous by quantifying predictability of the evolution of the candidate states, or of the associated observables. Einselected states provide optimal initial conditions: They can be employed for the purpose of prediction better than other Hilbert space alternatives – they retain correlations in spite of their immersion in the environment.

Three quantum systems – the measured system $\mathcal{S}$, the apparatus $\mathcal{A}$, and the environment $\mathcal{E}$ – and correlations between them are the subject of our study. In pre-measurements $\mathcal{S}$ and $\mathcal{A}$ interact. Their resulting entanglement transforms into an effectively classical correlation as a result of the interaction between $\mathcal{A}$ and $\mathcal{E}$.

This $\mathcal{SAE}$ triangle helps analyze decoherence and study its consequences. By keeping all

three corners of this triangle in mind, one can avoid confusion, and maintain focus on the *correlations* between, e.g., the memory of the observer and the state of the measured system. The evolution from a quantum entanglement to the classical correlation may be the easiest relevant theme to define operationally. In the language of the last part of Section II, we are about to justify the "outsider" point of view, Eq. (2.44c), before considering the "discoverer", Eq. (2.44b) and the issue of the "collapse". In spite of this focus on correlations, we shall often suppress one of the corners of the $\mathcal{SAE}$ triangle to simplify notation. All three parts will however play a role in formulating questions and in motivating criteria for classicality.

21.4.1 Models of einselection

The simplest case of a single act of decoherence involves just three one-bit systems (Zurek, 1981; 1983). They are denoted by $\mathcal{S}$, $\mathcal{A}$, and $\mathcal{E}$ in an obvious reference to their roles. The measurement starts with the interaction of the measured system with the apparatus:

$$|\uparrow\rangle|A_0\rangle \longrightarrow |\uparrow\rangle|A_1\rangle,\ |\downarrow\rangle|A_0\rangle \longrightarrow |\downarrow\rangle|A_0\rangle; \qquad (4.1a,\ b)$$

where $\langle A_0|A_1\rangle = 0$. For a general state:

$$(\alpha|\uparrow\rangle + \beta|\downarrow\rangle)|A_0\rangle \longrightarrow \alpha|\uparrow\rangle|A_1\rangle + \beta|\downarrow\rangle|A_0\rangle = |\Phi\rangle. \qquad (4.2)$$

These formulae are an example of a `c-not` like the premeasurement discussed in section 2.

The basis ambiguity – the ability to re-write $|\Phi\rangle$, Eq. (4.2), in any basis of, say, the system, with the superposition principle guaranteeing existence of the corresponding pure states of the apparatus – disappears when an additional system, $\mathcal{E}$, performs a premeasurement on $\mathcal{A}$:

$$\begin{aligned}&(\alpha|\uparrow\rangle|A_1\rangle + \beta|\downarrow\rangle|A_0\rangle)|\varepsilon_0\rangle \\ &\longrightarrow \alpha|\uparrow\rangle|A_1\rangle|\varepsilon_1\rangle + \beta|\downarrow\rangle|A_0\rangle|\varepsilon_0\rangle = |\Psi\rangle. \qquad 4.3\end{aligned} \qquad (21.19)$$

A collection of three correlated quantum systems is no longer subject to the basis ambiguity we have pointed out in connection with the EPR-like state $|\Phi\rangle$, Eq. (4.2). This is especially true when states of the environment are correlated with the simple products of the states of the apparatus - system combination (Zurek, 1981; Elby and Bub, 1994). In Eq. (4.3) this can be guaranteed (irrespective of the value of α and β) providing that:

$$\langle\varepsilon_0|\varepsilon_1\rangle = 0\ . \qquad (4.4)$$

When this orthogonality condition is satisfied, the state of the $\mathcal{A}-\mathcal{S}$ pair is given by a reduced density matrix:

$$\begin{aligned}\rho_{\mathcal{AS}} \ &= \ Tr_{\mathcal{E}}|\Psi\rangle\langle\Psi| = \\ |\alpha|^2|\uparrow\rangle\langle\uparrow||A_1\rangle\langle A_1| + |\beta|^2|\downarrow\rangle\langle\downarrow||A_0\rangle\langle A_0| \qquad 4.5a\end{aligned} \qquad (21.20)$$

containing only classical correlations.

If the condition of Eq. (4.4) did not hold – that is, if the orthogonal states of the environment were not correlated with the apparatus in the basis in which the original premeasurement was carried out – then the eigenstates of the reduced density matrix $\rho_{\mathcal{AS}}$ would be sums of products rather than simply products of states of $\mathcal{S}$ and $\mathcal{A}$. Extreme example of this situation is the pre-decoherence density matrix of the pure state:

$$\begin{aligned}|\Phi\rangle\langle\Phi| \quad &= |\alpha|^2|\uparrow\rangle\langle\uparrow||A_1\rangle\langle A_1| \ + \alpha\beta^*|\uparrow\rangle\langle\downarrow||A_1\rangle\langle A_0| \\ &+\alpha^*\beta|\downarrow\rangle\langle\uparrow||A_0\rangle\langle A_1| + |\beta|^2|\downarrow\rangle\langle\downarrow||A_0\rangle\langle A_0| \qquad 4.5b\end{aligned} \qquad (21.21)$$

Its eigenstate is $|\Phi\rangle$. When expanded, $|\Phi\rangle\langle\Phi|$ contains terms that are off-diagonal when expressed in any of the natural bases consisting of the tensor products of states in the two systems. Their disappearance as a result of tracing over the environment removes the basis ambiguity. Thus, for example, the reduced density matrix $\rho_{\mathcal{AS}}$, Eq. (4.5a), has the same form as the outsider description of the classical measurement, Eq. (2.44c).

In our simple model pointer states are easy to characterize: To leave pointer states untouched, the Hamiltonian of interaction $H_{\mathcal{AE}}$ should have the same structure as for the `c-not`, Eqs. (2.9) - (2.10): It should be a function of the pointer observable; $\hat{A} = a_0|A_0\rangle\langle A_0| + a_1|A_1\rangle\langle A_1|$ of the apparatus. Then the states of the environment will bear an imprint of the pointer states $\{|A_0\rangle, |A_1\rangle\}$. As noted in section II:

$$[H_{\mathcal{AE}}, \hat{A}] = 0 \tag{4.6}$$

immediately implies that $\hat{A}$ is a control, and its eigenstates will be preserved.

Decoherence of a single qubit

An example of continuous decoherence is afforded by a two-state apparatus $\mathcal{A}$ interacting with an environment of N other spins (Zurek, 1982). The two apparatus states are $\{|\Uparrow\rangle, |\Downarrow\rangle\}$. For the simplest, yet already interesting example the self-Hamiltonian of the apparatus disappears, $H_{\mathcal{A}} = 0$, and the interaction has the form:

$$\begin{aligned} H_{\mathcal{AE}} &= (|\Uparrow\rangle\langle\Uparrow| - |\Downarrow\rangle\langle\Downarrow|) \\ &\quad \otimes \sum_k g_k(|\uparrow\rangle\langle\uparrow| - |\downarrow\rangle\langle\downarrow|)_k \ , \qquad 4.7 \end{aligned} \tag{21.22}$$

Under the influence of this Hamiltonian the initial state:

$$|\Phi(0)\rangle = (a|\Uparrow\rangle + b|\Downarrow\rangle) \prod_{k=1}^{N}(\alpha_k|\uparrow\rangle_k + \beta_k|\downarrow\rangle_k) \qquad 4.8 \tag{21.23}$$

evolves into:

$$|\Phi(t)\rangle = a|\Uparrow\rangle|\mathcal{E}_{\Uparrow}(t)\rangle + b|\Downarrow\rangle|\mathcal{E}_{\Downarrow}(t)\rangle \ ; \tag{4.9}$$

$$|\mathcal{E}_{\Uparrow}(t)\rangle = \prod_{k=1}^{N}(\alpha_k e^{ig_k t}|\uparrow\rangle_k + \beta_k e^{-ig_k t}|\downarrow\rangle_k) = |\mathcal{E}_{\Downarrow}(-t)\rangle. \qquad 4.10 \tag{21.24}$$

The reduced density matrix is:

$$\begin{aligned} \rho_{\mathcal{A}} &= |a|^2|\Uparrow\rangle\langle\Uparrow| + ab^* r(t)|\Uparrow\rangle\langle\Downarrow| \\ &+ a^* b r^*(t)|\Downarrow\rangle\langle\Uparrow| + |b|^2|\Downarrow\rangle\langle\Downarrow| \ . \qquad 4.11 \end{aligned} \tag{21.25}$$

The coefficient $r(t) = \langle\mathcal{E}_{\Uparrow}|\mathcal{E}_{\Downarrow}\rangle$ determines the relative size of the off-diagonal terms. It is given by:

$$r(t) = \prod_{k=1}^{N}[\cos 2g_k t + i(|\alpha_k|^2 - |\beta_k|^2)\sin 2g_k t] \ . \qquad 4.12 \tag{21.26}$$

For large environments consisting of many (N) spins at large times the off-diagonal terms are typically small:

$$|r(t)|^2 \simeq 2^{-N}\prod_{k=1}^{N}[1 + (|\alpha_k|^2 - |\beta_k|^2)^2] \tag{4.13}$$

The density matrix of any two-state system can be represented by a point in the 3-D space. In terms of the coefficients a, b, and $r(t)$ coordinates of the point representing it are; $z = (|a|^2 - |b|^2)$, $x = \mathrm{Re}(ab^* r)$, $y = \mathrm{Im}(ab^* r)$. When the state is pure, $x^2 + y^2 + z^2 = 1$: Pure states lie on the surface of the Bloch sphere (Fig. 3).

Any conceivable (unitary or non-unitary) quantum evolution can be thought of as a transformation of the surface of the pure states into the ellipsoid contained inside the Bloch sphere. Deformation of the Bloch sphere surface caused by decoherence is a special case of such general evolutions (Zurek, 1982, 1983; Berry, 1995). Decoherence does not affect $|a|$ or $|b|$. Hence, evolution due to decoherence alone occurs in plane z=const. Such a "slice" through the Bloch sphere would show the point representing the state at a fraction $|r(t)|$ of its maximum distance. The complex $r(t)$ can be expressed as the sum of complex phase factors rotating with the frequencies given by differences $\Delta\omega_j$ between the energy eigenvalues of the interaction Hamiltonian, weighted with the probabilities of finding them in the initial state:

$$r(t) = \sum_{j=1}^{2^N} p_j \exp(-i\Delta\omega_j t) \ . \tag{4.14}$$

The index j denotes the environment part of the energy eigenstates of the interaction Hamiltonian, Eq. (4.7): $|j\rangle = |\uparrow\rangle_1 \otimes |\downarrow\rangle_2 \otimes \cdots \otimes |\uparrow\rangle_N$. The corresponding differences between the energies of the eigenstates $|\Uparrow\rangle|j\rangle$ and $|\Downarrow\rangle|j\rangle$ are; $\Delta\omega_j = \langle\Uparrow|\langle j|H_{\mathcal{AE}}|j\rangle|\Downarrow\rangle$. There are 2^N distinct $|j\rangle$'s, and, barring degeneracies, the same number of different $\Delta\omega_j$'s. Probabilities p_j are:

$$p_j = |\langle j|\mathcal{E}(t=0)\rangle|^2 \ , \tag{4.15}$$

which is in turn easily expressed in terms of the appropriate squares of α_k and β_k.

The evolution of $r(t)$, Eq. (4.14), is a consequence of the rotations of the complex vectors $p_k \exp(-i\Delta\omega_j t)$ with different frequencies. The resultant $r(t)$ will then start with the amplitude 1, and quickly "crumble"to

$$\langle |r(t)|^2 \rangle \sim \sum_{j=1}^{2^N} p_j^2 \sim 2^{-N} \ . \tag{4.16}$$

In this sense, decoherence is exponentially effective – the magnitude of the off-diagonal terms decreases exponentially fast with the physical size N of the environment effectively coupled to the state of the system.

We note that the effectiveness of einselection depends on the initial state of the environment: When $\mathcal{E}$ is in the k'th eigenstate of $H_{\mathcal{AE}}$, $p_j = \delta_{jk}$, the coherence in the system will be retained. This special environment state is, however, unlikely in realistic circumstances.

The classical domain and a quantum halo

Geometry of flows induced by decoherence in the Bloch sphere exhibits characteristics encountered in general:

(i) The classical set of the einselected pointer states ($\{|\Uparrow\rangle, |\Downarrow\rangle\}$ in our case). Pointer states are the pure states least affected by decoherence.

(ii) Classical domain consisting of all the pointer states and their mixtures. In Fig. 3 it corresponds to the section [-1,+1] of z-axis.

(iii) The quantum domain – the rest of the volume of the Bloch sphere – consisting of more general density matrices.

Visualizing decoherence-induced decomposition of the Hilbert space may be possible only in the simple case studied here, but whenever decoherence leads to classicality, emergence of generalized and often approximate version of the elements (i) – (iii) is an expected feature.

As a result of decoherence the part of the Hilbert space outside of the classical domain is "ruled out" by einselection. The severity of the prohibition on its states varies. One may measure "non-classicality" of (pure or mixed) states by quantifying their distance from this classical state with the rate of entropy production and comparing it with the much lower rate in the classical domain. Classical pointer states would be then enveloped by a "quantum halo" (Anglin and Zurek, 1996) of nearby, relatively decoherence - resistant but still somewhat quantum states, with a more flagrantly quantum (and more fragile) Schrödinger cat states further away.

By the same token, one can define einselection - induced metric in the classical domain, with the distance between two pointer states given by the rate of entropy production of their superposition. This is not the only way to define a distance: As we shall see in Section VII, redundancy of the record of a state imprinted on the environment is a very natural measure of its classicality. In course of decoherence, pointer states tend to be recorded redundantly and can be deduced by intercepting a very small fraction of the environment (Zurek, 2000; Dalvit, Dziarmaga and Zurek, 2001). One can then define distance using the fraction of the environment that needs to be intercepted to distinguish between two pointer states of the system (Ollivier, Poulin, and Zurek, 2002).

Einselection and controlled shifts

Discussion of decoherence can be generalized to the situation where the system, the apparatus, and the environment have many states, and their interactions are more complicated. Here we assume that the system is isolated, and that it interacts with the apparatus in a `c-shift` manner discussed in Section II. As a result of that interaction the state of the apparatus becomes entangled with the state of the system: $(\sum_i \alpha_i|s_i\rangle)|A_0\rangle \longrightarrow \sum_i \alpha_i|s_i\rangle|A_i\rangle$. This state suffers from the basis ambiguity: The $\mathcal{S}-\mathcal{A}$ entanglement implies that for any state of either there exists a corresponding pure state of its partner. Indeed, when the initial state of $\mathcal{S}$ is chosen to be one of the eigenstates of the conjugate basis:

$$|r_l\rangle = N^{-\frac{1}{2}} \sum_{k=0}^{N-1} \exp(2\pi ikl/N)|s_k\rangle \ , \tag{4.17}$$

`c-shift` could equally well represent a measurement of the apparatus (in the basis conjugate to $\{|A_k\rangle\}$) by the system. Thus, it is not just the basis which is ambiguous: Also the roles of the control (system) and of the target (apparatus) can be reversed when the conjugate basis is selected. These ambiguities can be removed by recognizing the role of the environment.

Figure 4 captures the essence of the idealized decoherence process, that allows the apparatus to be – in spite of the interaction with the environment – a noiseless classical communication channel (Schumacher, 1996; Lloyd, 1997). This is possible because the $\mathcal{A}-\mathcal{E}$ `c-shift`s do not disturb pointer states.

The advantage of this caricature of the decoherence process as a sequence of `c-shift`s lies in its simplicity. However, the actual process of decoherence is usually continuous (so that it can be only approximately broken up into discrete `c-shift`s). Moreover, in contrast to the `c-not`s used in quantum logic circuits, the record inscribed in the environment is usually distributed over many degrees of freedom. Last not least, the observable of the apparatus (or any other open system) may be subject to noise (and not just decoherence) or its self-Hamiltonian may rotate instantaneous pointer states into their superpositions. These very likely complications will be investigated in specific models below.

Decoherence is caused by a premeasurement - like process carried out by the environment

$\mathcal{E}$:

$$|\Psi_{\mathcal{SA}}\rangle|\varepsilon_0\rangle = (\sum_j \alpha_j|s_j\rangle|A_j\rangle)|\varepsilon_0\rangle$$
$$\longrightarrow \sum_j \alpha_j|s_j\rangle|A_j\rangle|\varepsilon_j\rangle \;=\; |\Phi_{\mathcal{SAE}}\rangle \qquad 4.18 \tag{21.27}$$

Decoherence leads to einselection when the states of the environment $|\varepsilon_j\rangle$ corresponding to different pointer states become orthogonal:

$$\langle\varepsilon_i|\varepsilon_j\rangle = \delta_{ij} \tag{4.19}$$

Then the Schmidt decomposition of the state vector $|\Phi_{\mathcal{SAE}}\rangle$ into a composite subsystem $\mathcal{SA}$ and $\mathcal{E}$ yields product states $|s_j\rangle|A_j\rangle$ as partners of the orthogonal environment states. The decohered density matrix describing $\mathcal{SA}$ pair is then diagonal in product states: For simplicity we shall often discard reference to the object that

$$\rho^D_{\mathcal{SA}} \;=\; \sum_j |\alpha_j|^2|s_j\rangle\langle s_j||A_j\rangle\langle A_j|$$
$$\;=\; Tr_{\mathcal{E}}|\Phi_{\mathcal{SAE}}\rangle\langle\Phi_{\mathcal{SAE}}| \; . \qquad 4.20 \tag{21.28}$$

does not interact with the environment (here – the system $\mathcal{S}$). Nevertheless, *preservation of the $\mathcal{SA}$ correlations is the criterion defining the pointer basis.* Invoking it would get rid of many a confusion (see, e.g, discussions in Halliwell, Perez-Mercader, and Zurek, 1994; Venugopalan, 1994). The density matrix of a single object in contact with the environment will be always diagonal in an (instantaneous) Schmidt basis. This instantaneous diagonality should not be used the *sole* criterion for classicality (although see Zeh, 1973, 1990; Albrecht, 1992&1993). Rather, ability of certain states to retain correlations in spite of the coupling to the environment is decisive.

When the interaction with the apparatus has the form:

$$H_{\mathcal{AE}} = \sum_{k,l,m} g^{\mathcal{AE}}_{klm}|A_k\rangle\langle A_k||\varepsilon_l\rangle\langle\varepsilon_m| + h.c. \; , \tag{4.21}$$

the basis $\{|A_k\rangle\}$ is left unperturbed and any correlation with the states $\{|A_k\rangle\}$ is preserved. But, by definition, pointer states preserve correlations in spite of decoherence, so that any observable A co-diagonal with the interaction Hamiltonian will be pointer observable. For, when the interaction is a function of A, it can be expanded in A as a power series, so it commutes with A:

$$[H_{\mathcal{AE}}(A), A] = 0 \tag{4.22}$$

The dependence of the interaction Hamiltonian on the observable is an obvious precondition for the monitoring of that observable by the environment. This admits existence of degenerate pointer eigenspaces of A.

21.4.2 Einselection as the selective loss of information

Establishment of the measurement-like correlation between the apparatus and the environment changes the density matrix from the premeasurement $\rho^P_{\mathcal{SA}}$ to the decohered $\rho^D_{\mathcal{SA}}$, Eq. (4.20). For the initially pure $|\Psi_{\mathcal{SA}}\rangle$, Eq. (4.18), this transition is represented by:

$$\rho^P_{\mathcal{SA}} = \sum_{i,j} \alpha_i\alpha^*_j|s_i\rangle\langle s_j||A_i\rangle\langle A_j| \longrightarrow$$
$$\longrightarrow \sum_i |\alpha_i|^2|s_i\rangle\langle s_i||A_i\rangle\langle A_i| = \rho^D_{\mathcal{SA}} \qquad 4.23 \tag{21.29}$$

Einselection is accompanied by the increase of entropy:

$$\Delta H(\rho_{\mathcal{SA}}) = H(\rho^D_{\mathcal{SA}}) - H(\rho^P_{\mathcal{SA}}) \geq 0 \tag{4.24}$$

and by the disappearance of the ambiguity in what was measured (Zurek, 1981, 1993a). Thus, before decoherence the conditional density matrices of the system $\rho_{\mathcal{S}|C_j\rangle}$ are pure for any state $|C_j\rangle$ of the apparatus pointer. They are defined using the unnormalized:

$$\tilde{\rho}_{\mathcal{S}|\Pi_j} = Tr_{\mathcal{A}}\Pi_j\rho_{\mathcal{SA}} \tag{4.25}$$

where in the simplest case $\Pi_j = |C_j\rangle\langle C_j|$ projects onto a pure state of the apparatus.[6]

Normalized $\rho_{\mathcal{S}|\Pi_j}$ can be obtained by using the probability of the outcome:

$$\rho_{\mathcal{S}|\Pi_j} = p_j^{-1}\tilde{\rho}_{\mathcal{S}|\Pi_j} \ ; \quad p_j = Tr\tilde{\rho}_{\mathcal{S}|\Pi_j} \ . \qquad 4.26 \tag{21.30}$$

Conditional density matrix represents the description of the system $\mathcal{S}$ available to the observer who knows that the apparatus $\mathcal{A}$ is in a subspace defined by Π_j.

Before decoherence, $\rho^P_{\mathcal{S}|C_j\rangle}$ is pure for any state $|C_j\rangle$:

$$(\rho^P_{\mathcal{S}|\Pi_j})^2 \ = \ \rho^P_{\mathcal{S}|\Pi_j} \quad \forall|C_j\rangle \tag{4.27a}$$

providing the initial premeasurement state, Eq. (4.23), was pure as well. It follows that:

$$H(\rho^P_{\mathcal{SA}|C_j\rangle}) = 0 \quad \forall|C_j\rangle \ . \tag{4.28a}$$

For this same case given by the initially pure $\rho^P_{\mathcal{SA}}$ of Eq. (4.23), conditional density matrices obtained from the decohered $\rho^D_{\mathcal{SA}}$ will be pure if and only if they are conditioned upon the pointer states $\{|A_k\rangle\}$;

$$(\rho^D_{\mathcal{S}|C_j\rangle})^2 = \rho^P_{\mathcal{S}|C_j\rangle} = |s_k\rangle\langle s_k| \iff |C_j\rangle = |A_j\rangle; \qquad 4.27\text{b} \tag{21.31}$$

$$H(\rho^D_{\mathcal{S}|A_j\rangle}) = H(\rho^P_{\mathcal{S}|A_j\rangle}) \ . \tag{4.28b}$$

This last equation is valid even when the initial states of the system and of the apparatus are not pure. Thus, only in the pointer basis the pre-decoherence strength of the $\mathcal{SA}$ correlation will be maintained. In all other bases:

$$Tr(\rho^D_{\mathcal{S}|C_j\rangle})^2 \ < \ Tr\rho^D_{\mathcal{S}|C_j\rangle}; \quad |C_j\rangle \notin \{|A_j\rangle\} \tag{4.27c}$$

$$H(\rho^P_{\mathcal{S}|C_j\rangle}) \ < \ H(\rho^D_{\mathcal{S}|C_j\rangle}); \quad |C_j\rangle \notin \{|A_j\rangle\} \tag{4.28c}$$

In particular, in the basis $\{|B_j\rangle\}$ conjugate to the pointer states $\{|A_j\rangle\}$, Eq. (2.14), there is no correlation left with the state of the system, that is:

$$\rho^D_{\mathcal{S}|B_j\rangle} = N^{-1}\sum_k |s_k\rangle\langle s_k| = \mathbf{1}/N \tag{4.29}$$

where $\mathbf{1}$ is a unit density matrix. Consequently;

$$(\rho^D_{\mathcal{S}|B_j\rangle})^2 = \rho_{\mathcal{S}|B_j\rangle}/N, \tag{4.27d}$$

$$H(\rho^D_{\mathcal{S}|B_j\rangle}) = H(\rho^P_{\mathcal{S}|B_j\rangle}) - \lg N = -\lg N \ . \tag{4.28d}$$

Note that, initially, conditional density matrices were pure also in the conjugate (and any other) basis, provided that the initial state was the pure entangled projection operator $\rho^P_{\mathcal{SA}} = |\Psi_{\mathcal{SA}}\rangle\langle\Psi_{\mathcal{SA}}|$, Eq. (4.23).

[6] This can be generalized to projections onto multidimensional subspaces of the apparatus. In that case, purity of the conditional density matrix will be usually lost during the trace over the states of the pointer. This is not surprising: When the observer reads off the pointer of the apparatus only in a coarse-grained manner, he will forgo part of the information about the system. Amplification we have considered before can prevent some of such loss of resolution due to coarse graining in the apparatus. Generalizations to density matrices conditioned upon projection operator valued measures (POVM's) (Kraus, 1983) are also possible.

Mutual information and discord

Selective loss of information everywhere except in the pointer states is the essence of einselection. It is reflected in the change of the mutual information which starts from:

$$\begin{aligned} \mathcal{I}^P(\mathcal{S}:\mathcal{A}) &= H(\rho^P_{\mathcal{S}}) + H(\rho^P_{\mathcal{A}}) - H(\rho^P_{\mathcal{S},\mathcal{A}}) \\ &= -2\sum_i |\alpha_i|^2 \lg |\alpha_i|^2 \qquad 4.30\text{a} \end{aligned} \tag{21.32}$$

As a result of einselection, for initially pure cases, it decreases to at most half its initial value:

$$\begin{aligned} \mathcal{I}^D(\mathcal{S}:\mathcal{A}) &= H(\rho^D_{\mathcal{S}}) + H(\rho^D_{\mathcal{A}}) - H(\rho^D_{\mathcal{S},\mathcal{A}}) \\ &= -\sum_i |\alpha_i|^2 \lg |\alpha_i|^2 \qquad 4.30\text{b} \end{aligned} \tag{21.33}$$

This level is reached when the pointer basis coincides with the Schmidt basis of $|\Psi_{\mathcal{SA}}\rangle$. The decrease in the mutual information is due to the increase of the joint entropy $H(\rho_{\mathcal{S},\mathcal{A}})$:

$$\begin{aligned} \Delta\mathcal{I}(\mathcal{S}:\mathcal{A}) &= \mathcal{I}^P(\mathcal{S}:\mathcal{A}) - \mathcal{I}^D(\mathcal{S}:\mathcal{A}) \\ &= H(\rho^D_{\mathcal{S},\mathcal{A}}) - H(\rho^P_{\mathcal{S},\mathcal{A}}) = \Delta H(\rho_{\mathcal{S},\mathcal{A}}) \qquad 4.31 \end{aligned} \tag{21.34}$$

Classically, equivalent definition of the mutual information obtains from the asymmetric formula:

$$\mathcal{J}_{\mathcal{A}}(\mathcal{S}:\mathcal{A}) = H(\rho_{\mathcal{S}}) - H(\rho_{\mathcal{S}|\mathcal{A}}) \tag{4.32}$$

with the help of the conditional entropy $H(\rho_{\mathcal{S}|\mathcal{A}})$. Above, subscript $\mathcal{A}$ indicates the member of the correlated pair that will be the source of the information about its partner. A symmetric counterpart of the above equation, $\mathcal{J}_{\mathcal{S}}(\mathcal{S}:\mathcal{A}) = H(\rho_{\mathcal{A}}) - H(\rho_{\mathcal{A}|\mathcal{S}})$, can be also written.

In the quantum case, definition of Eq. (4.32) is so far incomplete, as a quantum analogue of the classical conditional information has not been yet specified. Indeed, Eqs. (4.30a) and (4.32) jointly imply that in the case of entanglement a quantum conditional entropy $H(\rho_{\mathcal{S}|\mathcal{A}})$ would have to be negative! For, in this case;

$$H(\rho_{\mathcal{S}|\mathcal{A}}) = \sum_i |\alpha_i|^2 \lg |\alpha_i|^2 < 0 \tag{4.33}$$

would be required to allow for $\mathcal{I}(\mathcal{S}:\mathcal{A}) = \mathcal{J}_{\mathcal{A}}(\mathcal{S}:\mathcal{A})$. Various quantum redefinitions of $\mathcal{I}(\mathcal{S}:\mathcal{A})$ or $H(\rho_{\mathcal{S}|\mathcal{A}})$ have been proposed to address this (Lieb, 1975; Schumacher and Nielsen, 1996; Lloyd, 1997; Cerf and Adami, 1997). We shall simply regard this fact as an illustration of the strength of quantum correlations (i. e., entanglement), which allow $\mathcal{I}(\mathcal{S}:\mathcal{A})$ to violate the inequality:

$$\mathcal{I}(\mathcal{S}:\mathcal{A}) \leq min(H_{\mathcal{S}}, H_{\mathcal{A}}) \tag{4.34}$$

This inequality follows directly from Eq. (4.32) and the non-negativity of classical conditional entropy (see e.g. Cover and Thomas, 1991).

Decoherence decreases $\mathcal{I}(\mathcal{S}:\mathcal{A})$ to this allowed level (Zurek, 1983). Moreover, now the conditional entropy can be defined in the classical pointer basis as the average of partial entropies computed from the conditional $\rho^D_{\mathcal{S}|A_i\rangle}$ over the probabilities of different outcomes:

$$H(\rho_{\mathcal{S}|\mathcal{A}}) = \sum_i p_{|A_i\rangle} H(\rho^D_{\mathcal{S}|A_i\rangle}) \tag{4.35}$$

Prior to decoherence, the use of probabilities would not have been legal.

For the case considered here, Eq. (4.18), the conditional entropy $H(\rho_{\mathcal{S}|\mathcal{A}}) = 0$: In the pointer basis there is a perfect correlation between the system and the apparatus, providing that the premeasurement Schmidt basis and the pointer basis coincide. Indeed, it is tempting to define a good apparatus or a *classical* correlation by insisting on such a coincidence.

The difficulties with conditional entropy and mutual information are highly symptomatic. The trouble with $H(\rho_{\mathcal{S}|\mathcal{A}})$ arises for states that exhibit quantum correlations – entanglement of $|\Psi_{\mathcal{SA}}\rangle$ being an extreme example – and, thus, do not admit an interpretation based on probabilities. A useful sufficient condition for the classicality of correlations is then the existence of an apparatus basis that allows quantum versions of the two classically identical expressions for the mutual information to coincide, $\mathcal{I}(\mathcal{S}:\mathcal{A}) = \mathcal{J}_{\mathcal{A}}(\mathcal{S}:\mathcal{A})$, (Zurek, 2000b; 2002a; Ollivier and Zurek, 2002): Equivalently, the *discord*

$$\delta\mathcal{I}_{\mathcal{A}}(\mathcal{S}|\mathcal{A}) \;=\; \mathcal{I}(\mathcal{S}:\mathcal{A}) - \mathcal{J}_{\mathcal{A}}(\mathcal{S}:\mathcal{A}) \tag{4.36}$$

must vanish: Unless $\delta\mathcal{I}_{\mathcal{A}}(\mathcal{S}|\mathcal{A}) = 0$, probabilities of the distinct apparatus pointer states cannot exist.

We end this subsection with a part summary, part anticipatory remarks: Pointer states retain undiminished correlations with the measured system $\mathcal{S}$, or with any other system, including observers. The loss of information caused by decoherence is given by Eq. (4.31). It was precisely such as to lift conditional information from the paradoxical (negative) values to the classically allowed level, Eq. (4.33). This is equal to the information gained by the observer when he consults the apparatus pointer. This is no coincidence – the environment has 'measured' (became correlated with) the apparatus in the very same pointer basis in which observers have to access $\mathcal{A}$ to take advantage of the remaining (classical) correlation between the pointer and the system. Only when observers and the environment monitor co-diagonal observables they do not get in each others way.

In the idealized case, preferred basis was distinguished by its ability to retain perfect correlations with the system in spite of decoherence. This remark shall serve as a guide in other situations: It will lead to a criterion – predictability sieve – used to identify preferred states in less idealized circumstances. For example, when the self-Hamiltonian of the system is nontrivial, or when the commutation relation, Eq. (4.22), does not hold exactly for any observable, we shall seek states that are best in retaining correlations with the other systems.

21.4.3 Decoherence, entanglement, dephasing, and noise

In the symbolic representation of Fig. 4, noise is the process in which environment acts as a control, inscribing information about its state in the state of the system, that assumes the role of the target. However, the direction of the information flow in `c-nots` and `c-shifts` depends on the choice of initial states. Control and target switch roles when, for a given Hamiltonian of interaction, one prepares input of the `c-not` in the basis conjugate to the logical "pointer" states. Einselected states correspond to the set which – when used in `c-nots` or `c-shifts` – minimizes the effect of interactions directed from the environment to the system.

Einselection is caused by the premeasurement carried out by the environment on the pointer states. Decoherence follows from the Heisenberg's indeterminacy: Pointer observable is measured by the environment. Therefore, the complementary observable must become at least as indeterminate as is demanded by the Heisenberg's principle. As the environment and the systems entangle through an interaction that favors a set of pointer states, their phases become indeterminate (see Eq. (4.29) and discussion of envariance in section VI). Decoherence can be thought of as the resulting loss of phase relations.

Observers can be ignorant of phases for reasons that do not lead to an imprint of the state of the system on the environment. Classical noise can cause such *dephasing* when the observer does

not know the time-dependent classical perturbation Hamiltonian responsible for this unitary, but unknown evolution. For example, in the pre-decoherence state vector, Eq. (4.18), random phase noise will cause a transition:

$$|\Psi_{\mathcal{SA}}\rangle = (\sum_j \alpha_j |s_j\rangle|A_j\rangle)$$
$$\longrightarrow \sum_j \alpha_j \exp\Big(i\phi_j^{(n)}\Big)|s_j\rangle|A_j\rangle \;=\; |\Psi_{\mathcal{SA}}^{(n)}\rangle \;. \qquad 4.37 \tag{21.35}$$

A dephasing Hamiltonian acting either on the system or on the apparatus can lead to such an effect. In this second case its form could be:

$$H_D^{(n)} = \sum_j \dot{\phi}_j^{(n)}(t)|A_j\rangle\langle A_j| \;. \tag{4.38}$$

In contrast to interactions causing premeasurements, entanglement, and decoherence, H_D cannot influence the nature or the degree of the $\mathcal{SA}$ correlations: H_D does not imprint the state of $\mathcal{S}$ or $\mathcal{A}$ anywhere else in the Universe: For each individual realization n of the phase noise (each selection of $\{\phi_j^{(n)}(t)\}$ in Eq. (4.37)) the state $|\Phi_{\mathcal{SA}}^{(n)}\rangle$ remains pure. Given only $\{\phi_j^{(n)}\}$ one could restore pre-dephasing state on a case - by - case basis. However, in absence of such detailed information, one is often forced to represent $\mathcal{SA}$ by the density matrix averaged over the ensemble of noise realizations:

$$\overline{\rho}_{\mathcal{SA}} = \langle|\Psi_{\mathcal{SA}}\rangle\langle\Psi_{\mathcal{SA}}|\rangle = \sum_j |\alpha_j|^2 |s_j\rangle\langle s_j||A_j\rangle\langle A_j|$$
$$+\sum_{j,k}\sum_n e^{i(\phi_j^{(n)}-\phi_k^{(n)})}\alpha_j\alpha_k|s_j\rangle\langle s_k||A_j\rangle\langle A_k| \qquad 4.39 \tag{21.36}$$

In this phase - averaged density matrix off-diagonal terms may disappear. Nevertheless, each member of the ensemble may exist in a state as pure as it was before dephasing. NMR offers examples of dephasing (which can be reversed using spin echo). Dephasing is a loss of phase coherence due to noise in phases. It does not result in an information transfer to the environment.

Dephasing cannot be used to justify existence of preferred basis in individual quantum systems. Nevertheless, the ensemble as a whole may obey the same master equation as individual systems entangling with the environment. Indeed, many of the symptoms of decoherence arise in this setting. Thus, in spite of the light shed on this issue by the discussion of simple cases (Wootters and Zurek, 1979; Stern, Aharonov, and Imry, 1989) more remains to be understood, perhaps by considering implications of envariance (see Section VI).

Noise is an even more familiar and less subtle effect represented by transitions that break one-to-one correspondence in Eq. (4.39). Noise in the apparatus would cause a random rotation of states $|A_j\rangle$. It could be modelled by a collection of Hamiltonians similar to $H_D^{(n)}$ but not co-diagonal with the observable of interest. Then, after an ensemble average similar to Eq. (4.39), one-to-one correspondence between $\mathcal{S}$ and $\mathcal{A}$ would be lost. However – as before – the evolution is unitary for each n, and the unperturbed state could be reconstructed from the information observer could have in advance.

Hence, in case of dephasing or noise information about their cause obtained either in advance, or afterwards, suffices to undo their effect. Decoherence relies on entangling interactions (although, strictly speaking, it need not invlove entanglement (Eisert and Plenio, 2002). Thus, neither prior nor posterior knowledge of the state of environment is enough. Transfer of information about the decohering system to the environment is essential, and plays key role in the interpretation.

We note that, while nomenclature used here seems most sensible to this author and is widely used, it is unfortunately not universal. For example, in the context of quantum computation "decoherence" is sometimes used to describe any process that can cause errors (but see related discussion in Nielsen and Chuang, 2000).

21.4.4 Predictability sieve and einselection

Evolution of a quantum system prepared in a classical state should emulate classical evolution that can be idealized as a "trajectory" – a predictable sequence of objectively existing states. For a purely unitary evolution, all of the states in the Hilbert space retain their purity and are therefore equally predictable. However, in the presence of an interaction with the environment, a generic superposition representing correlated states of the system and of the apparatus will decay into a mixture diagonal in pointer states, Eq. (4.23). Only when the pre-decoherence state of $\mathcal{SA}$ is a product of a single apparatus pointer state $|A_i\rangle$ with the corresponding outcome state of the system (or a mixture of such product states), decoherence has no effect:

$$\rho^P_{\mathcal{SA}} = |s_i\rangle\langle s_i||A_i\rangle\langle A_i| = \rho^D_{\mathcal{SA}} \tag{4.40}$$

A correlation of a pointer state with any state of an isolated system is untouched by the environment. By the same token, when the observer prepares $\mathcal{A}$ in the pointer state $|A_i\rangle$, he can count on it remaining pure. One can even think of $|s_i\rangle$ as the record of the pointer state of $\mathcal{A}$. Einselected states are predictable: they preserve correlations, and hence are effectively classical.

In the above idealized cases predictability of some states follows directly from the structure of the relevant Hamiltonians (Zurek, 1981). Correlation with a subspace associated with a projection operator P_A will be immune to decoherence providing that:

$$[H_{\mathcal{A}} + H_{\mathcal{AE}}, P_A] = 0 \ . \tag{4.41}$$

In more realistic cases it is difficult to demand exact conservation guaranteed by such a commutation condition. Looking for approximate conservation may still be a good strategy. Various densities used in hydrodynamics are one obvious choice (Gell-Mann and Hartle, 1990, 1994).

In general, it is useful to invoke a more fundamental predictability criterion (Zurek, 1993a). One can measure the loss of predictability caused by the evolution for every pure state $|\Psi\rangle$ by von Neumann entropy or some other measure of predictability such as the purity:

$$\varsigma_\Psi(t) = Tr\rho^2_\Psi(t) \ . \tag{4.42}$$

In either case, predictability is a function of time and a functional of the initial state as $\rho_\Psi(0) = |\Psi\rangle\langle\Psi|$. Pointer states are obtained by maximizing predictability functional over $|\Psi\rangle$. When decoherence leads to classicality, good pointer states exist, and the answer is robust.

Predictability sieve sifts all of the Hilbert space, ordering states according to their predictability. The top of the list will be the most classical. This point of view allows for unification of the simple definition of the pointer states in terms of the commutation relation Eq. (4.41), with the more general criteria required to discuss classicality in other situations. The eigenstates of the exact pointer observable are selected by the sieve: Eq. (4.41) guarantees that they will retain their purity in spite of the environment, and are (somewhat trivially) predictable.

Predictability sieve can be generalized to situations where the initial states are mixed (Paraoanu, 2002). Often whole subspaces emerge from the predictability sieve, naturally leading to "decoherence-free subspaces" (see e. g. Lidar et al., 1999) and can be adapted to yield "noiseless subsystems" (which are a non-Abelian generalization of pointer states; see e.g. Zanardi, 2000;

Knill, Laflamme, and Viola, 2000). However, calculations are in general quite difficult even for the initial pure state cases.

The idea of the "sieve" selecting preferred to-be-classical states is novel and only partly explored. We shall see it "in action" below. We have outlined two criteria for sifting through the Hilbert space in search for classicality: von Neumann entropy and purity define, after all, two distinct functionals. Entropy is arguably an obvious information-theoretic measure of predictability loss. Purity is much easier to compute and is often used as a "cheap substitute", and has a physical significance of its own. It seems unlikely that pointer states selected by the predictability and purity sieves could substantially differ. After all, $-Tr\rho\ln\rho = Tr\rho\{(\mathbf{1}-\rho) - (\mathbf{1}-\rho)^2/2 + ...$ so that one can expect the most predictable states to also remain purest (Zurek, 1993a). However, the expansion, Eq. (4.43), is very slowly convergent. Therefore, a more mathematically satisfying treatment of the differences between the states selected by these two criteria would be desirable, especially in cases where (as we shall see in the next section for the harmonic oscillator) preferred states are coherent, and hence the classical domain forms relatively broad "mesa" in the Hilbert space.

The possible discrepancy between the states selected by the sieves based on the predictability and on the purity raises a more general question: Will all the sensible criteria yield identical answer? After all, one can imagine other reasonable criteria for classicality, such as the yet-to-be-explored "distinguishability sieve" of Schumacher (1999) which picks out states whose descendants are most distinguishable in spite of decoherence. Moreover, as we shall see in Section VII (also, Zurek 2000) one can ascribe classicality to states that are most redundantly recorded by the environment. The menu of various classicality criteria already contains several positions, and more may be added in the future. There is no *a priori* reason to expect that *all* of these criteria will lead to *identical* sets of preferred states. It is nevertheless reasonable to hope that, in the macroscopic limit in which classicality is indeed expected, differences between various sieves should be negligible. The same stability in the selection of the classical domain is expected with respect to the changes of, say, the time of the evolution from the initial pure state: Reasonable changes of such details within the time interval where einselection is expected to be effective should lead to more or less similar preferred states, and certainly to preferred states contained within each others "quantum halo" (Anglin and Zurek, 1996). As noted above, this seems to be the case in the examples explored to date. It remains to be seen whether all criteria will agree in other situations of interest.

21.5 Einselection in phase space

Einselection in phase space is a special, yet very important topic. It should lead to phase space points, trajectories, and to classical (Newtonian) dynamics. Special role of position in classical physics can be traced to the nature of interactions (Zurek, 1981; 1982; 1991) that depend on distance, and, therefore, commute with position (see Eq. (4.22)). Evolution of open systems includes, however, the flow in phase space induced by the self-Hamiltonian. Consequently, the set of preferred states turns out to be a compromise, localized in both position and momentum – localized in phase space.

Einselection is responsible for the classical structure of phase space. States selected by the predictability sieve become phase space "points", and their time-ordered sequences are "trajectories". In the underdamped, classically regular systems one can recover this phase space structure along with the (almost) reversible evolution. In chaotic systems there is a price to be paid for classicality: Combination of decoherence with the exponential divergence of classical trajectories (which is the defining feature of chaos) leads to entropy production at a rate given – in the classical limit – by the sum of positive Lyapunov exponents. Thus, the dynamical second law can emerge from the interplay of classical dynamics and quantum decoherence, with

the entropy production caused by the information "leaking" into the environment (Zurek and Paz 1994 & 1995a; Zurek, 1998b; Paz and Zurek 2001).

21.5.1 Quantum Brownian motion

Quantum Brownian motion model consists of an environment $\mathcal{E}$ – a collection of harmonic oscillators (coordinates q_n, masses m_n, frequencies ω_n, and coupling constants c_n) interacting with the system $\mathcal{S}$ (coordinate x), with a mass M and a potential $V(x)$. We shall often consider harmonic $V(x) = M\Omega_0^2 x^2/2$, so that the whole $\mathcal{SE}$ is linear and one can obtain an exact solution. This assumption will be relaxed later.

The Lagrangian of the system-environment entity is:

$$L(x, q_n) = L_{\mathcal{S}}(x) + L_{\mathcal{SE}}(x, \{q_n\}) \; ; \tag{5.1}$$

The system alone has the Lagrangian:

$$L_{\mathcal{S}}(x) = \frac{M}{2}\dot{x}^2 - V(x) \;\; = \;\; \frac{M}{2}(\dot{x}^2 - \Omega_0^2 x^2) \; . \tag{5.2}$$

The effect of the environment is modelled by the sum of the Lagrangians of individual oscillators and of the system-environment interaction terms:

$$L_{\mathcal{SE}} = \sum_n \frac{m_n}{2}\left(\dot{q}_n^2 - \omega_n^2\big(q_n - \frac{c_n x}{m_n\omega_n^2}\big)^2\right) \; . \tag{5.3}$$

This Lagrangian takes into account renormalization of potential energy of the Brownian particle. The interaction depends (linearly) on the position x of the harmonic oscillator. Hence, we expect x to be an instantaneous pointer observable. In combination with the harmonic evolution this leads Gaussian pointer states – well-localized in both x and p. An important characteristic of the model is the spectral density of the environment:

$$C(\omega) \;\; = \;\; \sum_n \frac{c_n^2}{2m_n\omega_n}\delta(\omega - \omega_n) \; . \tag{5.4}$$

The effect of the environment can be expressed through the propagator acting on the reduced $\rho_{\mathcal{S}}$:

$$\rho_{\mathcal{S}}(x, x', t) = \int dx_0 dx_0' J(x, x', t|x_0, x_0', t_0)\rho_{\mathcal{S}}(x_0, x_0', t_0). \tag{5.5}$$

We focus on the case when the system and the environment are initially statistically independent, so that their density matrices in a product state:

$$\rho_{\mathcal{SE}} \;\; = \;\; \rho_{\mathcal{S}}\rho_{\mathcal{E}} \; . \tag{5.6}$$

This is a restrictive assumption. One can try to justify it as an idealization of a measurement that correlates $\mathcal{S}$ with the observer and destroys correlations of $\mathcal{S}$ with $\mathcal{E}$, but that is only an approximation, as realistic measurements leave partial correlations with the environment intact. Fortunately, pre-existing post-measurement correlations lead only to minor differences in the salient features of the subsequent evolution of the system (Romero and Paz, 1997; Anglin, Paz and Zurek, 1997).

Evolution of the whole $\rho_{\mathcal{SE}}$ can be represented as:

$$\rho_{\mathcal{SE}}(x, q, x', q', t) = \int dx_0 dx_0' dq_0 dq_0' \; \rho_{\mathcal{SE}}(x_0, q_0, x_0', q_0', t_0)$$
$$K(x, q, t, x_0, q_0)K^*(x', q', t, x_0', q_0') \qquad 5.7 \tag{21.37}$$

Above, we suppress the sum over the indices of the individual environment oscillators. The evolution operator $K(x,q,t,x_0,q_0)$ can be expressed as a path integral:

$$K(x,q,t,x_0,q_0) = \int DxDq \exp\left(\frac{i}{\hbar} I[x,q]\right) \tag{5.8}$$

where $I[x,q]$ is the action functional that depends on the trajectories $x,\ q$. The integration must satisfy boundary conditions:

$$x(0) = x_0;\ x(t) = x;\ q(0) = q_0;\ q(t) = q\ . \tag{5.9}$$

The expression for the propagator of the density matrix can be now written in terms of actions corresponding to the two Lagrangians, Eqs. (5.1-3):

$$\begin{aligned} J(x,x',t|x_0,x_0',t_0) = \int\ Dx\ Dx' \exp\left\{\frac{i}{\hbar}\right\}(I_{\mathcal{S}}[x] - I_{\mathcal{S}}[x']) \\ \times \int\ dq\ dq_0\ dq_0'\ \rho_{\mathcal{E}}(q_0,q_0') \\ \int\ Dq\ Dq' \exp\left\{\frac{i}{\hbar}\right\}(I_{\mathcal{SE}}[x,q] - I_{\mathcal{SE}}[x',q'])\ . \qquad 5.10 \end{aligned} \tag{21.38}$$

The separability of the initial conditions, Eq. (5.6), was used to make propagator depend only on the initial conditions of the environment. Collecting all terms containing integrals over $\mathcal{E}$ in the above expression leads to the influence functional (Feynman and Vernon, 1963):

$$\begin{aligned} F(x,x') \quad = \int\ dq\ dq_0\ dq_0'\ \rho_{\mathcal{E}}(q_0,q_0') \\ \int\ Dq\ Dq' \exp\left\{\frac{i}{\hbar}\right\}(I_{\mathcal{SE}}[x,q] - I_{\mathcal{SE}}[x',q'])\ . \qquad 5.11 \end{aligned} \tag{21.39}$$

It can be evaluated explicitly for specific models of the initial density matrix of the environment.

Environment in thermal equilibrium provides a useful and tractable model for the initial state. The density matrix of the n'th mode of the thermal environment is:

$$\begin{aligned} \rho_{\mathcal{E}_n}(q,q') \ = \ \frac{m_n\omega_n}{2\pi\hbar\sinh\left(\frac{\hbar\omega_n}{k_BT}\right)} \times \exp -\Big\{\frac{m_n\omega_n}{2\pi\hbar\sinh\left(\frac{\hbar\omega_n}{k_BT}\right)} \\ \times\Big[(q_n^2+q_n'^2)\cosh\left(\frac{\hbar\omega_n}{k_BT}\right) - 2q_nq_n'\Big]\Big\}\ . \qquad 5.12 \end{aligned} \tag{21.40}$$

The influence functional can be written as (Grabert, Schramm, and Ingold, 1988):

$$\begin{aligned} i\ln F(x,x') = \int_0^t ds\ (x-x')(s)\ \int_0^s du \\ \Big(\eta(s-s')(x+x')(s') - i\nu(s-s')(x-x')(s')\Big)\ , \qquad 5.13 \end{aligned} \tag{21.41}$$

where $\nu(s)$ and $\eta(s)$ are dissipation and noise kernels, respectively, defined in terms of the spectral density:

$$\nu(s) = \int_0^\infty d\omega\ C(\omega)\coth(\hbar\omega\beta/2)\cos(\omega s); \tag{5.14}$$

$$\eta(s) = \int_0^\infty d\omega\ C(\omega)\sin(\omega s)\ . \tag{5.15}$$

With the assumption of thermal equilibrium at $k_BT = 1/\beta$, and in the harmonic oscillator case $V(x) = M\Omega_0^2 x^2/2$, the integrand of Eq. (5.10) for the propagator is Gaussian: The integral can be computed exactly, and should also have a Gaussian form. The result can be conveniently written in terms of the diagonal and off-diagonal coordinates of the density matrix in the position representation, $X = x + x'$, $Y = x - x'$:

$$\begin{aligned} J(X,Y,t|X_0,Y_0,t_0) \;&= \\ \frac{b_3}{2\pi}\frac{\exp i(b_1XY + b_2X_0Y - b_3XY_0 - b_4X_0Y_0)}{\exp(a_{11}Y^2 + 2a_{12}YY_0 + a_{22}Y_0^2)}\;. \qquad 5.16 \end{aligned} \tag{21.42}$$

The time-dependent coefficients b_k and a_{ij} are computed from the noise and dissipation kernels, that reflect the properties of the environment. They obtain from the solutions of the equation:

$$\ddot{u}(s) + \Omega_0^2 u(s) + 2\int_0^s ds\eta(s-s')u(s') = 0\;. \tag{5.17}$$

Two such solutions that satisfy boundary conditions $u_1(0) = u_2(t) = 1$ and $u_1(t) = u_2(0) = 0$ can be used for this purpose. They yield the coefficients of the Gaussian propagator through;

$$b_{1(2)}(t) = \dot{u}_{2(1)}(t)/2\;, \quad b_{3(4)}(t) = \dot{u}_{2(1)}(0)/2\;, \tag{5.18a}$$

$$a_{ij}(t) = \frac{1}{1+\delta_{ij}}\int_0^t ds\int_0^t ds' u_i(s)u_j(s')\nu(s-s'). \qquad 5.18\text{b} \tag{21.43}$$

The master equation can be now obtained by taking the time derivative of the Eq. (5.5), which in effect reduces to the computation of the derivative of the propagator, Eq. (5.16) above:

$$\begin{aligned} \dot{J} \;=\; & \{\dot{b}_3/b_3 + i\dot{b}_1XY + i\dot{b}_2X_0Y - i\dot{b}_3XY_0 \\ & -i\dot{b}_4X_0Y_0 - \dot{a}_{11}Y^2 - \dot{a}_{12}YY_0 - \dot{a}_{22}Y_0^2\}J\;. \qquad 5.19 \end{aligned} \tag{21.44}$$

The time derivative of $\rho_{\mathcal{S}}$ can be obtained by multiplying the operator on the right hand side by an initial density matrix and integrating over the initial coordinates X_0, Y_0. Given the form of Eq. (5.19), one may expect that this procedure will yield an integro-differential (non-local in time) evolution operator for $\rho_{\mathcal{S}}$. However, time dependence of the evolution operator disappears as a result of two identities satisfied by the propagator:

$$Y_0J = \Big(\frac{b_1}{b_3}Y + \frac{i}{b_3}\partial_X\Big)J\;, \tag{5.20a}$$

$$\begin{aligned} X_0J = \; & \Big(-\frac{b_1}{b_2}X - \frac{i}{b_2}\partial_Y \\ & -i\big(\frac{2a_{11}}{b_2} + \frac{a_{12}b_1}{b_2b_3}\big)Y + \frac{a_{12}}{b_2b_3}\partial_X\Big)J\;. \qquad 5.20b \end{aligned} \tag{21.45}$$

After the appropriate substitutions, the resulting equation with renormalized Hamiltonian has a form:

$$\begin{aligned} \dot{\rho}_{\mathcal{S}}(x,x',t) \;&=\; -\frac{i}{\hbar}\langle x|[H_{ren}(t),\rho_{\mathcal{S}}]|x'\rangle \\ &-\big(\gamma(t)(x-x')(\partial_x+\partial_{x'}) - D(t)(x-x')^2\big)\rho_{\mathcal{S}}(x,x',t) \\ &-if(t)(x-x')(\partial_x+\partial_{x'})\rho_{\mathcal{S}}(x,x',t). \qquad 5.21 \end{aligned} \tag{21.46}$$

The calculations leading to this master equation are non-trivial. They involve use of relations between the coefficients b_k and a_{ij}. The final result leads to explicit formulae for its coefficients:

$$\Omega_{ren}(t)/2 = b_1\dot{b}_2/b_2 - \dot{b}_1 \ , \tag{5.22a}$$

$$\gamma(t) = -b_1 - \dot{b}_2/2b_2 \ , \tag{5.23a}$$

$$\begin{aligned} D(t) = \quad & \dot{a}_{11} - 4a_{11}b_1 \\ & +\dot{a}_{12}b_1/b_3 - \dot{b}_2(2a_{11} + a_{12}b_1/b_3)/b_2 \ , \qquad 5.24a \end{aligned} \tag{21.47}$$

$$2f(t) = \dot{a}_{12}/b_3 - \dot{b}_2 a_{12}/(b_2 b_3) - 4a_{11} \ . \tag{5.25a}$$

The fact that the exact master equation (5.21) is local in time for an arbitrary spectrum of the environment is remarkable. It was demonstrated by Hu, Paz, and Zhang (1992) following discussions carried out under more restrictive assumptions by Caldeira and Leggett (1983), Haake and Reibold (1985), Grabert, Schramm, and Ingold (1988), and Unruh and Zurek (1989). It depends on the linearity of the problem, that allows one to anticipate (Gaussian) form of the propagator.

The above derivation of the exact master equation used the method of Paz (1994) (see also Paz and Zurek, 2001). Explicit formulae for the time-dependent coefficients can be obtained when one focuses on the perturbative master equation. It can be derived *ab initio* (see Paz and Zurek, 2001) but can be also obtained from the above results by finding a perturbative solution to Eq. (5.17), and then substituting it in Eqs. (5.22*a* - 5.25*a*). The resulting master equation in the operator form is:

$$\begin{aligned} \dot{\rho}_{\mathcal{S}} \ = \quad & -\frac{i}{\hbar}[H_{\mathcal{S}} + M\tilde{\Omega}(t)^2 x^2/2, \rho_{\mathcal{S}}] - \frac{i\gamma(t)}{\hbar}[x, \{p, \rho_{\mathcal{S}}\}] \\ & -D(t)[x,[x,\rho_{\mathcal{S}}]] - \frac{f(t)}{\hbar}[x,[p,\rho_{\mathcal{S}}]] \ . \qquad 5.26 \end{aligned} \tag{21.48}$$

Coefficients such as the frequency renormalization $\tilde{\Omega}$, the relaxation coefficient $\gamma(t)$, and the normal and anomalous diffusion coefficients $D(t)$ and $f(t)$ are given by:

$$\tilde{\Omega}^2(t) = -\frac{2}{M}\int_0^t ds \cos(\Omega s)\eta(s) \tag{5.22b}$$

$$\gamma(t) = \frac{2}{M\Omega}\int_0^t ds \sin(\Omega s)\eta(s) \tag{5.23b}$$

$$D(t) = \frac{1}{\hbar}\int_0^t ds \cos(\Omega s)\nu(s) \tag{5.24b}$$

$$f(t) = -\frac{1}{M\Omega}\int_0^t ds \sin(\Omega s)\eta(s) \tag{5.25b}$$

These coefficient can be made even more explicit when a convenient specific model for the spectral density:

$$C(\omega) = 2M\gamma_0\frac{\omega}{\pi}\frac{\Gamma^2}{\Gamma^2+\omega^2} \tag{5.27}$$

is adopted. Above, γ_0 characterizes the strength of the interaction, and Γ is the high-frequency cutoff. Then:

$$\tilde{\Omega}^2 = -\frac{2\gamma_0\Gamma^3}{\Gamma^2+\Omega^2}\left(1 - \left(\cos\Omega t - \frac{\Omega}{\Gamma}\sin\Omega t\right)e^{-\Gamma t}\right) \ ; \tag{5.22c}$$

$$\gamma(t) = \frac{\gamma_0 \Gamma^2}{\Gamma^2 + \Omega^2}\left(1 - \left(\cos\Omega t - \frac{\Gamma}{\Omega}\sin\Omega t\right)e^{-\Gamma t}\right) . \qquad (5.23c)$$

Note that both of these coefficients are initially zero. They grow to their asymptotic values on a timescale set by the inverse of the cutoff frequency Γ.

The two diffusion coefficients can be also studied, but it is more convenient to evaluate them numerically. In Fig. 5 we show their behavior. The normal diffusion coefficient quickly settles to its long-time asymptotic value:

$$D_\infty = M\gamma_0 \Omega \hbar^{-1} \coth(\hbar\Omega\beta/2)\Gamma^2/(\Gamma^2 + \Omega^2) . \qquad (5.28)$$

The anomalous diffusion coefficient $f(t)$ also approaches asymptotic value. For high temperature it is suppressed by a cutoff Γ with respect to D_∞, but the approach to f_∞ is more gradual, algebraic rather than exponential. Environments with different spectral content exhibit different behavior (Hu, Paz, and Zhang, 1992; Paz, Habib, and Zurek, 1993; Paz, 1994; Anglin, Paz and Zurek, 1997).

21.5.2 Decoherence in quantum Brownian motion

The coefficients of the master equation we have just derived can be computed under a variety of different assumptions. The two obvious characteristics of the environment one can change are its temperature T and its spectral density $C(\omega)$. One general conclusion: In case of high temperatures, $D(t)$ tends to a temperature-dependent constant, and dominates over $f(t)$. Indeed, in this case all of the coefficients settle to asymptotic values after an initial transient. Thus:

$$\begin{aligned} \dot\rho_{\mathcal S} = \quad & -\frac{i}{\hbar}[H_{ren}, \rho_{\mathcal S}] - \gamma(x-x')(\partial_x - \partial_{x'})\rho_{\mathcal S} \\ & -\frac{2M\gamma k_B T}{\hbar^2}(x-x')^2\rho_{\mathcal S} . \qquad 5.29 \end{aligned} \qquad (21.49)$$

This master equation for $\rho(x,x')$ obtains in the unrealistic but convenient limit known as the *high temperature approximation* valid when k_BT is much higher than all the other relevant energy scales, including the energy content of the initial state and the frequency cutoff in $C(\omega)$ (see, e.g, Caldeira and Leggett, 1983). However, when these restrictive conditions hold, Eq. (5.29) can be written for an arbitrary $V(x)$. To see why, we give a derivation patterned on Hu, Paz, and Zhang (1993).

We start with the propagator, Eq. (5.5), $\rho_{\mathcal S}(x,x',t) = J(x,x',t|x_0,x_0',t_0)\rho_{\mathcal S}(x_0,x_0',t_0)$, which we shall treat as if it were an equation for *state vector* of the *two dimensional* system with coordinates x, x'. The propagator is then given by the high-temperature version of Eq. (5.10);

$$\begin{aligned} J(x,x',t|x_0,x_0',t_0) = \int \; & DxDx' \exp\left\{\frac{i}{\hbar}\right\}\Big\{I_R(x) - I_R(x')\Big\} \\ & e^{-M\gamma\left(\int_0^t ds[x\dot x - x'\dot x' + x\dot x' - x'\dot x] + \frac{2k_BT}{\hbar^2}[x-x']^2\right)} . \qquad 5.30 \end{aligned} \qquad (21.50)$$

The term in the exponent can be interpreted as an effective Lagrangian of a two-dimensional system:

$$\begin{aligned} L_{eff}(x,x') = & M\dot x^2/2 - V_R(x) - M\dot x'^2/2 + V_R(x') \\ & +\gamma(x-x')(\dot x + \dot x') + i\frac{2M\gamma k_BT}{\hbar^2}(x-x')^2 . \qquad 5.31 \end{aligned} \qquad (21.51)$$

One can readily obtain the corresponding Hamiltonian;

$$H_{eff} \;=\; \dot{x}\partial L_{eff}/\partial\dot{x} + \;\dot{x}'\partial L_{eff}/\partial\dot{x}' - L_{eff}\;. \tag{5.32}$$

Conjugate momenta $p = p_x = M\dot{x} + \gamma(x - x')$ and $p' = p_{x'} = -M\dot{x}' + \gamma(x - x')$ are used to express the kinetic term of H_{eff}. After evaluating $\dot{x}$ and $\dot{x}'$ in terms of p and p' in the expression for H_{eff} one obtains:

$$\begin{aligned} H_{eff} = \quad & \big(p - \gamma(x - x')\big)^2/2M - \big(p' - \gamma(x - x')\big)^2/2M \\ & + V(x) - V(x') - i2M\gamma k_B T(x' - x)^2/\hbar^2\;. \qquad 5.33 \end{aligned} \tag{21.52}$$

This expression yields the operator that generates the evolution of the density matrix, Eq. (5.29).

The coefficients of Eq. (5.21) approach their high-temperature values quickly (see Fig. 5). Already for T well below what the rigorous derivation would demand high-temperature limit appears to be an excellent approximation. The discrepancy – manifested by symptoms such as some of the diagonal terms of $\rho_{\mathcal{S}}(x', x)$ assuming negative values when the evolutions starts from an initial state that is so sharply localized in position to have kinetic energy in excess of the values allowed by the high-temperature approximation – is limited to the initial instant of order $1/\Gamma$, and is known to be essentially unphysical for other reasons (Unruh and Zurek, 1989; Ambegoakar, 1991; Romero and Paz, 1997; Anglin, Paz, and Zurek, 1997). This short - time anomaly is closely tied to the fact that Eq. (5.33) (and, indeed, many of the exact or approximate master equations derived to date) does not have the Lindblad form (Lindblad, 1976; see also Gorini, Kossakowski and Sudarshan, 1976, Alicki and Lendi, 1987) of a dynamical semigroup.

High temperature master equation (5.29) is a good approximation in a wider range of circumstances than the one for which it was derived (Feynman and Vernon, 1963; Dekker, 1977; Caldeira and Leggett, 1983). Moreover, our key qualitative conclusion – rapid decoherence in the macroscopic limit – does not crucially depend on the approximations leading to Eq. (5.29). We shall therefore use it in our further studies.

Decoherence timescale

In the macroscopic limit (that is, when $\hbar$ is small compared to other quantities with dimensions of action, such as $\sqrt{2Mk_BT\langle(x - x')^2\rangle}$ in the last term) the high-temperature master equation is dominated by:

$$\partial_t\rho_{\mathcal{S}}(x, x', t) = -\gamma\Big\{\frac{(x - x')}{\lambda_T}\Big\}^2\rho_{\mathcal{S}}(x, x', t)\;. \tag{5.34}$$

Above;

$$\lambda_T \;=\; \frac{\hbar}{\sqrt{2Mk_BT}} \tag{5.35}$$

is thermal de Broglie wavelength. Thus, the density matrix looses off-diagonal terms in position representation:

$$\rho_{\mathcal{S}}(x, x', t) \;=\; \rho_{\mathcal{S}}(x, x', 0)e^{-\gamma t(\frac{x-x'}{\lambda_T})^2}\;. \tag{5.36}$$

while the diagonal ($x = x'$) remains untouched.

Quantum coherence decays exponentially at the rate given by the relaxation rate times the square of the distance measured in units of thermal de Broglie wavelength (Zurek, 1984a). Position is the "instantaneous pointer observable": If Eq. (5.36) was always valid, eigenstates of position would attain the classical status.

The importance of position can be traced to the nature of the interaction Hamiltonian between the system and the environment. According to Eq. (5.3):

$$H_{\mathcal{SE}} \ = \ x \sum_n c_n q_n \ . \tag{5.37}$$

This form of $H_{\mathcal{SE}}$ is motivated by physics (Zurek, 1982; 1991): Interactions depend on the distance. However, had we endeavored to find a situation where a different form of the interaction Hamiltonian – say, a momentum-dependent interaction – was justified, the form and consequently predictions of the master equation would have been analogous to Eq. (5.36), but with a substitution of the relevant observable "monitored" by the environment for x. Such situations may be experimentally accessible (Poyatos, Cirac, and Zoller, 1996) providing a test of one of the key ideas of einselection: the relation between the form of interaction and the preferred basis.

The effect of the evolution, Eqs. (5.34) - (5.36), on the density matrix in the position representation is easy to envisage. Consider a superposition of two minimum uncertainty Gaussians. Off-diagonal peaks represent coherence. They decay on a *decoherence timescale* τ_D, or with a *decoherence rate* (Zurek, 1984a, 1991);

$${\tau_D}^{-1} \ = \ \gamma(\frac{x-x'}{\lambda_T})^2 \ . \tag{5.38}$$

Thermal de Broglie wavelength, λ_T, is microscopic for massive bodies and for the environments at reasonable temperatures. For a mass 1g at room temperature and for the separation $x' - x$ =1cm, Eq. (5.38) predicts decoherence approximately 10^{40} times faster than relaxation! Even cosmic microwave background suffices to cause rapid loss of quantum coherence in objects as small as dust grains (Joos and Zeh, 1985). These estimates for the rates of decoherence and relaxation should be taken with a grain of salt: Often the assumptions that have led to the simple high temperature master equation (5.29) are not valid (Gallis & Fleming, 1990; Gallis, 1992; Anglin, Paz & Zurek, 1997). For example, the decoherence rate cannot be faster than inverse of the spectral cutoff in Eq. (5.27), or than the rate with which the superposition is created. Moreover, for large separations quadratic dependence of decoherence rate may saturate (Gallis and Fleming, 1990; Anglin, Paz, and Zurek, 1997) as seen in the "simulated decoherence" experiments of Cheng and Raymer (1999). Nevertheless, in the macroscopic domain decoherence of widely delocalized "Schrödinger cat" states will occur very much faster than relaxation, which proceeds at the rate given by γ.

Phase space view of decoherence

A useful alternative way of illustrating decoherence is afforded by the Wigner function representation:

$$W(x,p) = \frac{1}{2\pi\hbar}\int_{-\infty}^{+\infty} dy \ e^{(ipy/\hbar)}\rho(x+\frac{y}{2}, x-\frac{y}{2}) \ . \qquad 5.39 \tag{21.53}$$

Evolution equation followed by the Wigner function obtains through the Wigner transform of the corresponding master equation. In the high temperature limit, Eq. (5.29) (valid for general potentials) this yields:

$$\partial_t W = \{H_{ren}, W\}_{MB} + 2\gamma\partial_p(pW) + D\partial_{pp}W \ . \tag{5.40}$$

The first term – Moyal bracket – is the Wigner transform of the von Neumann equation (see Section III). In the linear case it reduces to the Poisson bracket. The second term is responsible for relaxation. The last diffusive term is responsible for decoherence.

Diffusion in momentum occurs at the rate set by $D = 2M\gamma k_B T$. Its origin can be traced to the continuous "measurement" of the position of the system by the environment: In accord with the Heisenberg indeterminacy, measurement of position results in the increase of the uncertainty in momentum (see Section IV).

Decoherence in phase space can be explained on the example of a superposition of two Gaussian wavepackets. Wigner function in this case is given by:

$$W(x,p) = G(x+x_0,p) \ + \ G(x-x_0,p)$$
$$+(\pi\hbar)^{-1}\exp\bigl(-p^2\xi^2/\hbar^2 - x^2/\xi^2\bigr)\cos(\Delta x p/\hbar) \ , \qquad 5.41 \tag{21.54}$$

where;

$$G(x\pm x_0, p-p_0) = \frac{e^{-(x\mp x_0)^2/\xi^2-(p-p_0)^2\xi^2/\hbar^2}}{\pi\hbar} \ . \qquad 5.42 \tag{21.55}$$

We have assumed the Gaussians are not moving ($p_0 = 0$).

The oscillatory term in Eq. (5.41) is the signature of superposition. The frequency of the oscillations is proportional to the distance between the peaks. When the separation is only in position x, this frequency is:

$$f = \Delta x/\hbar = 2x_0/\hbar \ . \tag{5.43}$$

Ridges and valleys of the interference pattern are parallel to the separation between the two peaks. This, and the fact that $\hbar$ appears in the interference term in W is important for phase space derivation of the decoherence time. We focus on the dominant effect and direct our attention on the last term of Eq. (5.40). Its effect on the rapidly oscillating interference term will be very different from its effect on the two Gaussians: The interference term is dominated by the cosine:

$$W_{int} \sim \cos\left(\frac{\Delta x}{\hbar}p\right) \ . \tag{5.44}$$

This is an eigenfunction of the diffusion operator. Decoherence timescale emerges (Zurek, 1991) from the corresponding eigenvalue;

$$\dot{W}_{int} \approx -\{D\Delta x^2/\hbar^2\} \times W_{int} \ . \tag{5.45}$$

We have recovered the formula for τ_D, Eq. (5.38), from a different looking argument: Eq. (5.40) has no explicit dependence on $\hbar$ for linear potentials (in the nonlinear case $\hbar$ enters through the Moyal bracket). Yet, the decoherence timescale contains $\hbar$ explicitly – $\hbar$ enters through Eq. (5.43), that is through its role in determining the frequency of the interference pattern W_{int}.

The evolution of the pure initial state of the type considered here is shown in Fig. 6. There we illustrate evolution of the Wigner function for two initial pure states: Superposition of two positions and superposition of two momenta. There is a noticeable difference in the rate at which the interference term disappears between these two cases. This was anticipated. The interaction in Eq. (5.3) is a function of x. Therefore, x is monitored by the environment directly, and the superposition of positions decoheres almost instantly. By contrast, the superposition of momenta is initially insensitive to the monitoring by the environment – the corresponding initial state is already well localized in the observable singled out by the interaction. However, a superposition of momenta leads to a superposition of positions, and hence to decoherence, albeit on a dynamical (rather than τ_D) timescale.

An intriguing example of a long-lived superposition of two seemingly distant Gaussians was pointed out by Braun, Braun and Haake (2000) in the context of superradiance. As they note, the relevant decohering interaction cannot distinguish between some such superpositions, leading to a 'Schrödinger cat' pointer subspace.

21.5.3 Predictability sieve in phase space

Decoherence rapidly destroys non-local superpositions. Obviously, states that survive must be localized. However, they cannot be localized to a point in x, as this would imply – by Heisenberg's indeterminacy – an infinite range in momenta, and, hence, of velocities. As a result, a wave function localized too well at one instant would become very non-local a moment later.

Einselected pointer states minimize the damage done by decoherence over the "timescale of interest" (usually associated with predictability or with dynamics). They can be found through the application of the predictability sieve outlined at the end of Section IV. To implement it, we compute entropy increase or purity loss for all initially pure states in the Hilbert space of the system under the cumulative evolution caused by the self-Hamiltonian and by the interaction with the environment. It would be a tall order to carry out the requisite calculations for an arbitrary quantum system interacting with a general environment. We focus on the exactly solvable case.

In the high temperature limit the master equations (5.26) and (5.29) can be expressed in the operator form:

$$\dot{\rho} = \frac{1}{i\hbar}[H_{ren},\rho] + \frac{\gamma}{i\hbar}[\{p,x\},\rho] - \frac{\eta k_B T}{\hbar^2}[x,[x,\rho]] - \frac{i\gamma}{\hbar}\big([x,\rho p]-[p,\rho x]\big) \qquad 5.46 \tag{21.56}$$

Above, $\eta = 2M\gamma$ is the viscosity. Only the last two terms can change entropy. Terms of the form:

$$\dot{\rho} = [\hat{O},\rho] \tag{5.47}$$

where $\hat{O}$ is Hermitean leave the purity $\varsigma = Tr\rho^2$ and the von Neumann entropy $H = -Tr\rho\lg\rho$ unaffected. This follows from the cyclic property of the trace:

$$\frac{d}{dt}Tr\rho^N = \sum_{k=1}^{N}(Tr\rho^{k-1}[\hat{O}\rho]\rho^{N-k}) = 0 \tag{5.48}$$

Constancy of $Tr\rho^2$ is obvious, while for $Tr\rho\lg\rho$ it follows when the logarithm is expanded in powers of ρ.

Equation (5.46) leads to the loss of purity at the rate (Zurek, 1993a):

$$\frac{d}{dt}Tr\rho^2 = -\frac{4\eta k_B T}{\hbar^2}Tr\big(\rho^2x^2-(\rho x)^2\big) + 2\gamma Tr\rho^2 \tag{5.49}$$

The second term increases purity – decreases entropy – as the system is damped from an initial highly mixed state. For predictability sieve this term is usually unimportant, as for a vast majority of the initially pure states its effect will be negligible when compared to the first, decoherence - related term. Thus, in the case of pure initial states:

$$\frac{d}{dt}Tr\rho^2 = -\frac{4\eta k_B T}{\hbar^2}(\langle x^2\rangle - \langle x\rangle^2), \tag{5.50}$$

Therefore, the instantaneous loss of purity is minimized for perfectly localized states (Zurek, 1993a). The second term of Eq. (5.49) allows for the equilibrium. (Nevertheless, early on, and for very localized states, its presence causes an (unphysical) *increase* of purity to *above* unity. This is a well-known artifact of the high-temperature approximation (see discussion following Eq. (5.33)).

To find most predictable states relevant for dynamics consider entropy increase over a period of the oscillator. For a harmonic oscillator with mass M and frequency Ω, one can compute purity loss averaged over $\tau = 2\pi/\Omega$:

$$\Delta\varsigma|_0^{2\pi/\Omega} = -2D\big(\Delta x^2 + \Delta p^2/(M\Omega)^2\big) \ . \tag{5.51}$$

Above, Δx and Δp are dispersions of the state at the initial time. By the Heisenberg indeterminacy, $\Delta x \Delta p \geq \hbar/2$. The loss of purity will be smallest when:

$$\Delta x^2 = \hbar/2M\Omega, \ \Delta p^2 = \hbar M\Omega/2 \ . \tag{5.52}$$

Coherent quantum states are selected by the predictability sieve in an underdamped harmonic oscillator (Zurek, 1993a; Zurek, Habib and Paz, 1993; Gallis, 1996; Tegmark and Shapiro, 1994; Wiseman and Vaccaro, 1998; Paraoanu, 2002). Rotation induced by the self-Hamiltonian turns preference for states localized in position into preference for localization in phase space. This is illustrated in Fig. 7.

We conclude that for an underdamped harmonic oscillator coherent Gaussians are the best quantum theory has to offer as an approximation to a classical point. Similar localization in phase space should obtain in the reversible classical limit in which the familiar symptoms of the "openness" of the system – such as the finite relaxation rate $\gamma = \eta/2M$ – become vanishingly small. This limit can be attained for large mass $M \longrightarrow \infty$, while the viscosity η remains fixed and sufficiently large to assure localization (Zurek, 1991; 1993a). This is, of course, not the only possible situation. Haake and Walls (1987) discussed the overdamped case, where pointer states are still localized, but relatively more narrow in position. On the other hand, "adiabatic" environment enforces einselection in energy eigenstates (Paz and Zurek, 1999).

21.5.4 Classical limit in phase space

There are three strategies that allow one to simultaneously recover both the classical phase space structure and the classical equations of motion.

Mathematical approach ($\hbar \to 0$)

This "mathematical" classical limit could not be implemented without decoherence, since the oscillatory terms associated with interference do not have an analytic $\hbar \to 0$ limit (see, e.g, Peres, 1993). However, in the presence of the environment, the relevant terms in the master equations increase as $\mathcal{O}(\hbar^{-2})$, and make the non-analytic manifestations of interference disappear. Thus, phase space distributions can be always represented by localized coherent state "points", or by the distributions over the basis consisting of such points.

This strategy is easiest to implement starting from the phase-space formulation. It follows from Eq. (5.45) that the interference term in Eq. (5.41) will decay (Paz, Habib, and Zurek, 1993) over the time interval Δt as:

$$W_{int} \sim \exp\big(-\Delta t \frac{D\Delta x^2}{\hbar^2}\big) \cos\big(\frac{\Delta x}{\hbar} p\big) \ . \tag{5.53}$$

As long as Δt is large compared to decoherence timescale $\tau_D \simeq \hbar^2/D\Delta x^2$, the oscillatory contributions to the Wigner function $W(x,p)$ shall disappear with $\hbar \to 0$. Simultaneously, Gaussians representing likely locations of the system become narrower, approaching δ-functions in phase space. For instance, in Eq. (5.42);

$$\lim_{\hbar\to 0} G(x - x_0, p - p_0) \ = \ \delta(x - x_0, p - p_0) \ , \tag{5.54}$$

providing half-widths of the coherent states in x and p decrease to zero as $\hbar \to 0$. This would be assured when, for instance, in Eqs. (5.41)-(5.42):

$$\xi^2 \sim \hbar \ . \tag{5.55}$$

Thus, individual coherent-state Gaussians approach phase space points. This behavior indicates that in a macroscopic open system nothing but probability distributions over localized phase space points can survive in the $\hbar \to 0$ limit for any time of dynamical or predictive significance. (Coherence between immediately adjacent points separated only by $\sim \xi$, Eq. (5.55), can last longer. This is no threat to the classical limit. Small scale coherence is a part of a "quantum halo" of the classical pointer states (Anglin and Zurek, 1996).)

The *mathematical classical limit* implemented by letting $\hbar \to 0$ becomes possible in presence of decoherence. It is tempting to take this strategy to its logical conclusion, and represent every probability density in phase space in the point(er) basis of narrowing coherent states. Such a program is beyond the scope of this review, but the reader should be by now convinced that it is possible. Indeed, Perelomov (1986) shows that a general quantum state can be represented in a sparse basis of coherent states that occupy sites of a regular lattice, providing that the volume per coherent state "point" is no more than $(2\pi\hbar)^d$ in the $d-$dimensional configuration space. In presence of decoherence arising from the coordinate-dependent interaction, evolution of a general quantum superposition should be – after a few decoherence times – well approximated by the probability distribution over such Gaussian "points".

Physical approach: The macroscopic limit

The possibility of the $\hbar \to 0$ classical limit in presence of decoherence is of interest. But $\hbar = 1.05459 \times 10^{-27}$erg s. Therefore, a physically more reasonable approach increases the size of the object, and, hence, its susceptibility to decoherence. This strategy can be implemented starting with Eq. (5.40). Reversible dynamics obtains as $\gamma \to 0$ while $D = 2M\gamma k_B T = \eta k_B T$ increases.

The decrease of γ and the simultaneous increase of $\eta k_B T$ can be anticipated with the increase of the size and mass. Assume that density of the object is independent of its size R, and that the environment quanta scatter from its surface (as would photons or air molecules). Then $M \sim R^3$ and $\eta \sim R^2$. Hence:

$$\eta \sim \mathcal{O}(R^2) \longrightarrow \infty \ , \tag{5.56}$$

$$\gamma = \eta/2M \sim \mathcal{O}(1/R) \longrightarrow 0 \ , \tag{5.57}$$

as $R \to \infty$: Localization in phase space and reversibility can be simultaneously achieved in a macroscopic limit.

Existence of macroscopic classical limit in simple cases has been pointed out some time ago (Zurek 1984a, 1991; Gell-Mann and Hartle, 1993). We shall analyze it in the next section in a more complicated chaotic setting, where reversibility can no longer be taken for granted. In the harmonic oscillator case approximate reversibility is effectively guaranteed, as the action associated with the 1-σ contour of the Gaussian state increases with time at the rate (Zurek, Habib, and Paz, 1993):

$$\dot{I} = \gamma \frac{k_B T}{\hbar \Omega} \tag{5.58}$$

Action I is a measure of the lack of information about phase space location. Hence, its rate of increase is a measure of the rate of predictability loss. Trajectory is a limit of the "tube" swept in phase space by the moving volume representing instantaneous uncertainty of the observer about the state of the system. Evolution is approximately deterministic when the area of this

contour is nearly constant. In accord with Eqs. (5.56)-(5.57) $\dot{I}$ tends to zero in the reversible macroscopic limit:

$$\dot{I} \sim \mathcal{O}(1/R) \tag{5.59}$$

The existence of an approximately reversible trajectory-like thin tubes provides an assurance that, having localized the system within a regular phase space volume at $t = 0$, we can expect that it can be found later inside the Liouville - transported contour of nearly the same measure. Similar conclusions follow for integrable systems.

Ignorance inspires confidence in classicality

Dynamical reversibility can be achieved with einselection in the macroscopic limit. Moreover, $\dot{I}/I$ or other measures of predictability loss decrease with the increase of I. This is especially dramatic when quantified in terms of the von Neumann entropy, that, for Gaussian states, increases at the rate (Zurek, Habib and Paz, 1993):

$$\dot{H} = \dot{I} \lg \frac{I+1}{I-1} \tag{5.60a}$$

The resulting $\dot{H}$ is infinite for pure coherent states ($I = 1$), but quickly decreases with increasing I. Similarly, the rate of purity loss for Gaussians is:

$$\dot{\varsigma} = \dot{I}/I^2 \ . \tag{5.60b}$$

Again, it tapers off for more mixed states.

This behavior is reassuring. It leads us to conclude that irreversibility quantified through, say, von Neumann entropy production, Eq. (5.60a), will approach $\dot{H} \approx 2\dot{I}/I$, vanishing in the limit of large I. When in the spirit of the macroscopic limit we do not insist on the maximal resolution allowed by the quantum indeterminacy, the subsequent predictability losses measured by the increase of entropy or through the loss of purity will diminish. Illusions of reversibility, determinism, and exact classical predictability become easier to maintain in presence of ignorance about the initial state!

To think about phase space points one may not even need to invoke a specific quantum state. Rather, a point can be regarded as a limit of an abstract recursive procedure, in which phase space coordinates of the system are determined better and better in a succession of increasingly accurate measurements. One may be tempted to extrapolate this limiting process *ad infintessimum* which would lead beyond Heisenberg's indeterminacy principle and to a false conclusion that idealized points and trajectories "exist objectively", and that the insider view of Section II can be always justified. While in our quantum Universe this conclusion is wrong, and the extrapolation described above illegal, the presence, within the Hilbert space, of localized wavepackets near the minimum uncertainty end of such imagined sequences of measurements is reassuring. Ultimately, the ability to represent motion in terms of points and their time - ordered sequences (trajectories) is the essence of classical mechanics.

21.5.5 Decoherence, chaos, and the Second Law

Breakdown of correspondence in this chaotic setting was described in section III. It is anticipated to occur in all non-linear systems, as the stretching of the wavepacket by the dynamics is a generic feature, absent only in a harmonic oscillator. However, exponential instability of chaotic dynamics implies rapid loss of quantum - classical correspondence after the Ehrenfest time, $t_\hbar = \Lambda^{-1} \ln \chi \Delta p/\hbar$. Here Λ is the Lyapunov exponent, $\chi = \sqrt{V_x/V_{xxx}}$ typically characterizes the dominant scale of nonlinearities in the potential $V(x)$, and Δp gives the coherence scale in the initial wavepacket. The above estimate, Eq. (3.5) depends on the initial conditions.

It is smaller than, but typically close to, $t_r = \Lambda^{-1} \ln I/\hbar$, Eq. (3.6), where I is the characteristic action of the system. By contrast, phase space patches of regular systems undergo stretching with a power of time. Consequently, loss of correspondence occurs only over a much longer $t_r \sim (I/\hbar)^\alpha$, that depends polynomially on $\hbar$.

Restoration of correspondence

Exponential instability spreads the wavepacket to a "paradoxical" extent at the rate given by the positive Lyapunov exponents $\Lambda_+^{(i)}$. Einselection attempts to enforce localization in phase space by tapering off interference terms at the rate given by the inverse of the decoherence timescale $\tau_D = \gamma^{-1}(\lambda_T/\Delta x)^2$. The two processes reach *status quo* when the coherence length ℓ_c of the wavepacket makes their rates comparable, that is:

$$\tau_D \Lambda_+ \simeq 1 \tag{5.61}$$

This yields an equation for the steady-state coherence length and for the corresponding momentum dispersion:

$$\ell_c \simeq \lambda_T \sqrt{\Lambda_+/2\gamma}\ ; \tag{5.62}$$

$$\sigma_c = \hbar/\ell_c = \sqrt{2D/\Lambda_+}\ . \tag{5.63}$$

Above, we have quoted results (Zurek and Paz, 1994) that follow from a more rigorous derivation of the coherence length ℓ_c than the "rough and ready" approach that led to Eq. (5.61). They embody the same physical argument, but seek asymptotic behavior of the Wigner function that evolves according to the equation:

$$\begin{aligned} \dot{W} = \quad & \{H, W\} + \sum_{n\geq 1} \frac{\hbar^{2n}(-)^n}{2^{2n}(2n+1)!} \partial_x^{2n+1} V \partial_p^{2n+1} W \\ & + D\partial_p^2 W\ . \qquad 5.64 \end{aligned} \tag{21.57}$$

The classical Liouville evolution generated by Poisson bracket ceases to be a good approximation of the decohering quantum evolution when the leading quantum correction becomes comparable to the classical force:

$$\frac{\hbar^2}{24} V_{xxx} W_{ppp} \approx \frac{\hbar^2}{24} \frac{V_x}{\chi^2} \frac{W_p}{\sigma_c^2} \tag{5.65}$$

The term $\partial_x V \partial_p W$ represents the classical force in Poisson bracket. Quantum corrections are small when;

$$\sigma_c \chi \gg \hbar \tag{5.66}$$

Equivalently, Moyal bracket generates approximately Liouville flow when the coherence length satisfies:

$$\ell_c \ll \chi \tag{5.67}$$

This last inequality has an obvious interpretation: It is a demand for the localization to within a region ℓ_c small compared to the scale χ of the nonlinearities of the potential. When this condition holds, classical force will dominate over quantum corrections.

Restoration of correspondence is illustrated in Fig. 8 where Wigner functions are compared with classical probability distributions in a chaotic system. The difference between the classical and quantum expectation values in same chaotic system is shown in Fig. 9. Even relatively weak decoherence suppresses the discrepancy, helping reestablish the correspondence: $D = 0.025$ translates through Eq. (5.62) into coherence over $\ell_c \simeq 0.3$, not much smaller than the nonlinearity scale $\chi \simeq 1$ for the investigated Hamiltonian of Fig. 8.

Entropy production

Irreversibility is the price for the restoration of quantum-classical correspondence in chaotic dynamics. It can be quantified through the entropy production rate. The simplest argument recognizes that decoherence restricts spatial coherence to ℓ_c. Consequently, as the exponential instability stretches the size $L^{(i)}$ of the distribution in directions corresponding to the positive Lyapunov exponents $\Lambda_+^{(i)}$, $L^{(i)} \sim \exp\left(\Lambda_+^{(i)} t\right)$ the squeezing mandated by the Liouville theorem in the complementary directions corresponding to $\Lambda_-^{(i)}$ will halt at $\sigma_c^{(i)}$, Eq. (5.63). In this limit, the number of pure states needed to represent resulting mixture increases exponentially

$$N^{(i)} \simeq L^{(i)}/\ell_c^{(i)} \tag{5.68}$$

in each dimension. The least number of pure states overlapped by W will be then $\mathcal{N} = \Pi_i N^{(i)}$. This implies:

$$\dot{H} \simeq \partial_t \ln \mathcal{N} \simeq \sum_i \Lambda_+^{(i)} \ . \tag{5.69}$$

This estimate for entropy production rate becomes accurate as the width of the Wigner function reaches saturation at $\sigma_c^{(i)}$. When a patch in phase space corresponding to the initial W is regular and smooth on scales large compared to $\sigma_c^{(i)}$, evolution will start nearly reversibly (Zurek and Paz, 1994). However, as squeezing brings the extent of the effective support of W close to $\sigma_c^{(i)}$, diffusion bounds from below the size of the smallest features of W. Stretching in the unstable directions continues unabated. As a consequence, the volume of the support of W will grow exponentially, resulting in an entropy production rate set by Eq. (5.69), the sum of the classical Lyapunov exponents. Yet, it has an obviously quantum origin in decoherence. This quantum origin may be apparent initially, as the rate of Eq. (5.69) will be approached from above when the initial state is a non-local. On the other hand, in a multidimensional system different Lyapunov exponents may begin to contribute to entropy production at different instants (as the saturation condition, Eq. (5.61), may not be met simultaneously for all $\Lambda_+^{(i)}$). Then the entropy production rate can accelerate (before subsiding as a consequence of approaching equilibrium).

The timescales on which this estimates of entropy production apply are still subject to investigation (Zurek and Paz, 1995a; Zurek, 1998b; Monteoliva and Paz 2000 & 2001) and even controversy (Casati and Chirikov, 1995b; Zurek and Paz, 1995b). The instant when Eq. (5.69) becomes a good approximation corresponds to the moment when the exponentially unstable evolution forces the Wigner function to develop small phase space structures on the scale of the effective decoherence - imposed "coarse graining", Eq. (5.63). This will be a good approximation until the time t_{EQ} at which equilibrium sets in. Both $t_\hbar$ have a logarithmic dependence on the corresponding (initial and equilibrium) phase space volumes I_0 and I_{EQ}, so the validity of Eq. (5.69) will be limited to $t_{EQ} - t_\hbar \simeq \Lambda^{-1} \ln I_{EQ}/I_0$.

There is a simple and conceptually appealing way to extend the interval over which entropy is produced at the rate given by Eq. (5.69): Imagine an observer monitoring a decohering chaotic system, finding out its state at time intervals small compared to Λ^{-1}, but large compared to the decoherence timescale. One can show (Zurek, 1998b) that the average increase of the size of the algorithmically compressed records of measurement of a decohering chaotic system (that is, the algorithmic randomness of the acquired data, see e.g. Cover and Thomas, 1991) is given – after conversion into bits from "nats" – by Eq. (5.69). This conclusion holds providing that the effect of the "collapses of the wavepacket" caused by the repeated measurements is negligible – i.e., the observer is "skillful". A possible strategy a skillful observer may adopt is that of indirect measurements, of monitoring a fraction of the environment responsible for decoherence to find out the state of the system. As we shall see in more detail in the following sections of the paper, this is a very natural strategy, often employed by the observers.

A classical analogue of Eq. (5.69) has been obtained by Kolmogorov (1960) and Sinai (1960) starting from very different, mathematical arguments that in effect relied on an arbitrary but fixed coarse graining imposed on phase space (see Wehrl, 1978). Decoherence leads to a similar looking *quantum* result in a very different fashion: Coarse graining is imposed by the coupling to the environment, but only in the sense implied by the einselection. Its "graininess" (resolution) is set by the accuracy of the monitoring environment. This is especially obvious when the indirect monitoring strategy mentioned immediately above is adopted by the observers. Preferred states will be partly localized in x and p, but (in contrast to the harmonic oscillator case with its coherent states) details of this environment - imposed coarse graining will likely depend on phase space location, precise nature of the coupling to the environment, etc. Yet, in the appropriate limit, Eqs. (5.66)-(5.67), the asymptotic entropy production rate defined with the help of the algorithmic contribution discussed above (i.e., in a manner of the *physical entropy*, Zurek (1989)) does not depend on the strength or nature of the coupling, but is instead given by the sum of the positive Lyapunov exponents.

Von Neumann entropy production consistent with the above discussion has been now seen in numerical studies of decohering chaotic systems (Shiokawa and Hu, 1995; Furuya, Nemes, and Pellegrino, 1998; Miller and Sarkar, 1999; Schack, 1998; Monteoliva and Paz, 2000 & 2001). Extensions to situations where relaxation matters, as well as in the opposite direction – to where decoherence is relatively gentle – have been also discussed (Brun, Percival, and Schack, 1995; Miller, Sarkar, and Zarum, 1998; Pattanyak, 2000). An exciting development is the experimental study of the Loschmidt echo using NMR techiques (Levstein, Usaj, and Pastawski, 1998; Levstein et al, 2000, Jalabert and Pastawski, 2001) which sheds a new light on the irreversibility in decohering complex dynamical systems. We shall briefly return to this subject in Section VIII, while discussing experimental investigations relevant for decoherence and quantum chaos.

Quantum predictability horizon

The cross section I of the trajectory-like tube containing the state of the harmonic oscillator in phase space increases only slowly, Eq. (5.58), at a rate which – once the limiting Gaussian is reached – does not depend on I. By contrast, in chaotic quantum systems this rate is:

$$\dot{I} \simeq I \sum_i \Lambda_+^{(i)} . \tag{5.70}$$

A fixed rate of entropy production implies an exponential increase of the cross-section of the tube of, say, the 1-σ contour containing points consistent with the initial conditions: Phase space support expands exponentially.

This quantum view of chaotic evolution can be compared with the classical "deterministic chaos". In both cases, in the appropriate classical limit – which may involve either mathematical $\hbar \to 0$, or a macroscopic limit – the future state of the system can be in principle predicted to a set accuracy for an arbitrarily long time. However, such predictability can be accomplished only when the initial conditions are given with the resolution that increases exponentially with the time interval over which the predictions are to be valid. Given the fixed value of $\hbar$, there is therefore a *quantum predictability horizon* after which the Wigner function of the system starting from an initial minimum uncertainty Gaussian becomes stretched to the size of the order of the characteristic dimension of the system (Zurek, 1998b). The ability to predict the location of the system in the phase space is then lost after $t \sim t_\hbar$, Eq. (3.5), regardless of whether evolution is generated by the Poisson or Moyal bracket, or, indeed, whether the system is closed or open.

The case of regular systems is closer to the harmonic oscillator. The rate of increase of the cross-section of phase space "trajectory tube" consistent with the initial patch in the phase

space will asymptote to $\dot{I} \simeq const$:

$$\dot{H} = \dot{I}/I \sim 1/t \ . \tag{5.71}$$

Thus, initial conditions allow one to predict future of a regular system for time intervals that are exponentially longer than in the chaotic case. The rate of entropy production of an open quantum system is therefore a very good indicator of the nature of its dynamics, as was conjectured some time ago (Zurek and Paz, 1995a), and as seems born out in the numerical simulations (Shiokawa and Hu, 1995; Miller, Sarkar and Zarum, 1998; Miller and Sarkar, 1999; Monteoliva and Paz, 2000 & 2001).

21.6 Einselection and Measurements

It is often said that quantum states play only an *epistemological* role in describing observers knowledge about the past measurement outcomes that have prepared the system (Jammer, 1974; d'Espagnat, 1976, 1995; Fuchs and Peres, 2000). In particular – and this is a key argument against their objective existence (against their *ontological* status) – it is impossible to find out what the state of an isolated quantum system *is* without prior information about the observables used to prepare it: Measurement of observables that do not commute with this original set will inevitably create a *different* state.

The incessant monitoring of the einselected observables by the environment allows pointer states to *exist* in much the same way classical states do. This ontological role of the einselected quantum states can be justified operationally, by showing that *in presence of einselection one can find out what the quantum state is, without inevitably re-preparing it by the measurement.* Thus, einselected quantum states are no longer just epistemological. In a system monitored by the environment *what is* – the einselected states – coincides with *what is known to be* – what is recorded by the environment (Zurek, 1993a,b; 1998a).

The conflict between the quantum and the classical was originally noted and discussed almost exclusively in the context of quantum measurements (Bohr, 1928; Mott, 1929; von Neumann, 1932; Dirac, 1947; Zeh, 1971, 1973, 1993; d'Espagnat, 1976, 1995; Zurek 1981, 1982, 1983, 1991, 1993a&b, 1998a; Omnès 1992, 1994; Elby, 1993, 1998; Butterfield, 1996; Donald, 1995; Giulini et al., 1996; Bub, 1997; Saunders, 1998; Healey, 1998; Bacciagaluppi and Hemmo, 1998; Healey and Hellman, 1998). Here I shall consider quantum measurements, and, more to the point, acquisition of information in quantum theory from the point of view of decoherence and einselection.

21.6.1 Objective existence of einselected states

To demonstrate *objective existence* of *einselected* states we now develop an operational definition of existence and show how, in the open system, one can find out what the state *was and is*, rather than just "prepare" it. This point was made before (Zurek, 1993a; 1998a), but this is first time I discuss it in more detail.

Objective existence of states can be defined operationally by considering two observers. The first of them is the *record keeper* **R**. He prepares the states with the original measurement and will use his records to find out if they were disturbed by the measurements carried out by other observers, e.g. the *spy* **S**. The goal of **S** is to discover the state of the system without perturbing it. When an observer can consistently find out the state of the system without changing it, that state – by our operational definition – will be said to *exist objectively.*

In absence of einselection the situation of the spy **S** is hopeless: **R** prepares states by measuring sets of commuting observables. Unless **S** picks, by sheer luck, the same observables *in case of each state*, his measurements will re-prepare states of the systems. Thus, when **R**

re-measures using the original observables, he will likely find answers different from his records. The spy **S** will "get caught", because it is impossible to find out an initially unknown state of an isolated quantum system.

In presence of environmental monitoring the nature of the "game" between **R** and **S** is dramatically altered. Now it is no longer possible for **R** to prepare an arbitrary pure state that will persist or predictably evolve without losing purity. Only the einselected states that are already monitored by the environment – that are selected by the predictability sieve – will survive. By the same token, **S** is no longer clueless about the observables he can measure without leaving incriminating evidence. For example, he can independently prepare and test survival of various states in the same environment to establish which states are einselected, and then measure appropriate pointer observables. Better yet, **S** can forgo direct measurements of the system, and gather information indirectly, by monitoring the environment.

This last strategy may seem contrived, but indirect measurements – acquisition of information about the system by examining fragments of the environment that have interacted with it – is in fact more or less the only strategy employed by the observers. Our eyes, for example, intercept only a small fraction of the photons that scatter from various objects. The rest of the photons constitute the environment, which retains at least as complete a record of the same einselected observables as we can obtain (Zurek, 1993; 1998a).

The environment $\mathcal{E}$ acts as a persistent observer, dominating the game with frequent questions, always about the same observables, compelling both **R** and **S** to focus on the einselected states. Moreover, $\mathcal{E}$ can be persuaded to share its records of the system. This accessibility of the einselected states is not a violation of the basic tenets of quantum physics. Rather, it is a consequence of the fact that the data required to turn quantum state into an ontological entity – an einselected pointer state – are abundantly supplied by the environment.

We emphasize the *operational* nature of this criterion for existence: There may be in principle a pure state of the Universe including the environment, the observer, and the measured system. While this may matter to some (Zeh, 2000), real observers are forced to perceive the Universe the way we do: We are a part of the Universe, observing it from within. Hence, for us, *environment-induced superselection specifies what exists.*

Predictability emerges as a key criterion of *existence*. The only states **R** can rely on to store the information are the pointer states. They are also the obvious choice for **S** to measure. Such measurements can be accomplished without danger of re-preparation. Einselected states are insensitive to measurement of the pointer observables – they have already been "measured" by the environment. Therefore, additional projections P_i onto the einselected basis will not perturb the density matrix (Zurek, 1993a) – it will be the same before and after the measurement:

$$\rho^D_{after} = \sum_i P_i \rho^D_{before} P_i \ . \tag{6.1}$$

Correlations with the einselected states will be left intact (Zurek 1981; 1982).

Superselection for the observable $\hat{A} = \sum_i \lambda_i P_i$ with essentially arbitrary non-degenerate eigenvalues λ_i and eigenspaces P_i can be expressed (Bogolubov et al., 1990) through Eq. (6.1). Einselection attains this, guaranteeing diagonality of density matrices in the projectors P_i corresponding to pointer states. These are sometimes called *decoherence - free subspaces* when they are degenerate; compare also nonabelian case of *noiseless subsystems* discussed in quantum computation; see Zanardi and Rasetti, 1997; Zanardi 1998; Duan and Guo 1998; Lidar, Bacon, and Whaley, 1999; Knill, Laflamme, and Viola, 2000; Blanchard and Olkiewicz, 2000; Zanardi 2000).

21.6.2 Measurements and memories

The memory of an apparatus or of an observer can be modelled as an open quantum $\mathcal{A}$, interacting with $\mathcal{S}$ through a Hamiltonian explicitly proportional to the measured observable $\hat{s}$ [7]

$$H_{int} = -g\hat{s}\hat{B} \sim \hat{s}\frac{\partial}{\partial \hat{A}} \ . \tag{6.2}$$

Von Neumann (1932) considered an apparatus isolated from the environment. At the instant of the interaction between the apparatus and the measured system this is a convenient assumption. For us it suffices to assume that, at that instant, the interaction Hamiltonian between the system and the apparatus dominates. This can be accomplished by taking the coupling g in Eq. (6.2) to be $g(t) \sim \delta(t - t_0)$. Premeasurement happens at t_0:

$$(\sum_i \alpha_i |s_i\rangle)|A_0\rangle \ \longrightarrow \ \sum_i \alpha_i |s_i\rangle|A_i\rangle \ . \tag{6.3}$$

In practice the action is usually large enough to accomplish amplification. As we have seen in section II, all this can be done without an appeal to the environment.

For a real apparatus interaction with the environment is inevitable. Idealized effectively classical memory will retain correlations, but will be subject to einselection: Only the einselected memory states (rather than their superpositions) will be useful for (or, for that matter, accessible to) the observer: Decoherence timescale is very short compared to the time after which memory states are typically consulted (i. e., copied or used in information processing), which is in turn much shorter than the relaxation timescale, on which memory "forgets".

Decoherence leads to *classical* correlation:

$$\begin{aligned} \rho^P_{\mathcal{SA}} &= \sum_{i,j} \alpha_i \alpha_j^* |s_i\rangle\langle s_j||A_i\rangle\langle A_j| \longrightarrow \\ &\longrightarrow \sum_i |\alpha_i|^2 |s_i\rangle\langle s_i||A_i\rangle\langle A_i| = \rho^D_{\mathcal{SA}} \qquad 6.4 \end{aligned} \tag{21.58}$$

following an entangling premeasurement. Left hand side of Eq. (6.4) coincides with Eq. (2.44c), the "outsiders" view of the classical measurement. We shall see how and to what extent its other aspects – including the insiders Eq. (2.44a) and the discoverers Eq. (2.44b) – can be understood through einselection.

21.6.3 Axioms of quantum measurement theory

Our goal is to establish whether the above model can fulfill requirements expected from measurement in textbooks (that are, essentially without exception, written in the spirit of the Copenhagen Interpretation). There are several equivalent 'textbook' formulations of axioms of quantum theory. We shall (approximately) follow Farhi, Goldstone, and Gutmann (1989) and posit:

(i) The states of a quantum system $\mathcal{S}$ are associated with the vectors $|\psi\rangle$ which are the elements of the Hilbert space $\mathcal{H}_\mathcal{S}$ that describes $\mathcal{S}$.

[7] The observable $\hat{s}$ of the system and $\hat{B}$ of the apparatus memory need not be discrete with a simple spectrum as was previously assumed. Even when $\hat{s}$ has a complicated spectrum, the outcome of the measurement can be recorded in the eigenstates of the memory observable $\hat{A}$, conjugate of $\hat{B}$, Eq. (2.21). For the case of discrete $\hat{s}$ the necessary calculations that attain premeasurement – the quantum correlation that is the first step in the creation of the record – were already carried out in section II. For the other situations they are quite similar. In either case, they follow the general outline of the von Neumann's (1932) discussion.

(ii) The states evolve according to $i\hbar|\dot{\psi}\rangle = H|\psi\rangle$ where H is Hermitean.

(iii a) Every observable O is associated with a Hermitian operator $\hat{O}$.

(iii b) The only possible outcome of a measurement of O is an eigenvalue o_i of $\hat{O}$.

(iv) Immediately after a measurement that yields the value o_i the system is in the eigenstate $|o_i\rangle$ of $\hat{O}$.

(v) If the system is in a normalized state $|\psi\rangle$, then a measurement of $\hat{O}$ will yield the value o_i with the probability $p_i = |\langle o_i|\psi\rangle|^2$.

The first two axioms make no reference to measurements. They state the formalism of the theory. Axioms (iii) - (v) are, on the other hand, at the heart of the present discussion. In the spirit, they go back to Bohr and Born. In the letter, they follow von Neumann (1932) and Dirac (1947). The two key issues are the *projection postulate*, implied by a combination of (iv) with (iiib), and the (Born's) *probability interpretation*, axiom (v).

To establish (iiib), (iv) and (v) we shall interpret – in operational terms – statements such as "the system *is* in the eigenstate" and "measurement will yield value ... with *the probability* ..." by specifying what these statements mean for the sequences of *records* made and maintained by an idealized, but physical *memory*.

We note that the above Copenhagen-like axioms presume existence of quantum systems and of classical measuring devices. This (unstated) "axiom (o)" complements axioms (i) - (v). Our version of axiom (o) demands that the Universe consists of systems, and asserts that a composite system can be described by a tensor product of the Hilbert spaces of the constituent systems. Some quantum systems can be measured, others can be used as measuring devices and/or memories, and as quantum environments that interact with either or both.

Axioms (iii) - (v) contain many idealizations. For instance, in real life or in laboratory practice measurements have errors (and hence can yield outcomes other than the eigenvalues o_i). Moreover, only rarely do they "prepare" the system in the eigenstate of the observable they are designed to measure. Furthermore, coherent states – often an outcome of measurements, e. g., in quantum optics – form an overcomplete basis. Thus, their detection does not correspond to a measurement of a Hermitean observable. Last not least, the measured quantity may be inferred from some other quantity (e.g. deflection of a beam in the Stern-Gerlach experiment). Yet, we shall not go beyond the idealizations of (i) - (v) above. Our goal is to describe measurements in a quantum theory "without collapse", to use axioms (o), (i) and (ii) to understand the origin of the other axioms. Non-ideal measurements are a fact of life incidental to this goal.

Observables are Hermitean – axiom (iiia)

In the model of measurement considered here the observables are Hermitean as a consequence of the assumed premeasurement interaction, e.g. Eq. (2.24). In particular, H_{int} is a product of the to-be-measured observable of the system and of the "shift operator" in the pointer of the apparatus or in the record state of the memory. Interactions involving non-Hermitean operators (e.g., $H_{int} \sim a^\dagger b + ab^\dagger$) may be, however, also considered.

It is tempting to speculate that one could dispose of the observables (and, hence, of the postulate (iiia)) altogether in the formulation of the axioms of quantum theory. The only ingredients necessary to describe measurements are then the effectively classical, but ultimately quantum apparatus, and the measured system. Observables emerge as a derived concept, as a useful idealization, ultimately based on the structure of the Hamiltonians. Their utility relies on the conservation laws that relate outcomes of several measurements. Most basic of these laws states that the system that did not (have time to) evolve will be found in the same state

when it is re-measured: This is the content of axiom (iv). Other conservation laws are also reflected in the patterns of correlation in the measurement records, that must in turn arise from the underlying symmetries of the Hamiltonians.

Einselection should be included in this program, as it decides which of the observables are accessible and useful – which are effectively classical. It is conceivable that also the "fundamental" superselection may emerge in this manner (see Zeh, 1970; Zurek, 1982; for early speculations; Giulini, Kiefer, and Zeh, 1995; and Kiefer, 1996; Giulini, 2000, for the present status of this idea).

Eigenvalues as outcomes – axiom (iiib)

This statement is the first part of the "collapse" postulate. Given einselection, (iiib) is easy to justify: We need to show that only the records inscribed in the einselected states of the apparatus pointer can be read off, and that – in a well-designed measurement – they correlate with the eigenstates (and, therefore, eigenvalues) of the measured observable $\hat{s}$.

With Dirac (1947) and von Neumann (1932) we assume that the apparatus is built so that it satisfies the obvious "truth table" when the eigenstates of the measured observable are at the input:

$$|s_i\rangle|A_0\rangle \longrightarrow |s_i\rangle|A_i\rangle \tag{6.5}$$

To assure this one can implement the interaction in accord with Eq. (6.2) and the relevant discussion in section II. This is not to say that there are no other ways: Braginski and Khalili (1996), Aharonov, Anandan and Vaidman (1993), and Unruh (1994) have all considered "adiabatic measurements", that correlate the apparatus with the discrete energy eigenstates of the measured system, nearly independently of the structure of H_{int}.

Truth table of Eq. (6.5) does not require collapse – for any initial $|s_i\rangle$ it represents a "classical measurement in quantum notation" in the sense of Section II. However, Eq. (6.5) typically leads to a superposition of outcomes. This is the "measurement problem". To address it, we assume that the record states $\{|A_i\rangle\}$ are einselected. This has two related consequences: (i) Following the measurement, the joint density matrix of the system and the apparatus decoheres, Eq. (6.3), so that it satisfies the superselection condition, Eq. (6.1), for $P_i = |A_i\rangle\langle A_i|$. (ii) Einselection restricts states that can be read of "as if they were classical" to pointer states.

Indeed, following decoherence only pointer states $\{|A_i\rangle\}$ of the memory can be measured without diminishing the correlation with the states of the system. Without decoherence, as we have seen in section II, one could use entanglement between $\mathcal{S}$ and $\mathcal{A}$ to end up with an almost arbitrary superposition states of either, and, hence, to violate the letter and the spirit of (iiib).

Outcomes are restricted to the eigenvalues of measured observables because of einselection. Axiom (iiib) is then a consequence of the effective classicality of pointer states, the only ones that can be "found out" without being disturbed. They can be consulted repeatedly and remain unaffected under the joint scrutiny of the observers and of the environment (Zurek, 1981; 1993a; 1998a).

Immediate repeatability, axiom (iv)

This axiom supplies the second half of the "collapse" postulate. It asserts that in the absence of (the time for) evolution quantum system will remain in the same state, and its re-measurement will lead to the same outcome. Hence, once the system is found out to be in a certain state, it really is there. As in Eq. (2.44b) observer perceives potential options "collapse" to a single actual outcome. (The association of the axiom (iv) with the collapse advocated here seems obvious, but it is not common: Rather, some form of our axiom (iiib) is usually regarded as the sole "collapse postulate".)

Immediate repeatability for Hermitean observables with discrete spectra is straightforward to justify on the basis of Schrödinger evolution generated by H_{int} of Eq. (6.2) alone, although its implications depend on whether the premeasurement is followed by einselection. Everett (1957) used the "no decoherence" version as a foundation of his relative state interpretation. On the other hand, without decoherence and einselection one could postpone the choice of what was actually recorded by taking advantage of the entanglement between the system and the apparatus, evident on the left hand side of Eq. (6.3). For instance, a measurement carried out on the apparatus in a basis different from $\{|A_i\rangle\}$ would also exhibit a one-to-one correlation with the system: $\sum_i \alpha_i|s_i\rangle|A_i\rangle = \sum_k \beta_k|r_k\rangle|B_k\rangle$. This flexibility to re-write wavefunctions in different bases comes at a price of relaxing the demand that the outcome states $\{|r_k\rangle\}$ be orthogonal (so that there would be no associated Hermitean observable). However, as was already noted, coherent states associated with a non-Hermitean annihilation operator can also be an outcome of a measurement. Therefore (and in spite of the strict interpretation of axiom (iiia)) this is not a very serious restriction.

In presence of einselection the basis ambiguity disappears. Immediate repeatability would apply only to the records made in the einselected states. Other apparatus observables lose correlation with the state of the system on decoherence timescale. In the effectively classical limit it is natural to demand repeatability extending beyond that very short time interval. This demand makes the role of einselection in establishing axiom (iv) evident. Indeed, such repeatability is – albeit in a more general context – the motivation for the predictability sieve.

Probabilities, einselection and records

Density matrix alone – without the preferred set of states – does not suffice as a foundation for a probability interpretation. For, any mixed state density matrix $\rho_{\mathcal{S}}$ can be decomposed into sums of density matrices that add up to the same resultant $\rho_{\mathcal{S}}$, but need not share the same eigenstates. For example, consider $\rho^a_{\mathcal{S}}$ and $\rho^b_{\mathcal{S}}$, representing two different preparations (i.e., involving measurement of two distinct, non-commuting observables) of two ensembles, each with multiple copies of a system $\mathcal{S}$. When they are randomly mixed in proportions p^a and p^b, the resulting density matrix:

$$\rho^{a\vee b}_{\mathcal{S}} = p^a\rho^a_{\mathcal{S}} + p^b\rho^b_{\mathcal{S}}$$

is the complete description of the unified ensemble (see Schrödinger (1936); Jaynes (1957)).

Unless $[\rho^a_{\mathcal{S}}, \rho^b_{\mathcal{S}}] = 0$, the eigenstates of $\rho^{a\vee b}_{\mathcal{S}}$ do not coincide with the eigenstates of the components. This feature makes it difficult to regard any density matrix in terms of probabilities and ignorance. Such ambiguity would be especially troubling if it arose in the description of an observer (or, for that matter, of any classical system). Ignorance interpretation – i.e., the idea that probabilities are observer's way of dealing with uncertainty about the outcome we have briefly explored in the discussion of the insider-outsider dichotomy, Eqs. (2.44), – requires at the very least that the set of events ("the sample space") exists independently of the information at hand – i.e, independently of p^a and p^b in the example above. Eigenstates of the density matrix do not supply such events, since the additional loss of information associated with mixing of the ensembles alters the candidate events.

Basis ambiguity would be disastrous for record states. Density matrices describing a joint state of the memory $\mathcal{A}$ and of the system $\mathcal{S}$:

$$\rho^{a\vee b}_{\mathcal{AS}} = p_a\rho^a_{\mathcal{AS}} + p_b\rho^b_{\mathcal{AS}}$$

would have to be considered. In absence of einselection the eigenstates of such $\rho^{a\vee b}_{\mathcal{AS}}$ need not be even associated with a fixed set of record states of the presumably classical $\mathcal{A}$. Indeed, in general

$\rho^{a\vee b}_{\mathcal{AS}}$ has a non-zero discord,[8] and its eigenstates are entangled (even when the above $\rho^{a\vee b}_{\mathcal{AS}}$ is separable, and can be expressed as mixture of matrices that have no entangled eigenstates). This would imply an ambiguity of what are the record states, precluding probability interpretation of measurement outcomes.

Observer may nevertheless have records of a system that is in an ambiguous situation described above. Thus;

$$\rho^{a\vee b}_{\mathcal{AS}} \;=\; \sum_k w_k |A_k\rangle\langle A_k| (p^a_k \rho^a_{\mathcal{S}_k} + p^b_k \rho^b_{\mathcal{S}_k})$$

are admissible for an effectively classical $\mathcal{A}$ correlated with a quantum $\mathcal{S}$. Now the discord $\delta_{\mathcal{A}}\mathcal{I}(\mathcal{S}|\mathcal{A}) = 0$.

Mixing of ensembles of pairs of correlated systems one of which is subject to einselection does not lead to ambiguities discussed above. Discord $\delta_{\mathcal{A}}(\mathcal{S}|\mathcal{A})$ disappears in the einselected basis of $\mathcal{A}$, and the eigenvalues of the density matrices can behave as classical probabilities associated with 'events' – with the records. The "menu" of possible events in the sample space – e.g., records in memory – is fixed by einselection. Whether one can really justify this interpretation of the eigenvalues of the reducued density matrix is a separate question we are about to address.

21.6.4 Probabilities from Envariance

The view of 'the emergence of the classical' based on the environment – induced superselection has been occassionally described as "for practical purposes only" (see, e.g., Bell, 1990), to be contrasted with more fundamental (if nonexistent) solutions of the problem one could imagine (i.e., by modifying quantum theory; see Bell, 1987, 1990). This attitude can be in part traced to the reliance of einselection on reduced density matrices: For, even when explanations of all aspects of the effectively classical behavior are accepted in the framework of, say, Everett's MWI, and after the operational approach to objectivity and perception of unique outcomes based on the existential interpretation explained earlier is adopted, one major gap remains: Born's rule – axiom (v) connecting probabilities with the amplitudes, $p_k = |\psi_k|^2$ – has to be postulated in addition to axioms (o) - (ii). True, one can show that within the framework of einselection Born's rule emerges naturally (Zurek, 1998a). Decoherence is, however, based on on reduced density matrices. Now, since they were introduced by Landau (1927), it is known that "partial trace" leading to reduced density matrices is predicated on Born's rule (see Nielsen and Chuang, 2000, for discussion). Thus, derivations of Born's rule that employ reduced density matrices are open to charge of circularity (Zeh, 1997). Moreover, repeated attempts to justify $p_k = |\psi_k|^2$

[8] As we have seen in section IV, Eqs. (4.30) – (4.36), *discord* $\delta\mathcal{I}_{\mathcal{A}}(\mathcal{S}|\mathcal{A}) = \mathcal{I}(\mathcal{S}:\mathcal{A}) - \mathcal{J}_{\mathcal{A}}(\mathcal{S}:\mathcal{A})$ is a measure of the"quantumness" of correlations. It should disappear as a result of the classical equivalence of two definitions of the mutual information, but is in general positive for quantum correlations, including, in particular, predecoherence $\rho_{\mathcal{SA}}$. Discord is asymmetric, $\delta\mathcal{I}_{\mathcal{A}}(\mathcal{S}|\mathcal{A}) \neq \delta\mathcal{I}_{\mathcal{S}}(\mathcal{A}|\mathcal{S})$. Vanishing of $\delta\mathcal{I}_{\mathcal{A}}(\mathcal{S}|\mathcal{A})$ (i.e., of the discord in the direction exploring the classicality of the states of $\mathcal{A}$, on which $H(\rho_{\mathcal{S}|\mathcal{A}})$ in the asymmetric $J_{\mathcal{A}}(S:A)$, Eq. (4.32), is conditioned) is necessary for the classicality of the measurement outcome (Zurek, 2000; Ollivier and Zurek, 2002, Zurek, 2002a). $\delta\mathcal{I}_{\mathcal{A}}(\mathcal{S}|\mathcal{A})$ can disappear as a result of decoherence in the einselected basis of the apparatus. Following einselection it is then possible to ascribe probabilities to the pointer states.
In perfect measurements of Hermitean observables discord vanishes "both ways": $\delta\mathcal{I}_{\mathcal{A}}(\mathcal{S}|\mathcal{A}) = \delta\mathcal{I}_{\mathcal{S}}(\mathcal{A}|\mathcal{S}) = 0$ for the pointer basis and for the eigenbasis of the measured observable correlated with it. Nevertheless, it is possible to encounter situations when vanishing of the discord in one direction is *not* accompanied by its vanishing "in reverse". Such correlations are "classical one way" (Zurek, 2002a) and could arise, for instance, in measurements of non-hermitean observables (which – as we have already noted – happen, in spite of the axiom (iii)).
This asymmetry between classical $\mathcal{A}$ and quantum $\mathcal{S}$ arises from the einselection. Classical record states are not arbitrary superpositions. Observer accesses his memory in the basis in which it is monitored by the environment. The information stored is effectively classical because it is being widely disseminated. States of the observers memory exist objectively – they can be found out through their imprints in the environment.

within the no - collapse MWI (Everett, 1957 a&b; DeWitt, 1970; DeWitt and Graham, 1973; Geroch, 1984) have failed (see e.g., Stein, 1984; Kent, 1990; Squires, 1990): The problem is their circularity: An appeal to the connection (especially in certain limiting procedures) between the smallnes of the amplitude and the vanishing of probabilities has to be made to establish that relative frequencies of events averaged over branches of the universal state vector are consitent with Born's rule. In particular, one must a claim that "maverick" branches of the MWI state vector that have "wrong" relative frequencies are of measure zero because their Hilbert space measures are small. This is circular, as noted even by the proponents (DeWitt, 1970).

My aim here is to look at the origin of ignorance, information, and, therefore, probabilities from a very quantum and fundamental perspective: Rather than focus on probabilities for an individual isolated system I shall – in the spirit of einselection, but without employing its usual tools such as trace or reduced density matrices – consider what the observer can (and cannot) know about a system entangled with its environment. Within this context I shall demonstrate that Born's rule follows from the very quantum fact that one can know precisely the state of the composite system and yet be provably ignorant of the state of its components. This is due to *environment - assited invariance* or *envariance*, a hitherto unrecognised symmetry I am about to describe. Envariance of pure states is conspicuously missing from classical physics. It allows one to define ignorance as aconsequence of invariance, and thus to understand the origin of Born's rule, probabilities, and ultimately the origin of information through arguments based on assumptions different from Gleason's (1957) famous theorem. Rather, it is based on the Machian idea of 'relativity of quantum states' entertained by this author two decades ago (see p. 772 of Wheeler and Zurek, 1983), but not developed untill now. Envariance (Zurek, 2002b) addresses the question of meaning of these probabilities by defining "ignorance", and justifies a relative frequency argument, although in a manner different from the previous attempts.

Envariance

Environment - assisted invariance is a symmetry exhibited by the system $\mathcal{S}$ correlated with the other system (usually 'the environment' $\mathcal{E}$). When a state of the composite $\mathcal{SE}$ can be transformed by $u_{\mathcal{S}}$ acting solely on the Hilbert space $\mathcal{H}_{\mathcal{S}}$, but the effect of this transformation can be undone with an appropriate $u_{\mathcal{E}}$ acting only on $\mathcal{H}_{\mathcal{E}}$, so that the joint state $|\psi_{\mathcal{SE}}\rangle$ remains unaltered;

$$u_{\mathcal{S}} u_{\mathcal{E}} |\psi_{\mathcal{SE}}\rangle \ = \ |\psi_{\mathcal{SE}}\rangle \tag{6.6}$$

such $|\psi_{\mathcal{SE}}\rangle$ is envariant under $u_{\mathcal{S}}$. Generalization to mixed $\rho_{\mathcal{SE}}$ is obvious, but we shall find it easier to assume that $\mathcal{SE}$ has been purified in the usual fashion – i.e., by enlarging the environment.

Envariance is best elucidated by considering an example – an entangled state of $\mathcal{S}$ and $\mathcal{E}$. It can be expressed in the Schmidt basis as:

$$|\psi_{\mathcal{SE}}\rangle \ = \ \sum_k \alpha_k |s_k\rangle |\varepsilon_k\rangle \ , \tag{6.7}$$

where α_k are complex, while $\{|s_k\rangle\}$ and $\{|\varepsilon_k\rangle\}$ are orthonormal. For $|\psi_{\mathcal{SE}}\rangle$ (and, hence – given our above remark about purification – for any system correlated with the environment) it is easy to demonstrate:

Lemma 6.1: Unitary transformations co-diagonal with the Schmidt basis of $|\psi_{\mathcal{SE}}\rangle$ leave it envariant.

The *proof* relies on the form of such transformations:

$$u_{\mathcal{S}}^{\{|s_k\rangle\}} = \sum_k e^{i\sigma_k} |s_k\rangle\langle s_k| \ , \tag{6.8}$$

where σ_k is a phase. Hence;

$$u_{\mathcal{S}}^{\{|s_k\rangle\}}|\psi_{\mathcal{SE}}\rangle \; = \; \sum_k \alpha_k e^{i\sigma_k}|s_k\rangle|\varepsilon_k\rangle \; , \tag{6.9}$$

can be undone by:

$$u_{\mathcal{E}}^{\{|\varepsilon_k\rangle\}} = \sum_k e^{i\epsilon_k} \; |\varepsilon_k\rangle\langle\varepsilon_k| \tag{6.10}$$

providing that $\epsilon_k = 2\pi l_k - \sigma_k$ for some integer l_k. QED.

Thus, phases associated with the Schmidt basis are envariant. We shall see below that they are the only envariant property of entangled states. The transformations defined by Eq. (6.8) are rather specific – they share (Schmidt) eigenstates. Still, their existence leads us to:

Theorem 6.1: Local description of the system $\mathcal{S}$ entangled with a causally disconnected environment $\mathcal{E}$ must not depend on the phases of the coefficients α_k in the Schmidt decomposition of $|\psi_{\mathcal{SE}}\rangle$.

It follows that *all the measurable properties of the $\mathcal{S}$ are completely specified by the list of pairs* $\{|\alpha_k|; |s_k\rangle\}$. An equivalent way of establishing this phase envariance theorem appeals even more directly to causality: Phases of $|\psi_{\mathcal{SE}}\rangle$ can be arbitrarily changed by acting on $\mathcal{E}$ alone (e.g, by the local Hamiltonian with eigenstates $|\varepsilon_k\rangle$, generating evolution of the from of Eq. (6.9)). But causality prevents faster than light communication. Hence, no measurable property of $\mathcal{S}$ can be effected. QED.

Phase envariance theorem will turn out to be the crux of our argument. It relies on an input – entanglement and causality – which has not been employed to date in discussions of the origin of probabilities. In particular, this input is different and more "physical" than that of the succesfull derivation of Born's rules by Gleason (1957).

We also note that information contained in the "data base" $\{|\alpha_k|; |s_k\rangle\}$ implied by the Theorem 6.1 is the same as in the reduced density matrix of the system $\rho_{\mathcal{S}}$: Although we do not yet know probabilities of various $|s_k\rangle$, preferred basis of $\mathcal{S}$ has been singled out – Schmidt states (sometimes regarded as instantaneous pointer states; see e.g. Albrecht, (1992; 1993)) play a special role as the eigenstates of envariant transformations. Moreover, probabilities can depend on $|\alpha_k|$ (but not on the phases). We still do not know that $p_k = |\alpha_k|^2$.

The causality argument we could have used to establis Theorem 6.1 applies of course to arbitrary transformations one could perform on $\mathcal{E}$. However, such transformations would not be in general envariant (i.e., could not be undone by acting on $\mathcal{S}$ alone). Indeed – by the same token – all envariant transformations must be diagonal in Schmidt basis:

Lemma 6.2: All of the unitary envariant transformations of $|\psi_{\mathcal{SE}}\rangle$ have Schmidt eigenstates.

The proof relies on the fact that other unitary transformations would rotate Schmidt basis, $|s_k\rangle \rightarrow |\tilde{s}_k\rangle$. The rotated basis becomes a new 'Schmidt', and this fact cannot be affected by unitary transformations of $\mathcal{E}$ – by state rotations in the environment. But a state that has a different Schmidt decomposition from the original $|\psi_{\mathcal{SE}}\rangle$ is different. Hence, unitary transformation must be co-diagonal with Schmidt states to leave it envariant. QED.

Born's rule from envariance

When absolute values of some of the coefficients in Eq. (6.7) are equal, any orthonormal basis is 'Schmidt' in the corresponding subspace of $\mathcal{H}_{\mathcal{S}}$. This implies envariance of more general nature, e.g. under a *swap*;

$$u_{\mathcal{S}}(k \leftrightarrow j) = e^{i\phi_{kj}}|s_k\rangle\langle s_j| + h.c. \tag{6.11}$$

Swap can be generated by a phase rotation, Eq. (6.8), but in a basis complementary to the one swapped. Its envariance does not contradict Lemma 6.2, as any orthonormal basis in this case

is also 'Schmidt'). So, when $|\alpha_k| = |\alpha_j|$, the effect of a swap on the system can be undone by an obvious *counterswap* in the environment:

$$u_{\mathcal{S}}(k \leftrightarrow j) = e^{-i(\phi_{kj}+\phi_k-\phi_j+2\pi l_{kj})}|\varepsilon_k\rangle\langle\varepsilon_j| + h.c. \tag{6.12}$$

Swap can be applied to states that do not have equal absolute values of the coefficients, but in that case it is no longer envariant. Partial swaps can be also generated e.g., by underrotating or by a $u_{\mathcal{S}}^{\{|r_i\rangle\}}$, Eq. (6.8), but with the eigenstates $\{|r_i\rangle\}$ intermediate between these of the swapped and the complementary (Hadamard) basis. Swap followed by a counterswap exchanges coefficients of the swapped states in the Schmidt expansion, Eq. (6.7).

Classical correlated states can also exhibit something akin to envariance under a classical version of "swaps". For instance, a correlated state of system and an apparatus described by: $\rho_{\mathcal{SA}} \sim |s_k\rangle\langle s_k||A_k\rangle\langle A_k| + |s_j\rangle\langle s_j||A_j\rangle\langle A_j|$ can be swapped and counterswapped. The corresponding transformations would be still given by, in effect, Eqs. (6.11) - (6.12), but without phases, and swaps could no longer be generated by the rotations around the complementary basis. This situation corresponds to the "outsiders view" of the measurement process, Eq. (2.44c): Outsider can be aware of the correlation between the system and of the apparatus, but ignorant of their individual states. This connection between ignorance and envariance shall be exploited below.

Envariance based on ignorance may be found in the classical setting, but envariance of pure states is purely quantum: Observers can know perfectly the quantum joint state of $\mathcal{SE}$, yet be provably ignorant of $\mathcal{S}$. Consider a measurement carried out on the state vector of $\mathcal{SE}$ from the point of view of envariance:

$$|A_0\rangle\sum_{k=1}^{N}|s_k\rangle|\varepsilon_k\rangle \rightarrow \sum_{k=1}^{N}|A_k\rangle|s_k\rangle|\varepsilon_k\rangle \sim |\Phi_{\mathcal{SAE}}\rangle \tag{6.13}$$

Above, we have assumed that the absolute values of the coefficients are equal (and omitted them for notational simplicity). We also have ignored phases (which need not be equal) since – by the phase envariance theorem – they will not influence the state (and, hence, the probabilities) associated with $\mathcal{S}$.

Before the measurement observer with access to $\mathcal{S}$ cannot notice swaps in the state (such as Eq. (6.13)) with equal absolute values of the Schmidt coefficients. This follows from envariance of the pre-measurement $|\psi_{\mathcal{SE}}\rangle$ under swaps, Eq. (6.11).

One could argue this point in more detail by comparing what happens for two very different input states; an entangled $|\psi_{\mathcal{SE}}\rangle$ with equal absolute values of Schmidt coefficients and a product state:

$$|\varphi_{\mathcal{SE}}\rangle = |s_J\rangle|\varepsilon_J\rangle \ .$$

When observer knows he is dealing with $\varphi_{\mathcal{SE}}$, he knows the state and can predict outcome of the corresonding measurement on $\mathcal{S}$: Schrödinger equation or just the resulting truth table, Eq. (6.5), imply with certainty that his state – the future state of his memory – will be $|A_J\rangle$. Moreover, swaps involving $|s_J\rangle$ are *not* envariant for $\varphi_{\mathcal{SE}}$. They just swap the outcomes (i.e. when $u_{\mathcal{S}}(J \leftrightarrow L)$ precedes the measurement, memory will end up in $|A_L\rangle$).

By contrast,

$$|\psi_{\mathcal{SE}}\rangle \sim \sum_{k=1}^{N} e^{i\phi_k}|s_k\rangle|\varepsilon_k\rangle$$

is envariant under swaps. This allows the observer (who knows the joint state of $\mathcal{SE}$ exactly) to conclude that the probabilities of all the envariantly swappable outcomes must be the same. *Observer cannot predict his memory state after the measurement of $\mathcal{S}$ because he knows too much; the exact combined state of $\mathcal{SE}$.*

For completeness, we note that when there are system states that are absent from the above sum – i.e., states that 'appear with zero amplitude' – they cannot be envariantly swapped with the states present in the sum. Of course, observer can predict with certainty he will not detect any of the corresponding zero - amplitude outcomes.

This argument about *the ignorance of the observer concerning his future state – concerning the outcome of the measurement he is about to perform – is based on his perfect knowledge of a joint state of* $\mathcal{SE}$.

Probabilities refer to the guess observer makes on the basis of his information *before the measurement* about the state of his memory – "the future outcome" – after the measurement. As the left hand side of Eq. (6.13) is envariant under swaps of the system states, probabilities of all the states must be equal. Thus, by normalisation;

$$p_k = 1/N \ . \tag{6.14}$$

Moreover, probability of n mutually exclusive events that all appear in Eq. (6.13) with equal coefficients must be:

$$p_{k_1 \vee k_2 \vee ... \vee \ k_n} = n/N \ . \tag{6.15}$$

This concludes discussion of the equal probability case. Our case rests on the independence of the state of $\mathcal{S}$ entangled with $\mathcal{E}$ from the phases of the coefficients in the Schmidt representation – the Theorem 6.1 – which in the case of equal coefficients Eq. (6.13), allows envariant swapping, and yields Eqs. (6.14)-(6.15).

After a measurement situation changes. In accord with our preceding discussion we interpret presence of the term $|A_k\rangle$ in Eq. (6.13) as evidence that an outcome $|s_k\rangle$ can be (or indeed has been – the language here is somewhat dependent on the interpretation) recorded. Conversely, absence of some $|A_{k'}\rangle$ in the sum above implies that the outcome $|s_{k'}\rangle$ cannot occur. After a measurement memory of the observer who has detected $|s_k\rangle$ will contain the record $|A_k\rangle$. Futher measurements of the same observable on the same system will confirm that $\mathcal{S}$ is in indeed in the state $|s_k\rangle$.

This post-measurement state is still envariant, but only under swaps that involve *jointly* the state of the system and the correlated state of the memory:

$$u_{\mathcal{AS}}(k \leftrightarrow j) = e^{i\phi_{kj}} |s_k, A_k\rangle\langle s_j, A_j| + h.c. \tag{6.16}$$

Thus, if another observer ('Wigner's friend') was getting ready to find out – either by direct measurement of $\mathcal{S}$ or by communicating with observer $\mathcal{A}$ – the outcome of his measurement, he would be (on the basis of envariance) provably ignorant of the outcome $\mathcal{A}$ has detected, but could be certain of the $\mathcal{AS}$ correlation. We shall employ this joint envariance in the discussion of the case of unequal probabilities immediately below.

Note that our reasoning does not really appeal to the "information lost in the environment" in a sense in which this phrase is often used. Perfect knowledge of the combined state of the system and the environment is the basis of the argument for the ignorance od $\mathcal{S}$ alone: For entangled $\mathcal{SE}$, perfect knowlegde of $\mathcal{SE}$ is incompatible with perfect knowledge of $\mathcal{S}$. This is really a consequence of indeterminacy – joint observables with entangled eigenstates such as $\psi_{\mathcal{SE}}$ simply do not commute (as the reader is invited to verify) with the observables of the system alone. Hence, ignorance associated with envariance is ultimately mandated by Heisenberg indeterminacy.

The case of unequal coefficients can be reduced to the case of equal coefficients. This can be done in several ways, of which we choose one that makes use of the preceding discussion of envariance of the post-measurement state. We start with:

$$|\Phi_{\mathcal{SAE}}\rangle \sim \sum_{k=1}^{N} \alpha_k |A_k\rangle|s_k\rangle|\varepsilon_k\rangle \tag{6.17}$$

where $\alpha_k \sim \sqrt{m}_k$ and m_k is a natural number (and, by phase envariance theorem, we drop the phases). To get an envariant state we "increase the resolution" of $\mathcal{A}$ by assuming that;

$$|A_k\rangle = \sum_{j_k=1}^{m_k} |a_{j_k}\rangle/\sqrt{m}_k \tag{6.18}$$

An increase of resolution is a standard trick, used in classical probability theory "to even the odds". Note that we assume that basis states such as $|A_k\rangle$ are normalised (as they must be in a Hilbert space). This leads to:

$$|\Phi_{\mathcal{SAE}}\rangle \sim \sum_{k=1}^{N} \sqrt{m}_k \frac{\sum_{j_k=1}^{m_k} |a_{j_k}\rangle}{\sqrt{m}_k} |s_k\rangle|\varepsilon_k\rangle \tag{6.19}$$

We now assume that $\mathcal{A}$ and $\mathcal{E}$ interact (e.g., through a `c-shift` of section 2, with a truth table $|a_{j_k}\rangle|\varepsilon_k\rangle \rightarrow |a_{j_k}\rangle|e_{j_k}\rangle$ where $\{|e_{j_k}\rangle\}$ are all orthonormal), so that after simplifying and re-arranging terms we get a sum, over a new 'fine-grained' index, with the states of $\mathcal{S}$ that remain the same within 'coarse - grained cells', i.e., intervals measured by m_k:

$$|\tilde{\Phi}_{\mathcal{SAE}}\rangle \sim \sum_{k=1}^{N} |s_k\rangle(\sum_{j_k=1}^{m_k} |a_{j_k}\rangle|e_{j_k}\rangle) = \sum_{j=1}^{M} |s_{k(j)}\rangle|a_j\rangle|e_j\rangle \tag{6.20}$$

Above, $M = \sum_{k=1}^{N} m_k$, and $k(j) = 1$ for $j \leq m_1$, $k(j) = 2$ for $j \leq m_1 + m_2$, etc. The above state is envariant under combined swaps;

$$u_{\mathcal{SA}}(j \leftrightarrow j') = \exp(i\phi_{jj'})|s_{k(j)}, a_j\rangle\langle a_{j'}, s_{k(j')}| + h.c.$$

Suppose that an additional observer measures $\mathcal{SA}$ in the obviously swappable joint basis. By our equal coefficients argument, Eq. (6.14), we get $p(s_{k(j)}, a_j) = 1/M$. But the observer can ignore states a_j. Then the probability of different Schmidt states of $\mathcal{S}$ is, by Eq. (6.15);

$$p(s_k) = m_k/M = |\alpha_k|^2 \ . \tag{6.21}$$

This is Born's rule.

The case with coefficients that do not lead to commensurate probabilities can be treated by assuming continuity of probabilities as a function of the amplitudes and taking appropriate (and obvious) limits. This can be physically motivated: One would not expect probabilities to change drastically depending on the infinitesimal changes of the state. One can also extend the strategy outlined above to deal with probabilities (and probability densities) in cases such as $|s(x)\rangle$, i.e. when the index of the state vector changes continuously. This can be accomplished by discretising it (so that the measurement of Eq. (6.17) correlates different apparatus states with small intervals of x) and then repeating the strategy of Eqs. (6.17) - (6.21). The wavefuction $s(x)$ should be sufficiently smooth for this strategy to succeed.

We note that the "increase of resolution" we have exploited, Eqs. (6.18)-(6.21), need not be physically implemented for the argument to go through: The very possibility of carrying out these steps within the quantum formalism forces one to adopt Born's rule. For example, if the apparatus did not have the requisite extra resolution, Eq. (6.18), interaction of the environment with a still different 'counterweight' system $\mathcal{C}$ that yields

$$|\Psi_{\mathcal{SAEC}}\rangle = \sum_{k=1}^{N} \sqrt{m}_k |s_k\rangle|A_k\rangle|\varepsilon_k\rangle|C_k\rangle \tag{6.22}$$

would lead one to the Born's rule through steps similar to these we have invoked before, providing that $|C_k\rangle\}$ has the requisite resolution, $|C_k\rangle = \sum_{j_k=1}^{m_k} |c_{j_k}\rangle/\sqrt{m}_k$. Interaction resulting in a correlation, Eq. (6.22), can occur between $\mathcal{E}$ and $\mathcal{C}$, and happen far from the system of interest or from the apparatus. Thus, it will not influence probabilities of the outcomes of measurements carried out on $\mathcal{S}$ or of the records made by $\mathcal{A}$. Yet, the fact that it can happen leads us to the desired conclusion.

Relative frequencies from envariance

Relative frequency is a common theme studied with the aim of elucidating the physical meaning of probabilities in quantum theory (Everett, 1957; Hartle, 1968; DeWitt, 1970; Graham, 1970; Farhi, Goldstone, and Gutmann, 1989; Aharonov and Resnik, 2002). In particular, in the context of the "no collapse" MWI relative frequency seem to offer the best hope of arriving at the Born's rule and elucidating its physical significance. Yet, it is generally acknowledged that the MWI derivations offered to date have failed to attain this goal (Kent, 1990).

We postpone brief discussion of these efforts to the next section, and describe an approach to relative frequencies based on envariance. Consider an ensemble of many ($\mathcal{N}$) distinguishable systems prepared in the same initial state:

$$|\sigma_{\mathcal{S}}\rangle = \alpha|0\rangle + \beta|1\rangle \tag{6.23}$$

We focus on the two state case to simplify the notation. We also assume that $|\alpha|^2$ and $|\beta|^2$ are commensurate, so that the state vector of the whole ensemble of correlated triplets $\mathcal{SAE}$ after the requisite increases of resolution (see Eqs. (6.18)-(6.20) above) is given by:

$$|\Phi^{\mathcal{N}}_{\mathcal{SAE}}\rangle \sim \big(\sum_{j=1}^{m} |0\rangle|a_j\rangle|e_j\rangle + \sum_{j=m+1}^{M} |1\rangle|a_j\rangle|e_j\rangle\big)^{\otimes\mathcal{N}} \tag{6.24}$$

save for the obvious normalisation. This state is envariant under swaps of the joint states $|s, a_j\rangle$, as they appear with the same (absolute value) of the amplitude in Eq. (6.24). (By Theorem 6.1 we can omitt phases.)

After the exponentiation is carried out, and the resulting product states are sorted by the number of 0's and 1's in the records, we can calculate the number of terms with exactly n 0's, $\nu_{\mathcal{N}}(n) = \binom{\mathcal{N}}{n} m^n (M-m)^{\mathcal{N}-n}$. To get probability, we normalise:

$$p_{\mathcal{N}}(n) = \binom{\mathcal{N}}{n} \frac{m^n (M-m)^{\mathcal{N}-n}}{M^{\mathcal{N}}} = \binom{\mathcal{N}}{n} |\alpha|^{2n} |\beta|^{2(\mathcal{N}-n)} \ . \tag{6.25}$$

This is the distribution one would expect from Born's rule. To establish the connection with relative frequencies we appeal to the de Moivre - Laplace theorem (Gnedenko, 1982) which allows one to approximate above $p_{\mathcal{N}}(n)$ with a Gaussian:

$$p_{\mathcal{N}}(n) \simeq \frac{1}{\sqrt{2\pi\mathcal{N}}|\alpha\beta|} e^{-\frac{1}{2}\left(\frac{n-\mathcal{N}|\alpha|^2}{\sqrt{\mathcal{N}}|\alpha\beta|}\right)^2} \tag{6.26}$$

This last step requires large $\mathcal{N}$, but our previous discussion including Eq. (6.25) is valid for arbitrary $\mathcal{N}$. Indeed, equation (6.21) can be regarded as the $\mathcal{N} = 1$ case.

Nevertheless, for large $\mathcal{N}$ relative frequency is sharply peaked around the expected $\langle n\rangle = \mathcal{N}|\alpha|^2$. Indeed, in the limit $\mathcal{N} \to \infty$ appropriately rescaled $p_{\mathcal{N}}(n)$ tends to a Dirac $\delta(\upsilon - |\alpha|^2)$ in relative frequency $\upsilon = n/\mathcal{N}$. This justifies the relative frequency interpretation of the squares of amplitudes as probabilities in the MWI context. 'Maverick universes' with different

relative frequencies exist, but have a vanishing *probability* (and not just vanishing Hilbert space measure) for large $\mathcal{N}$.

Our derivation of the physical significance of probabilities – while it led to the relative frequency argument – was based on a very different set of assumptions than previous derivations. The key idea behind it is the connection between a symmetry (envariance) and ignorance (impossibility of knowing something). The unusual feature of our argument is that this ignorance (for an individual system $\mathcal{S}$) is demonstrated by appealing to the perfect knowledge of the larger joint system that includes $\mathcal{S}$ as a subsystem.

We emphasize that one could not carry out the basic step of our argument – the proof of the independence of the likelihoods from the phases of the Schmidt expansion coefficients – for an equal amplitude pure state of a single, isolated system. The problem with: $|\psi\rangle = N^{-\frac{1}{2}} \sum_k^N \exp(i\phi_k)|k\rangle$ is the accessibility of the phases. Consider, for instance; $|\psi\rangle \sim |0\rangle+|1\rangle-|2\rangle$ and $|\psi'\rangle \sim |2\rangle + |1\rangle - |0\rangle$. *In absence of decoherence* swapping of k's is detectable: Interference measurements (i.e., measurements of the observables with phase-dependent eigenstates $|1\rangle + |2\rangle$; $|1\rangle - |2\rangle$, etc.) would have revealed the difference between $|\psi\rangle$ and $|\psi'\rangle$. Indeed, given an ensemble of identical *pure* states an observer will simply find out what they are. Loss of phase coherence is essential to allow for the shuffling of the states and coefficients.

Note that in our derivation environment and einselection play an additional, more subtle role: Once a measurement has taken place – i.e., a correlation with the apparatus or with the memory of the observer was established – one would hope that records will retain validity over a long time, well beyond the decoherence timescale. This is a pre-condition for the axiom (iv). Thus, a "collapse" from a multitude of possibilities to a single reality can be confirmed by subsequent measurements only in the einselected pointer basis.

Other approaches to probabilities

Gnedenko (1982), in his classic textbook, lists three classical approaches to probability:

a. Definitions that appeal to *relative frequency* of occurrence of events in a large number of trials.

b. Definitions of probability as a *measure of certainty* of the observer.

c. Definitions that reduce probability to the more primitive notion of *equal likelihood*.

In the quantum setting, the relative frequency approach has been to date the most popular, especially in the context of the "no collapse" MWI ' (Everett, 1957a&b; Graham, 1970; DeWitt, 1970). Counting the number of the "clicks" seems most directly tied to the experimental manifestations of probability. Yet, Everett interpretation versions were generally found lacking (Kent, 1990; Squires, 1990), as they relied on circular reasoning, invoking *without physical justification* an abstract measure of Hilbert space to obtain a physical measure (frequency). Some of the criticisms seem relevant also for the versions of this approach that allow for the measurement postulates (iii) and (iv) (Hartle, 1968; Farhi, Goldstone and Guttmann, 1989). Nevertheless, for the infinite ensembles considered in the above references, (where, in effect, the Hilbert space measure of the MWI branches that violate relative frequency predictions is zero) that the eigenvalues of the *frequency operator* acting on a large or infinite ensemble of identical states will be consistent with the (Born formula) prescription for probabilities.

However, the infinite size of the ensemble necessary to prove this point is troubling (and unphysical) and taking the limit starting from a finite case is difficult to justify (Stein, 1984; Kent, 1990; Squires, 1990). Moreover, the frequency operator is a collective observable of the whole ensemble. It may be possible to relate observables defined for such an infinite ensemble supersystem to the states of individual subsystems, but the frequency operator does not do

it. This is well illustrated by the gedankenexperiment envisaged by Farhi et al. (1989). To provide a physical implementation of the frequency operator they consider a version of the Stern-Gerlach experiment where all the spins are attached to a common lattice, so that – during the passage through the inhomogeneity of the magnetic field – the center of mass of the whole lattice is deflected by an angle proportional to the projection of the net magnetic moment associated with the spins on the direction defined by the field gradient. The deflection is proportional to the eigenvalue of the frequency operator that is then a *collective* observable – states of individual spins remain in superpositions, uncorrelated with anything outside. This difficulty can be addressed with the help of decoherence (Zurek, 1998a), but using decoherence without justifying Born's formula first is fraught with danger of circularity.

Measure of certainty seems to be a rather vague concept. Yet, Cox (1946) has demonstrated that Boolean logic leads – after addition of a few reasonable assumptions – to the definition of probabilities that, in a sense, appear as an extension of the logical truth values. However, the rules of symbolic logic that underlie Cox's theorems are *classical*. One can adopt this approach (Zurek, 1998a) to probabilities in quantum physics only after decoherence "intervenes" restoring the validity of the distributive law, which is not valid in quantum physics (Birkhoff and von Neumann, 1936).

One can carry out equal likelihood approach in the context of decoherence (Zurek, 1998a). The problem is – as pointed out before – the use of trace, and the dangers of circularity. An attempt to pursue a strategy akin to equal likelihood in the quantum setting at the level of pure states of individual systems has been also made by Deutsch in his (unpublished) "signalling" approach to probabilities. The key idea is to consider a source of pure states, and to find out when the permutations of a set of basis states can be detected, and, therefore, used for communication. When permutations are undetectable, probabilities of the permuted set of states are declared equal. The problem with this idea (or with its more formal version described by DeWitt, 1998) is that it works only for superposition that have all the coefficients identical, *including their phases*. Thus, as we have already noted, for closed systems phases matter and there is no invariance under swapping. In a recent paper Deutsch (1999) has adopted a different approach based on decision theory. The basic argument focuses again on individual states of quantum systems, but – as noted in the critical comment by Barnum et al. (2000) – seems to make appeal to some of the aspects of decision theory that do depend on probabilities. In my view, it also leaves the problem of the phase dependence of the coefficients unaddressed.

Among other approaches, recent work of Gottfried (2000) shows that in a discrete quantum system coupled with a continuous quantum system Born's formula follows from the demand that the continuous system should follow classical mechanics in the appropriate limit. A somewhat different strategy, with a focus on the coincidences of the expected magnitude of fluctuations was proposed by Aharonov and Resnik (2002).

In comparison with all of the above strategies, 'probabilities from envariance' is the most radically quantum, in that it ultimately relies on entanglement (which is still sometimes regarded as 'a paradox', and 'to be explained': I have used it as an explanation). This may be the reason why it has not been discovered untill now. The insight offered by envariance into the nature ignorance and information sheds a new light on probabilities in physics. The (very quantum) ability to prove ignorance of a part of a system by appealing to perfect knowledge of the whole may resolve some of the difficulties of the classical approaches.

21.7 Environment as a Witness

Emergence of classicality can be viewed either as a consequence of the widespread dissemination of the information about the pointer states through the environment, or as a result of the censorship imposed by decoherence. So far I have focused on this second view, defining

existence as persistence – predictability in spite of the environmental monitoring. Predictability sieve is a way of discovering states that are classical in this sense (Zurek, 1993a&b; Zurek, Habib and Paz, 1993; Gallis, 1996).

A complementary approach focusses *not* on the system, but on the records of its state spread throughout the environment. Instead of "the least perturbed states" one can ask "what states of the system are easiest to discover by looking at the environment". Thus, environment is no longer just a source of decoherence, but acquires a role of a communication channel with a basis - dependent noise that is minimised by the preferred pointer states.

This approach can be motivated by the old dilemma: On the one hand, quantum states of isolated systems are purely "epistemic" (see e.g., Peres, (1993); Fuchs and Peres (2000)). Quantum cryptography (Bennett and DiVincenzo, 2000; Nielsen and Chuang, 2000, and references therein) uses this impossibility of finding out what is an unknown state of an isolated quantum system. On the other hand classical reality seems to be made up of quantum building blocks: States of macroscopic systems exist objectively – they can be found out by many observers independently without being destroyed or re-prepared. So – the question arises – how can objective existence — the "reality" of the classical states – emerge from "purely epistemic" wavefunctions?

There is not much one can do about this in case of a single state of an isolated quantum system. But open systems are subject to einselection and can bridge the chasm dividing their epistemic and ontic roles. The most direct way to see this arises from the recognition of the fact that we never *directly* observe any system. Rather, we discover states of macroscopic systems from the imprints they make on the environment: A small fraction of the photon environment intercepted by our eyes is often all that is needed. States that are recorded most redundantly in the rest of the Universe (Zurek, 1983; 1998a; 2000) are also easiest to discover. They can be found out indirectly, from multiple copies of the evidence imprinted in the environment, without a threat to their existence. Such states exist and are real – they can be found out without being destroyed as if they were really classical.

Environmental monitoring creates an ensemble of "witness states" in the subsystems of the environment, that allow one to invoke some of the methods of the statistical interpretation (Ballentine, 1970) while subverting its ideology – to work with an *ensemble* of objective evidence of a state of a *single* system. From this ensemble of witness states one can infer the state of the quantum system that has led to such "advertising". This can be done without disrupting the einselected states.

Predictability sieve selects states that entangle least with the environment. Question about predictability simultaneously lead to states that are most redundantly recorded in the environment. Indeed, this idea touches on the "quantum Darwinism" we have alluded to in the introduction: The einselected pointer states are not only best in surviving the environment, but, also, they broadcast the information about themselves – spread out their "copies" – throughout the rest of the Universe: Amplified information is easiest to amplify. This leads to analogies with "fitness" in the Darwinian sense, and suggests looking at einselection as a sort of natural selection.

21.7.1 Quantum Darwinism

Consider the "bit by byte" example of Section IV. Spin - system $\mathcal{S}$ is correlated with the environment:

$$\begin{aligned} |\psi_{\mathcal{SE}}\rangle &= a|\uparrow\rangle|00\ldots0\rangle + b|\downarrow\rangle|11\ldots1\rangle \\ &= a|\uparrow\rangle|\mathcal{E}_\uparrow\rangle + b|\downarrow\rangle|\mathcal{E}_\downarrow\rangle \qquad 7.1 \end{aligned} \tag{21.59}$$

The basis $\{|\uparrow\rangle, |\downarrow\rangle\}$ of $\mathcal{S}$ is singled out by the redundancy of the record. By comparison, the same $|\psi_{\mathcal{SE}}\rangle$ is:

$$\begin{aligned} |\psi_{\mathcal{SE}}\rangle &= |\odot\rangle(a|00\ldots0\rangle + b|11\ldots1\rangle)\sqrt{2} \\ &+ |\otimes\rangle(a|00\ldots0\rangle - b|11\ldots1\rangle)/\sqrt{2} \\ &= (|\odot\rangle|\mathcal{E}_{\odot}\rangle + |\otimes\rangle|\mathcal{E}_{\otimes}\rangle)/\sqrt{2} \qquad 7.2 \end{aligned} \tag{21.60}$$

in terms of the Hadamard-transformed $\{|\odot\rangle, |\otimes\rangle\}$.

One can find out whether $\mathcal{S}$ is $|\uparrow\rangle$ or $|\downarrow\rangle$ from a small subset of the environment bits. By contrast, states $\{|\odot\rangle, |\otimes\rangle\}$ cannot be easily inferred from the environment. States $\{|\mathcal{E}_{\odot}\rangle, |\mathcal{E}_{\otimes}\rangle\}$ are typically not even orthogonal, $\langle\mathcal{E}_{\odot}|\mathcal{E}_{\otimes}\rangle = |a|^2 - |b|^2$. And even when $|a|^2 - |b|^2 = 0$, the record in the environment is fragile: Only one relative phase distinguishes $|\mathcal{E}_{\odot}\rangle$ from $|\mathcal{E}_{\otimes}\rangle$ in that case, in contrast with multiple records of the pointer states in $|\mathcal{E}_{\uparrow}\rangle$ and $|\mathcal{E}_{\downarrow}\rangle$. Remarks that elaborate this observation follow. They correspond to several distinct measures of 'fitness' of states.

Consensus and algorithmic simplicity

>From the state vector $|\psi_{\mathcal{SE}}\rangle$, Eqs. (7.1) and (7.2), observer can find the state of the quantum system just by looking at the environment. To accomplish this, the total N of the environment bits can be divided into samples of n bits each, with $1 \ll n \ll N$. These samples can be then measured using observables that are the same within each sample, but differ between samples. They may correspond, for example, to different antipodal points in the Bloch spheres of the environment bits. In the basis $\{|0\rangle, |1\rangle\}$ (or bases closely aligned with it) the record inferred from the bits of information scattered in the environment will be easiest to come by. Thus, starting from the environment part of $|\psi_{\mathcal{SE}}\rangle$, Eq. (7.1), *the observer can find out, with no prior knowledge, the state of the system*: Redundancy of the record in the environment allows for a trial-and-error 'indirect' approach while leaving the system untouched.

In particular, measurement of n environment bits in a Hadamard transform of the basis $\{|0\rangle, |1\rangle\}$ yields a random-looking sequence of outcomes (i.e., $\{|+\rangle_1, |-\rangle_2, \ldots |-\rangle_n\}$). This record is algorithmically random: Its algorithmic complexity is of the order of its length (Li and Vitànyi, 1994):

$$K(\langle\mathcal{E}_n|+,-\rangle) \simeq n \tag{7.3}$$

By contrast, algorithmic complexity of the measurement outcomes in the $\{|0\rangle, |1\rangle\}$ basis will be small:

$$K(\langle\mathcal{E}_n|0,1\rangle) \ll n \ , \tag{7.4}$$

since the outcomes will be either $00\ldots0$ or $11\ldots1$. Observer seeking preferred states of the system by looking at the environment should then search for the minimal record size and, thus, for the maximum redundancy in the environmental record. States of the system that are recorded redundantly in the environment must have survived repeated instances of the environment monitoring, and are obviously robust and predictable.

Predictability we have utilized before to devise a "sieve" to select preferred states is used here again, but in a different guise: Rather than search for predictable sets of states of the system we are now looking for the records of the states of the system in the environment. Sequences of states of environment subsystems correlated with pointer states are mutually predictable and, hence, collectively algorithmically simple. States that are predictable in spite of the interactions with the environment are also easiest to predict from their impact on its state.

The state of the form of Eq. (7.1) can serve as an example of amplification. Generation of redundancy through amplification brings about objective existence of the otherwise subjective quantum states. States $|\uparrow\rangle$ and $|\downarrow\rangle$ of the system can be found out reliably from a small

fraction of the environment. By contrast, to find out whether the system was in a state $|\odot\rangle$ or $|\otimes\rangle$ one would need to detect *all* of the environment. Objectivity can be defined as the ability of many observers to reach consensus independently. Such consensus concerning states $|\uparrow\rangle$ and $|\downarrow\rangle$ is easily established – many ($\sim N/n$) can independently measure fragments of the environment.

Action distance

One measure of robustness of the environmental records is the action distance (Zurek, 1998a). It is given by the total *action* necessary to undo the distinction between the states of the environment corresponding to different states of the system, subject to the constraints arising from the fact that the environment consists of subsystems. Thus, to obliterate the difference between $|\mathcal{E}_\uparrow\rangle$ and $|\mathcal{E}_\downarrow\rangle$ in Eq. (7.1), one needs to "flip" one-by-one N subsystems of the environment. That implies an action – i.e., the least total angle by which a states must be rotated, see Section IIB – of:

$$\Delta(|\mathcal{E}_\uparrow\rangle, |\mathcal{E}_\downarrow\rangle) = N \left[\frac{\pi}{2} \cdot \hbar\right] \ . \tag{7.5}$$

By contrast a "flip" of phase of just one bit will reverse the correspondence between the states of the system and of the environment superpositions that make up $|\mathcal{E}_\odot\rangle$ and $|\mathcal{E}_\otimes\rangle$ in Eq (7.2). Hence:

$$\Delta(|\mathcal{E}_\odot\rangle, |\mathcal{E}_\otimes\rangle) = 1 \left[\frac{\pi}{2} \cdot \hbar\right] \ . \tag{7.6}$$

Given a fixed division of the environment into subsystems the action distance is a metric on the Hilbert space (Zurek, 1998a). That is;

$$\Delta(|\psi\rangle, |\psi\rangle) = 0 \ , \tag{7.7}$$

$$\Delta(|\psi\rangle, |\varphi\rangle) = \Delta(|\varphi\rangle, |\psi\rangle) \geq 0, \tag{7.8}$$

and the triangle inequality:

$$\Delta(|\psi\rangle, |\varphi\rangle) + \Delta(|\varphi\rangle, |\gamma\rangle) \geq \Delta(|\psi\rangle, |\gamma\rangle) \tag{7.9}$$

are all satisfied.

In defining Δ it is essential to restrict rotations to the subspaces of the subsystems of the whole Hilbert space, and to insist that the unitary operations used in defining distance act on these subspaces. It is possible to relax constraints on such unitary operations by allowing, for example, pairwise or even more complex interactions between subsystems. Clearly, in absence of any restrictions the action required to rotate any $|\psi\rangle$ into any $|\varphi\rangle$ would be no more than $\frac{\pi}{2}\hbar$. Thus, constraints imposed by the natural division of the Hilbert space of the environment into subsystems play an essential role. Preferred states of the system can be sought by extremizing action distance between the corresponding record states of the environment. In simple cases (e.g., see "bit-by-byte", Eq. (4.7) and below) the action distance criterion for preferred states coincides with the predictability sieve definition (Zurek, 1998a).

Redundancy and mutual information

The most direct measure of reliability of the environment as a witness is the information-theoretic redundancy of einselection itself. When environment monitors the system (see Fig. 4), the information about its state will spread to more and more subsystems of the environment. This can be represented by the state vector $|\psi_{\mathcal{SE}}\rangle$, Eq. (7.1), with increasingly long sequences of 0's and 1's in the record states. The record size – the number N of the subsystems of the environment involved – does not affect the density matrix of the system $\mathcal{S}$. Yet, it obviously

changes accessibility abd robustness of the information analogues of the Darwinian "fitness". As an illustration, let us consider `c-shift`'s. One subsystem of the environment (say, $\mathcal{E}_1$) with the dimension of the Hilbert space no less than that of the system

$$Dim\mathcal{H}_{\mathcal{E}1} \geq Dim\mathcal{H}_{\mathcal{S}}$$

suffices to eradicate off-diagonal elements of $\rho_{\mathcal{S}}$ in the control basis. On the other hand, when N subsystems of the environment correlate with the same set of states of $\mathcal{S}$, the information about these states is simultaneously accessible more widely. While $\rho_{\mathcal{S}}$ is no longer changing, spreading of the information makes the existence of the pointer states of $\mathcal{S}$ more objective – they are easier to discover without being perturbed.

Information theoretic *redundancy* is defined as the difference between the least number of bits needed to uniquely specify the message and the actual size of the encoded message. Extra bits allow for detection and correction of errors (Cover and Thomas, 1991). In our case, the message is the state of the system, and the channel is the environment. The information about the system will often spread over all of the Hilbert space $\mathcal{H}_{\mathcal{E}}$ that is enormous compared to $\mathcal{H}_{\mathcal{S}}$. Redundancy of the record of the pointer observables of selected systems can be also huge. Moreover, typical environments consist of obvious subsystems (i.e., photons, atoms, etc.). It is then useful to define redundancy of the record by the number of times the information about the system has been copied, or by how many times it can be independently extracted from the environment.

In the simple example of Eq. (7.1) such *redundancy ratio* $\mathcal{R}$ for the $\{|\uparrow\rangle, |\downarrow\rangle\}$ basis will be given by N, the number of environment bits perfectly correlated with the obviously preferred basis of the system. More generally, but in the same case of perfect correlation we obtain:

$$\mathcal{R} = \frac{\lg(Dim\mathcal{H}_{\mathcal{E}})}{\lg(Dim\mathcal{H}_{\mathcal{S}})} = \log_{Dim\mathcal{H}_{\mathcal{S}}}(Dim\mathcal{H}_{\mathcal{E}}) = N \tag{7.10}$$

where $\mathcal{H}_{\mathcal{E}}$ is the Hilbert space of the environment perfectly correlated with the pointer states of the system.

On the other hand, with respect to the $\{|\odot\rangle, |\otimes\rangle\}$ basis, the redundancy ratio for $|\psi_{\mathcal{SE}}\rangle$ of Eq. (7.2) is only $\sim$1 (see also Zurek, 1983; 2000): Redundancy measures the number of errors that can obliterate the difference between two records, and in this basis one phase flip is clearly enough. This basis dependence of redundancy suggests an alternative strategy to seek preferred states.

To define $\mathcal{R}$ in general we can start with mutual information between the subsystems of the environment $\mathcal{E}_k$ and the system $\mathcal{S}$. As we have already seen in section IV, definition of mutual information in quantum mechanics is not straightforward. The basis-independent formula:

$$\mathcal{I}_k = \mathcal{I}(\mathcal{S} : \mathcal{E}_k) = H(\mathcal{S}) + H(\mathcal{E}_k) - H(\mathcal{S}, \mathcal{E}_k) \tag{7.11}$$

is simple to evaluate (although it does have some strange features; see Eqs. (4.30) - (4.36)). In the present context it involves joint density matrix:

$$\rho_{\mathcal{SE}_k} = Tr_{\mathcal{E}/\mathcal{E}_k}\rho_{\mathcal{SE}} \tag{7.12}$$

where the trace is carried out over all of the environment except for its singled out fragment $\mathcal{E}_k$. In the example of Eq. (7.1) for any of the environment bits

$$\rho_{\mathcal{SE}_k} = |a|^2|\uparrow\rangle\langle\uparrow| \otimes |0\rangle\langle 0| + |b|^2|\downarrow\rangle\langle\downarrow| \otimes |1\rangle\langle 1| \quad .$$

Given the partitioning of the environment into subsystems, the redundancy ratio can be defined as:

$$\mathcal{R}_{\mathcal{I}(\{\otimes\mathcal{H}_{\mathcal{E}_k}\})} = \sum_k \mathcal{I}(\mathcal{S} : \mathcal{E}_k)/H(\mathcal{S}) \quad . \tag{7.13}$$

When $\mathcal{R}$ is maximized over all of the possible partitions,

$$\mathcal{R}_{\mathcal{I}max} = R_{\{\otimes \mathcal{H}_{\mathcal{E}k}\}} \tag{7.14}$$

obtains. Roughly speaking, and in the case when the number of the environment subsystems is large, $\mathcal{R}_{\mathcal{I}max}$ is the total number of copies of the information about (the optimal basis of) $\mathcal{S}$ that exist in $\mathcal{E}$. Maximal redundancy ratio $\mathcal{R}_{\mathcal{I}max}$ is of course basis - independent.

The information defined through the symmetric $\mathcal{I}_k$, Eq. (7.11), is in general inaccessible to observers who interrogate environment one subsystem at a time (Zurek, 2002a). It makes therefore a lot of sense to consider the basis-dependent locally accessible information and define the corresponding redundancy ratio $\mathcal{R}_{\mathcal{J}}$ using:

$$\mathcal{J}_k = \mathcal{J}(\mathcal{S} : \mathcal{E}_k) = H(\mathcal{S}) + H(\mathcal{E}_k) - (H(\mathcal{S}) + H(\mathcal{E}_k|\mathcal{S})). \tag{7.15}$$

Conditional entropy must be computed in a specific basis of the system (see Eq. (4.32)). All of the other steps that have led to the definition of $\mathcal{R}_{\mathcal{I}max}$ can be now repeated using $\mathcal{J}_k$. In the end, a basis - dependent:

$$\mathcal{R}_{\mathcal{J}}(\{|s\rangle\}) = \mathcal{R}_{\mathcal{J}}(\otimes \mathcal{H}_{\mathcal{E}k}) \tag{7.16}$$

obtains. $\mathcal{R}_{\mathcal{J}}(\{|s\rangle\})$ quantifies the mutual information between the collection of subsystems $\mathcal{H}_{\mathcal{E}k}$ of the environment and the basis $\{|s\rangle\}$ of the system. We note that the condition of non-overlapping partitions guarantees that all of the corresponding measurements commute, and that the information can be indeed extracted independently from each environment fragment $\mathcal{E}_k$.

Preferred basis of $\mathcal{S}$ can be now defined by maximizing $\mathcal{R}_{\mathcal{J}}(\{|s\rangle\})$ with respect to the selection of $\{|s\rangle\}$:

$$\mathcal{R}_{\mathcal{J}max} = \max_{\{|s\rangle\};\{\otimes \mathcal{H}_{\mathcal{E}k}\}} \mathcal{R}_{\mathcal{J}}(\{|s\rangle\}) \tag{7.17}$$

This maximum can be sought either by varying the basis of the system only (as it is indicated above) or by varying both the basis and the partition of the environment.

It remains to be seen whether and under what circumstances pointer basis "stands out" through its definition in terms of $\mathcal{R}_{\mathcal{J}}$. The criterion for a well - defined set of pointer states $\{|p\rangle\}$ would be:

$$\mathcal{R}_{\mathcal{J}max} = \mathcal{R}_{\mathcal{J}}(\{|p\rangle\}) \gg \mathcal{R}_{\mathcal{J}}(\{|s\rangle\}) \tag{7.18}$$

where $\{|s\rangle\}$ are typical superpositions of states belonging to different pointer eigenstates.

This definition of preferred states directly employs the notion of multiplicity of records available in the environment. Since $\mathcal{J} \leq \mathcal{I}$, it follows that:

$$\mathcal{R}_{\mathcal{J}max} \leq \mathcal{R}_{\mathcal{I}max} \tag{7.19}$$

The important feature of either version of $\mathcal{R}$ that makes them useful for our purpose is their independence on $H(\mathcal{S})$: The dependence on $H(\mathcal{S})$ is in effect "normalized out" of $\mathcal{R}$. $\mathcal{R}$ characterizes the "fan-out" of the information about the preferred basis throughout environment, without a reference to what is known about the system. The usual redundancy (in bits) is then $\sim \mathcal{R} \cdot \mathcal{H}(\mathcal{S})$, although other implementations of this program (Ollivier, Poulin, and Zurek, 2002) employ different measures of redundancy, which may be even more specific than the redundancy ratio we have described above. Indeed, what is important here is the genreal idea of measuring classicality of quantum states through the number of copies they imprint throughout the Universe. This is a very Darwinian approach: We define classicality related to einselection in ways reminiscent of 'fitness' in natural selection: States that spawn most of the (information-theoretic) progeny are the most classical.

Redundancy ratio rate

The rate of change of redundancy is of interest as another measure of 'fitness', perhaps closest to the definitions of fitness used in modeling natural selection. Redundancy can increase either as a result of interactions between the system and the environment, or because the environment already correlated with $\mathcal{S}$ is passing on the information to more distant environments. In this second case 'genetic information' is passed on by the 'progeny' of the original state. Even an observer consulting the environment becomes a part of such a more distant environment. Redundancy rate is defined as:

$$\dot{\mathcal{R}} = \frac{d}{dt}\mathcal{R} \tag{7.20}$$

Either basis-dependent or basis-independent versions of $\dot{\mathcal{R}}$ may be of interest.

In general, it may not be easy to compute either $\mathcal{R}$ or $\dot{\mathcal{R}}$ exactly. This is nevertheless possible in models (such as those leading to Eqs. (7.1) - (7.2)). The simplest illustrative example corresponds to the `c-not` model of decoherence in Fig. 4. One can imagine that the consecutive record bits get correlated with the two branches (corresponding to $|0\rangle$ and $|1\rangle$ in the "control") at discrete moments of time. $\mathcal{R}(t)$ would be then the total number of `c-not`s that have acted over the time t, and $\dot{\mathcal{R}}$ is the number of new `c-not`s added per unit time.

Redundancy rate measures information flow from the system to the environment. Note that, after the first `c-not` in the example of Eqs. (7.1) - (7.2), $\mathcal{R}_{\mathcal{I}}$ will jump immediately from 0 to 2 bits, while the basis-specific $\mathcal{R}_{\mathcal{J}}$ will increase from 0 to 1. In our model this initial discrepancy (which reflects quantum discord, Eq. (4.36), between $\mathcal{I}$ and $\mathcal{J}$) will disappear after the second `c-not`.

Finally, we note that $\mathcal{R}$ and, especially, $\dot{\mathcal{R}}$ can be used to introduce new predictability criteria: The states (or the observables) that are being recorded most redundantly are the obvious candidates for the "objective", and therefore for the "classical".

21.7.2 Observers and the Existential Interpretation

Von Neumann (1932), London and Bauer (1939) and Wigner (1963) have all appealed to the special role of the *conscious* observer. Consciousness was absolved from following unitary evolution, and, thus, could collapse the wavepacket. Quantum formalism has led us to a different view, that nevertheless allows for a compatible conclusion. In essence, macroscopic systems are open, and their evolution is almost never unitary. Records maintained by the observers are subject to einselection. In a binary alphabet decoherence will allow only for the two logical states, and prohibit their superpositions (Zurek, 1991). For human observers neurons conform to this binary convention and the decoherence times are short (Tegmark, 2000). Thus, even if a cell of the observer entangles through a premeasurement with a pure quantum state, the record will become effectively classical almost instantly: As a result, it will be impossible to "read it off" in any basis except for the einselected one. This censorship of records is the key difference between the existential interpretation and the original Everett's MWI.

Decoherence treats observer as any other macroscopic system. There is, however, one feature distinguishing observers from the rest of the Universe: They are *aware* of the content of their memory. Here we are using *aware* in a down - to - earth sense: Quite simply, observers know what they know. Their information processing machinery (that must underlie higher functions of the mind such as "consciousness") can readily consult the content of their memory.

The information stored in the memory comes with 'strings attached'. The physical state of the observer is described in part by the data in his records. *There is no information without representation.* The information observer has could be, in principle, deduced from his physical state. Observer is – in part – information. Moreover, this information encoded in states of macroscopic quantum systems (neurons) is by no means secret: As a result of lack of isolation

the environment – having redundant copies of the relevant data – 'knows' in detail everything observer knows. Configurations of neurons in our brains, while at present undecipherable, are in principle as objective and as widely accessible as the information about the states of other macroscopic objects.

The observer *is* what he knows. In the unlikely case of a flagrantly quantum input the physical state of the observers memory will decohere, resulting almost instantly in the einselected alternatives, each of them representing simultaneously both observer and his memory. The 'advertising' of this state throughout the environment makes it effectively objective.

An observer perceiving the Universe from within is in a very different position than an experimental physicist studying a state vector of a quantum system. In a laboratory, Hilbert space of the investigated system is typically tiny. Such systems can be isolated, so that often the information loss to the environment can be prevented. Then the evolution is unitary. The experimentalist can know everything there is to know about it. Common criticisms of the approch advocated in this paper are based on an unjustified extrapolation of the above laboratory situation to the case of the observer who is a part of the Universe. Critics of decoherence often note that the differences between the laboratory example above and the case of the rest of the Universe are 'merely quantitative' – the system under investigation is bigger, etc. So why cannot one analyze – they ask – interactions of the observer and the rest of the Universe as before, for a small isolated quantum system?

In the context of the existential interpretation the analogy with the laboratory is, in effect, turned "upside down": For, now the observer (or the apparatus, or anything effectively classical) is continuously monitored by the rest of the Universe. Its state is repeatedly collapsed – forced into the einselected states – and very well (very redundantly) 'known' to the rest of the Universe.

The 'higher functions' of observers – e.g., consciousness, etc. – may be at present poorly understood, but it is safe to assume that they reflect physical processes in the information processing hardware of the brain. Hence, mental processes are in effect objective, as they leave an indelible imprint on the environment: The observer has no chance of perceiving either his memory, or any other macroscopic part of the Universe in some arbitrary superposition. Moreover, memory capacity of observers is miniscule compared to information content of the Universe. So, while observers may know exact state of laboratory systems, their records of the Universe will be very fragmentary. By contrast, the Universe has enough memory capacity to acquire and maintain detailed records of states of macroscopic systems and their histories.

21.7.3 Events, Records, and Histories

Suppose that instead of a monotonous record sequence in the environment basis corresponding to the pointer states of the system $\{|\uparrow\rangle, |\downarrow\rangle\}$ implied by Eq. (7.1) the observer looking at the environment detects:

$$000...0111...1000...0111...$$

Given appropriate additional assumptions, such sequences consisting of long stretches of record 0's and 1's justify inference of the history of the system. Let us further assume that observer's records come from intercepting a small fragment of the environment. Other observers will be then able to consult their independently accessible environmental records, and will infer (more or less) the same history. Thus, in view of the "preponderance of evidence" history defined as a sensible inference from the available records can be probed by many independently, and can be regarded as classical and objective.

The redundancy ratio of the records $\mathcal{R}$ is a measure of this objectivity. Note that this *relatively objective existence* (Zurek, 1998a) is an operational notion, quantified by the number of times the state of the system can be found out independently, and not some "absolute objectivity". However, and in a sense that can be rigorously defined, relative objectivity tends

to absolute objectivity in the limit $\mathcal{R} \longrightarrow \infty$. For example, cloning of unknown states becomes possible (Bruss, Ekert, and Macchiavello, 1999, Jozsa, 2002) in spite of the "no cloning" theorem (Wootters and Zurek, 1982, Dieks 1982). In that limit, and given same reasonable constraints on the nature of the interactions and on the structure of the environment which underlie the definition of $\mathcal{R}$, it would take infinite resources such as action, Eqs. (7.5) - (7.9), to hide or subvert evidence of such an objective history.

There are differences and parallels between relatively objective histories introduced here and consistent histories proposed by Griffiths (1984, 1996), and investigated by Gell-Mann and Hartle (1990; 1993; 1997), Omnès (1988; 1992; 1994), Halliwell (1999), and others (Dowker and Kent, 1996; Kiefer, 1996). Such histories are defined as time-ordered sequences of projection operators $P^1_{\alpha_1}(t_1), P^2_{\alpha_2}(t_2), \ldots, P^n_{\alpha_n}(t_n)$ and are abbreviated $[P_\alpha]$. Consistency is achieved when they can be combined into coarse grained sets (where the projectors defining coarse - grained set are given by sums of the projectors in the original set) while obeying probability sum rules: Probability of a bundle of histories should be a sum of the probabilities of the constituent histories. The corresponding condition can be expressed in terms of the *decoherence functional* (Gell-Mann and Hartle, 1990);

$$D([P_\alpha],[P_\beta]) = Tr\left((P^n_{\alpha_n}(t_n)\ldots P^1_{\alpha_1}(t_1)\rho P^1_{\beta_1}(t_1)\ldots P^n_{\beta_n}(t_n)\right) \tag{7.21}$$

Above, the state of the system of interest is described by the density matrix ρ. Griffiths' condition is equivalent to the vanishing of the real part of the expression above, $Re\{D([P_\alpha],[P_\beta]\} = p_\alpha\delta_{\alpha,\beta}$. As Gell-Mann and Hartle (1990) emphasize, it is more convenient – and in the context of and emergent classicality more realistic – to demand instead $D([P_\alpha],[P_\beta]) = p_\alpha\delta_{\alpha,\beta}$. Both weaker and stronger conditions for the consistency of histories were considered (Goldstein and Page, 1995; Gell-Mann and Hartle, 1997). The problem with all of them is that the resulting histories are very subjective: Given an initial density matrix of the Universe it is in general quite easy to specify many different, mutually incompatible consistent sets of histories. This subjectivity leads to serious interpretational problems (d'Espagnat, 1989; 1995; Dowker and Kent, 1996). Thus, a demand for exact consistency as one of the conditions for classicality is both uncomfortable (overly restrictive) and insufficient (as the resulting histories are very non-classical). Moreover, coarse-grainings that help secure approximate consistency have to be, in effect, guessed.

The attitudes adopted by the practitioners of the consistent histories approach in view of its unsuitability for the role of the cornerstone of the emergent classicality differ. Initially – before difficulties became apparent – it was hoped that such approach would answer all of the interpretational questions, perhaps when supplemented by a subsidiary condition, i.e. some assumption about favored coarse-grainings. At present, some still aspire to the original goals of deriving classicality from consistency alone. Others may uphold the original aims of the program, but they also generally rely on environment-induced decoherence, using in calculations variants of models we have presented in this paper. This strategy has been quite successful – after all, decoherence leads to consistency. For instance, special role of the hydrodynamic observables (Gell-Mann and Hartle, 1990; Dowker and Halliwell, 1992; Halliwell, 1999; Brun and Hartle, 1999) can be traced to their predictability, or to their approximate commutativity with the total Hamiltonian (see Eq. (4.41)). On the other hand, the original goals of Griffiths (1984, 1996) have been more modest: Using consistent histories, one can discuss sequences of events in an evolving quantum system without logical contradictions. The "golden middle" is advocated by Griffiths and Omnès (1999) who regard consistent histories as a convenient language, rather than as an explanation of classicality.

The origin of the effective classicality can be traced to decoherence and einselection. As was noted by Gell-Mann and Hartle (1990), and elucidated by Omnès (1992; 1994) decoherence suffices to ensure approximate consistency. But consistency is both not enough and too much

– it is too easy to accomplish, and does not necessarily lead to classicality (Dowker and Kent, 1996). What is needed instead is the objectivity of events and their time-ordered sequences – histories. As we have seen above, both can appear as a result of einselection.

Relatively Objective Past

We have already provided an operational definition of relatively objective existence of quantum states. It is easy to apply it to events and histories: When many observers can independently gather compatible evidence concerning an event, we call it *relatively objective*. Relatively objective history is then a time-ordered sequence of relatively objective events.

Monitoring of the system by the environment leads to decoherence and einselection. It will also typically lead to redundancy and hence effectively objective classical existence in the sense of 'quantum Darwinism'. Observers can independently access redundant records of events and histories imprinted in the environmental degrees of freedom. The number of observers who can examine evidence etched in the environment can be of the order of, and is bounded from above by $\mathcal{R}_{\mathcal{J}}$. Redundancy is a measure of this objectivity and classicality.

As observers record their data, $\mathcal{R}_{\mathcal{J}}$ changes: Consider an observer who measures the 'right observable' of $\mathcal{E}$ (i.e., the one with the eigenstates $|0\rangle, |1\rangle$ in the example of Eq. (7.1)). Then his records and – as his records decohere, their environment – become a part of evidence, and are correlated with the preferred basis of the system. Consequently, $\mathcal{R}_{\mathcal{J}}$ computed from Eq. (7.14) increases. Every interaction that increases the number of the records also increases $\mathcal{R}_{\mathcal{J}}$. This is obvious for the "primary" interactions with the system, but it is also true for the secondary, tertiary, etc. acts of replication of the information obtained from the observers who recorded primary state of the system, from the environment, from the environment of the environment, and so on.

A measurement reveals to the observer "his" branch of the universal state vector. The correlations established alter observer's state – his records – and "attach" him to this branch. He will share it with other observers who examined the same set of observables, and who have recorded compatible results.

It is also possible to imagine a stubborn observer who insists on measuring either the relative phase between the two obvious branches of the environment in Eq. (7.2), or the state of the environment in the Hadamard-transformed basis $\{|+\rangle, |-\rangle\}$. In either case the distinction between the two outcomes could determine the state of the spin in the $\{|\odot\rangle, |\otimes\rangle\}$ basis. However, in that basis $\mathcal{R}_{\mathcal{J}} = 1$. Hence, while in principle these measurements can be carried out and yield the correct result, the information concerning $\{|\odot\rangle, |\otimes\rangle\}$ basis is not redundant, and, therefore, not objective: Only one stubborn observer can access it directly. As a result $\mathcal{R}_{\mathcal{J}}$ will decrease. Whether the $\mathcal{R}_{\mathcal{J}}(\{|\odot\rangle, |\otimes\rangle\})$ will become larger than $\mathcal{R}_{\mathcal{J}}(\{|\uparrow\rangle, |\downarrow\rangle\})$ was before the measurement of the stubborn observer will depend on detailed comparison of the initial redundancy with the amplification involved, decoherence, etc.

There is a further significant difference between the two stubborn observers considered above. When the observer measures the phase between the two sequences of 0's and 1's in Eq. (7.2), correlations between the bits of the environment remain. Thus, even after his measurement one could find relatively objective evidence of the past event – past state of the spin – and, in more complicated cases, of the history. On the other hand, measurement of all the environment bits in the $\{|+\rangle, |-\rangle\}$ basis will obliterate evidence of such a past.

Relatively objective existence of events is the strongest condition we have considered here. It is a consequence of the existence of multiple records of the same set of states of the system. It allows for such manifestations of classicality as unimpeded cloning. It implies einselection of states most closely monitored by the environment. Decoherence is clearly weaker and easier to accomplish.

"The past exists only insofar as it is recorded in the present" (dictum often repeated by

Wheeler) may the best summary of the above discussion. Relatively objective reality of few selected observables in our familiar Universe is measured by their fitness – by the redundancy with which they are recorded in the environment. This multiplicity of available copies of the same information can be regarded as a consequence of amplification, and as a cause of indelibility. Multiple records safeguard objectivity of our past.

21.8 Decoherence in the Laboratory

The biggest obstacle in the experimental study of decoherence is – paradoxically – its effectiveness. In the macroscopic domain only the einselected states survive. Their superpositions are next to impossible to prepare. In the mesoscopic regime one may hope to adjust the size of the system, and, thus, interpolate between quantum and classical. The strength of the coupling to the environment is the other parameter one may employ to control the decoherence rate.

One of the key consequences of monitoring by the environment is the inevitable introduction of the Heisenberg uncertainty into the observable complementary to the one that is monitored. One can *simulate* such uncertainty without any monitoring environment by introducing classical noise. In each specific run of the experiment – for each realization of time-dependent noise – quantum system will evolve deterministically. However, after averaging over different noise realizations evolution of the density matrix describing an *ensemble* of systems may approximate decoherence due to an entangling quantum environment. In particular, the master equation may be essentially the same as for true decoherence, although the interpretational implications are more limited. Yet, using such strategies one can simulate much of the dynamics of open quantum systems.

The strategy of simulating decoherence can be taken further: Not just the effect of the environment, but also the dynamics of the quantum system can be simulated by classical means. This can be accomplished when classical wave phenomena follow equations of motion related to Schrödinger equation. We shall discuss experiments that fall into all of the above categories.

Last not least, while decoherence – through einselection – helps solve the measurement problem, it is also a major obstacle to quantum information processing. We shall thus end this section briefly describing strategies that may allow one to tame decoherence.

21.8.1 Decoherence due to entangling interactions

Several experiments fit this category, and more have been proposed. Decoherence due to emission or scattering of photons has been investigated by the MIT group (Chapman et al., 1995; Kokorowski et al., 2001) using atomic interferometry. Emission or scattering deposits a record in the environment. It can store information about the path of the atom providing photon wavelength is shorter than the separation between the two of the atoms. In case of emission this record is not redundant, as the atom and photon are simply entangled – $\mathcal{R}_{\mathcal{J}} \sim 1$ in any basis. Scattering may involve more photons, and the recent careful experiment has confirmed the saturation of decoherence rate at distances in excess of photon wavelength (Gallis and Fleming, 1990; Anglin, Paz, and Zurek, 1997).

There is an intimate connection between interference and complementarity in the two-slit experiment on one hand, and the entanglement on the other (Wootters and Zurek, 1979). Consequently, appropriate measurements of the photon allow one to restore interference fringes in the conditional subensembles corresponding to a definite phase between the two photon trajectories (see especially Chapman et al. (1995), as well as Kwiat, Steinberg and Chiao (1993); Pfau et al., 1994; Herzog, Kwiat, Weinfurter and Zeilinger, (1995) for implementations of this "quantum erasure" trick due to Hillery and Scully (1983)). Similar experiments have

been also carried out using neutron interferometry (see e.g. Rauch, (1998)).

In all of these experiments one is dealing with a very simplified situation involving a single microsystem and a single "unit" of decoherence ($\mathcal{R}_\mathcal{J} \sim 1$) caused by a single quantum of the environment. Experiments on a mesoscopic system monitored by the environment are obviously much harder to devise. Nevertheless, Sergé Haroche, Jean-Michel Raimond, Michel Brune and their colleagues (Brune et al., 1996; Haroche 1998, Raimond, Brune, and Haroche, 2001) have carried out a spectacular experiment of this type, yielding solid evidence in support of the basic tenets of the environment-induced transition from quantum to classical. Their system is a microwave cavity. It starts in a coherent state with an amplitude corresponding to a few photons.

"Schrödinger cat" is created by introducing an atom in a superposition of two Rydberg states, $|+\rangle = |0\rangle + |1\rangle$: The atom passing through the cavity puts its refractive index in a superposition of two values. Hence, the phase of the coherent state shifts by the amount correlated with the state of the atom, creating an entangled state:

$$|\rightarrow\rangle(|0\rangle + |1\rangle) \implies |\nearrow\rangle|0\rangle + |\searrow\rangle|1\rangle = |\vartheta\rangle \tag{8.1}$$

Arrows indicate relative phase space locations of coherent states. States of the atom are $|0\rangle$ and $|1\rangle$. "Schrödinger kitten" is prepared from this entangled state by measuring the atom in the $\{|+\rangle, |-\rangle\}$ basis:

$$|\vartheta\rangle = (|\nearrow\rangle + |\searrow\rangle)|+\rangle + (|\nearrow\rangle - |\searrow\rangle)|-\rangle \tag{6.2}$$

Thus, atom in the state $|+\rangle$ implies preparation of a "positive cat" $|\uplus\rangle = |\nearrow\rangle + |\searrow\rangle$ in the cavity. Such superpositions of coherent states could survive forever if there was no decoherence. However, radiation leaks out of the cavity. Hence, environment acquires information about the state inside. Consequences are tested by passing another atom in the state $|+\rangle = |0\rangle + |1\rangle$ through the cavity. In absence of decoherence the state would evolve as:

$$\begin{aligned} |\uplus\rangle|+\rangle \;&=\; (|\nearrow\rangle + |\searrow\rangle)(|0\rangle + |1\rangle) \Longrightarrow \\ (|\uparrow\rangle|0\rangle + |\rightarrow\rangle|1\rangle) \;&+\; (|\rightarrow\rangle|0\rangle + |\downarrow\rangle|1\rangle) \\ = (|\uparrow\rangle|0\rangle + |\downarrow\rangle|1\rangle) &+ \sqrt{2}|\rightarrow\rangle|+\rangle \;. \qquad 8.3 \end{aligned} \tag{21.61}$$

Above we have omitted the overall normalization, but retained the (essential) relative amplitude.

For the above state detection of $|+\rangle$ in the first (preparatory) atom implies the conditional probability of detection of $|+\rangle$, $p_{+|+} = \frac{3}{4}$, for the second (test) atom. Decoherence will suppress off-diagonal terms of the density matrix, so that, some time after the preparation, ρ_{cavity} that starts, say, as $|\uplus\rangle\langle\uplus|$ becomes:

$$\begin{aligned} \rho_{cavity} \;&=\; (|\nearrow\rangle\langle\nearrow| + |\searrow\rangle\langle\searrow|)/2 \\ &+\; z(|\nearrow\rangle\langle\searrow| + |\searrow\rangle\langle\nearrow|)/2 \;. \qquad 8.4 \end{aligned} \tag{21.62}$$

When $z = 0$ the conditional probability is $p(+|+) = \frac{1}{2}$.

In the intermediate cases intermediate values of this and other relevant conditional probabilities are predicted. The rate of decoherence, and, consequently, the time-dependent value of z can be estimated from the cavity quality factor Q, and from the data about the coherent state initially present in the cavity. Decoherence rate is a function of separation of the two components of the cat $|\uplus\rangle$. Experimental results agree with predictions.

The discussion above depends on the special role of coherent states. Coherent states are einselected in harmonic oscillators, and, hence, in the underdamped bosonic fields (Anglin and Zurek, 1996). Thus, they are the pointer states of the cavity. Their special role is recognized implicitly above: If number eigenstates were einselected, predictions would be obviously quite

different. Therefore, while the ENS experiment is focused on decoherence rate, confirmation of the predicted special role of coherent states in bosonic fields is its important (albeit implicit) corollary.

21.8.2 Simulating decoherence with classical noise

>From the fundamental point of view, the distinction between cases when decoherence is caused by entangling interactions with the quantum state of the environment and when it is simulated by a classical noise in the observable complementary to the "pointer" is essential. However, from the engineering point of view (adopted, e.g., by the practitioners of quantum computation, see Nielsen and Chuang, 2000 for discussion) this may not matter. For instance, quantum error correction techniques (Shor, 1995; Steane, 1996; Preskill, 1999) are capable of dealing with either. Moreover, experimental investigations of this subject often involve both.

The classic experiment in this category was carried out recently by David Wineland, Chris Monroe, and their collaborators (Myatt et al, 2000; Turchette et al., 2000). They use ion trap to study behavior of individual ions in a "Schrödinger cat" state (Monroe et al., 1996) under the influence of injected classical noise. They also embark on a preliminary study of "environment engineering".

Superpositions of two coherent states as well as of number eigenstates were subjected to simulated high temperature amplitude and phase "reservoirs". This was done through time-dependent modulation of the self-Hamiltonian of the system. For the amplitude noise these are in effect random fluctuations of the location of the minimum of the harmonic trap. Phase noise corresponds to random fluctuations of the trap frequency.

In either case, the resulting loss of coherence is well described by the exponential decay with time, with the exponent that scales with the square of the separation between the two components of the macroscopic quantum superposition (e.g., Eq. (5.34)). The case of the amplitude noise approximates decoherence in quantum Brownian motion in that the coordinate is monitored by the environment, and, hence, the momentum is perturbed. (Note that in the underdamped harmonic oscillator rotating wave approximation blurs the distinction between x and p, leading to einselection of coherent states.) The phase noise would arise in an environment monitoring the number operator, thus leading to uncertainty in phase. Consequently, number eigenstates are einselected.

The applied noise is classical, and the environment does not acquire any information about the ion ($\mathcal{R}_{\mathcal{I}} = 0$). Thus, following a particular realization of the noise the state of the system is still pure. Nevertheless, an ensemble average over many noise realizations is represented by the density matrix that follows an appropriate master equation. Thus, as Wineland, Monroe, and their colleagues note, decoherence simulated by the classical noise could be in each individual case – for each realisation – reversed by simply measuring the corresponding time-dependent noise run either beforehand or afterwards, and then applying the appropriate unitary transformation to the state of the system. By contrast, in the case of entangling interactions, two measurements – one preparing the environment before the interaction with the environment, the other following it – would be the least required for a chance of undoing the effect of decoherence.

The same two papers study decay of a superposition of number eigenstates $|0\rangle$ and $|2\rangle$ due to an indirect coupling with the vacuum. This proceeds through entanglement with the first order environment (that, in effect, consists of the other states of the harmonic oscillator) and a slower transfer of information to the distant environment. Dynamics involving the system and its first - order environment leads to non-monotonic behavior of the off-diagonal terms representing coherence. Further studies of decoherence in the ion trap setting are likely to follow, as this is an attractive implementation of the quantum computer (Cirac and Zoller, 1995).

Decoherence, Noise, and Quantum Chaos

Following a proposal of Graham, Schlautmann, and Zoller (1993) Mark Raizen and his group (Moore et al., 1994) used a one-dimensional optical lattice to implement a variety of 1-D chaotic systems including the "standard map". Various aspects of the behavior expected from a quantized version of a classically chaotic system were subsequently found, including, in particular, dynamical localization (Casati and Chirikov, 1995a; Reichl, 1992).

Dynamical localization establishes, in a class of driven quantum chaotic systems, a saturation of momentum dispersion, and leads to a characteristic exponential form of its distribution (Casati and Chirikov, 1995a). Localization is obviously a challenge to the quantum-classical correspondence, since in these very same systems classical prediction has the momentum dispersion growing unbounded, more or less with the square root of time. However, it sets in after $t_L \sim \hbar^{-\alpha}$, where $\alpha \sim 1$ (rather than on the much shorter $t_\hbar \sim \ln \hbar^{-1}$ we have discussed in Section III) so it can be ignored for macroscopic systems. On the other hand, its signature is easy to detect.

Demonstration of dynamical Anderson localization in the optical lattice implementation of the δ-kicked rotor and related studies of quantum chaos are a significant success (Moore et al., 1994). More recently, attention of both Raizen and his group in Texas as well as of Christensen and his group in New Zealand has shifted towards the effect of decoherence on quantum chaotic evolution (Ammann et al, 1998; Klappauf et al., 1998).

In all of the above studies the state of the chaotic system (δ-kicked rotor) was perturbed by spontaneous emission from the trapped atoms, that was induced by decreasing detuning of the lasers used to set up the optical lattice. In addition, noise was occasionally introduced into the potential. Both groups find that, as a result of spontaneous emission, localization disappears, although the two studies differ in some of the details. More experiments, including some that allow gentler forms of monitoring by the environment (rather than spontaneous emission noise) appear to be within reach.

In all of the above cases one deals, in effect, with a large ensemble of identical atoms. While each atom suffers repeated disruptions of its evolution due to spontaneous emission, the ensemble evolves smoothly and in accord with the appropriate master equation. The situation is reminiscent of the "decoherence simulated by noise".

Experiments that probe the effect of classical noise on chaotic systems have been carried out earlier (Koch, 1995). They were, however, analyzed from the point of view that does not readily shed light on decoherence.

A novel experimental approach to decoherence and to irreversibility in open complex quantum systems is pursued by Levstein, Pastawski, and their colleagues (Levstein, Usaj, and Pastawski, 1998; Levstein et al., 2000). Using NMR techniques the investigate reversibility of dynamics by implementing a version of spin echo. This promising "Loschmidt echo" approach has led to renewed interest in the issues that touch on quantum chaos, decoherence, and related subjects (see e.g., Gorin and Seligman, 2001; Prosen, 2001; Jalabert and Pastawski, 2001; Jacquod, Silvestrov and Beenakker, 2001).

21.8.3 Analogue of decoherence in a classical system

Both the system and the environment are effectively classical in the last category of experiments, represented by the work of Cheng and Raymer (1999). They have investigated behavior of transverse spatial coherence during the propagation of the optical beam through a dense, random dielectric medium. This problem can be modelled by a Boltzmann-like transport equation for the Wigner function of the wave field, and exhibits characteristic increase of decoherence rate with the square of the spatial separation, followed by a saturation at sufficiently large distances. This saturation contrasts with the simple models of decoherence in quantum Brow-

nian motion that are based on dipole approximation. However, it is in good accord with the more sophisticated discussions which recognize that, for separations of the order of the prevalent wavelength in the environment, dipole approximation fails and other more complicated behaviors can set in (Gallis and Fleming, 1990; Anglin, Paz and Zurek, 1997; Paz and Zurek, 1999). Similar result in a completely quantum case was obtained using atomic interferometry by Kokorowski et al. (2001).

21.8.4 Taming decoherence

In many of the applications of quantum mechanics the quantum nature of the information stored or processed needs to be protected. Thus, decoherence is an enemy. Quantum computation is an example of this situation. Quantum computer can be thought of as a sophisticated interference device that works by performing in parallel a coherent superposition of a multitude of classical computations. Loss of coherence would disrupt this quantum parallelism essential for the expected speedup.

In the absence of the ideal – completely isolated absolutely perfect quantum computer, something easy for a theorist to imagine but impossible to attain in the laboratory – one must deal with imperfect hardware "leaking" some of its information to the environment. And maintaining isolation while simultaneously achieving a reasonable "clock time" for the quantum computer is likely to be difficult since both are in general controlled by the same interaction (although there are exceptions – for example, in the ion trap proposal of Cirac and Zoller (1995) interaction is in a sense "on demand", and is turned on by the laser coupling internal states of ions with the vibrational degree of freedom of the ion chain).

The need for error correction in quantum computation was realized early on (Zurek, 1984b) but methods for accomplishing this goal have evolved dramatically from the Zeno effect suggested then to very sophisticated (and much more effective) strategies in the recent years. This is fortunate: Without error correction even fairly modest quantum computations (such as factoring number 15 in an ion trap with imperfect control of the duration of laser pulses) go astray rapidly as a consequence of relatively small imperfections (Miquel, Paz, and Zurek, 1997).

Three different, somewhat overlapping approaches that aim to control and tame decoherence, or to correct errors caused by decoherence or by the other imperfections of the hardware have been proposed. We summarize them very briefly, spelling out main ideas and pointing out references that discuss them in greater detail.

Pointer states and noiseless subsystems

The most straightforward strategy to suppress decoherence is to isolate the system of interest (e.g., quantum computer). Failing that, one may try to isolate some of its observables with degenerate pointer subspaces, which then constitute niches in the Hilbert space of the information processing system that do not get disrupted in spite of its the coupling to the environment. Decoherence free subspaces (DFS's for brevity) are thus identical in conception with the pointer subspaces introduced some time ago (Zurek, 1982), and satisfy (exactly or approximately) the same Eqs. (4.22) and (4.41) or their equivalents (given, e.g., in terms of "Krauss operators" (Krauss, 1983)) that represent non-unitary consequences of the interaction with the environment in the Lindblad (1976) form of the master equation). DFS's were (re)discovered in the context of quantum information processing. They appear as a consequence of an exact or approximate symmetries of the Hamiltonians that govern the evolution of the system and its interaction with the environment (Zanardi and Rasetti, 1997; Duan and Guo, 1998; Lidar et al., 1998; Zanardi, 1998; 2000).

An active extension of this approach aimed at finding quiet corners of the Hilbert space is known as dynamical decoupling. There the effectively decoupled subspaces are induced by time-

dependent modifications of the evolution of the system deliberately introduced from the outside by time-dependent evolution and / or measurements (see e.g. Viola and Lloyd, 1998; Zanardi, 2000). A further generalization and unification of various techniques leads to the concept of noiseless quantum subsystems (Knill, Laflamme, and Viola, 1999; Zanardi, 2000), which may be regarded as a non-abelian (and quite non-trivial) generalization of pointer subspaces.

A sophisticated and elegant strategy that can be regarded as a version of the decoherence free approach was devised independently by Kitaev (1997a, b). He has advocated using states that are topologically stable, and, thus, that can successfully resist arbitrary interactions with the environment. The focus here (in contrast to much of the DFS work) is on devising a system with self-Hamiltonian that – as a consequence of the structure of the gap its energy spectrum related to the "cost" of topologically non-trivial excitations – acquires a subspace *de facto* isolated from the environment. This approach has been further developed by Bravyi and Kitaev (1998) and by Freedman and Meyer (1998).

Environment engineering

This strategy involves altering the (effective) interaction Hamiltonian between the system and the environment or influencing the state of the environment to selectively suppress decoherence. There are many ways to implement it, and we shall describe under this label variety of proposed techniques (some of which are not all that different from the strategies we have just discussed) that aim to protect quantum information stored in selected subspaces of the Hilbert space of the system, or even to exploit pointer states induced or redefined in this fashion.

The basic question that started this line of research – can one influence the choice of the preferred pointer states? – arose in the context of ion trap quantum computer proposed by Cirac and Zoller (1995). The answer given by the theory is, of course, that the choice of the einselected basis is predicated on the details of the situation, and, in particular, on the nature of the interaction between the system and the environment (Zurek, 1981; 1982; 1993a). Yet, Poyatos, Cirac and Zoller (1996) have suggested a scheme suitable for implementation in an ion trap, where interaction with the environment – and, in accord with Eq. (4.41), the pointer basis itself – can be adjusted. The key idea is to recognize that the effective coupling between the vibrational degrees of freedom of an ion (the system) and the laser light (which plays the role of the environment) is given by:

$$H_{int} = \frac{\Omega}{2}(\sigma_+ e^{-i\omega_L t} + \sigma_- e^{i\omega_L t}) \sin[\kappa(a + a^+) + \phi] \ . \tag{8.5}$$

Above, Ω is the Rabi frequency, ω_L the laser frequency, ϕ is related to the relative position of the center of the trap with respect to the laser standing wave, κ is the Lamb-Dicke parameter of the transition, while σ_- (σ_+) and a (a^+) are the annihilation (creation) operators of the atomic transition and of the harmonic oscillator (trap).

By adjusting ϕ and ω_L and adopting appropriate set of approximations (that include elimination of the internal degrees of freedom of the atom) one is led to the master equation for the system – i.e, for the density matrix of the vibrational degree of freedom:

$$\dot{\rho} \ = \ \gamma(2f\rho f^+ - f_+ f\rho - \rho f_+ f) \tag{8.6}$$

Above, f is the operator with a form that depends on the adjustable parameters ϕ and ω_L in H_{int}, while γ is a constant that depends also on Ω and η. As Poyatos et al. show, one can alter the effective interaction between the slow degree of freedom (the oscillator) and the environment (laser light) by adjusting parameters of the actual H_{int}.

First steps towards realization of this "environment engineering" proposals were taken by the NIST group (Myatt et al., 2000; Turchette et al., 2000). Similar techniques can be employed to protect deliberately selected states from decoherence (Carvalho et al., 2000).

Other ideas aimed at channeling decoherence have been also explored in contexts that range from quantum information processing (Beige et al., 2000) to preservation of Schrödinger cats in Bose-Einstein condensates (Dalvit, Dziarmaga, and Zurek, 2000).

Error correction and resilient computing

This strategy is perhaps most sophisticated and comprehensive, and capable of dealing with the greatest variety of errors in a most hardware - independent manner. It is a direct descendant of the error correction techniques employed in dealing with the classical information, based on redundancy: Multiple copies of the information are made, and the errors are found and corrected by sophisticated "majority voting' techniques.

One might have thought that implementing error correction in the quantum setting will be difficult for two reasons. To begin with, quantum states – and, hence, quantum information – cannot be "cloned" (Dieks, 1982; Wootters and Zurek, 1982). Moreover, quantum information is very "private", and a measurement that is involved in majority voting would infringe on this privacy and destroy quantum coherence, making quantum information classical. Fortunately, both of these difficulties can be simultaneously overcome by encoding quantum information in entangled states of several qubits. Cloning turns out not to be necessary. And measurements can be carried out in a way that identifies errors while keeping quantum information untouched. Moreover, error correction is *discrete* – measurements that reveal error syndromes have "yes - no" outcomes. Thus, even though information stored in a qubit represents a continuum of possible quantum states (e.g., corresponding to a surface of the Bloch sphere) error correction is discrete, allaying one of the earliest worries concerning the feasibility of quantum computation – the unchecked "drift" of the quantum state representing information (Landauer, 1995).

This strategy (discovered by Shor (1995) and Steane (1996)) has been since investigated by many (Ekert and Macchiavello, 1996; Bennett et al., 1996; Laflamme et al., 1996) and codified into a mathematically appealing formalism (Gottesman, 1996; Knill and Laflamme, 1997). Moreover, first examples of successful implementation (see e.g. Cory et al., 1999) are already at hand.

Error correction allows one, at least in principle, to compute forever, providing that the errors are suitably small ($\sim 10^{-4}$ per computational step seems to be the error probability threshold sufficient for most error correction schemes). Strategies that accomplish this encode qubits in already encoded qubits (Aharonov and Ben-Or 1997; Kitaev 1997c; Knill, Laflamme and Zurek, 1996; 1998a, b; Preskill 1998). The number of layers of such concatenation necessary to achieve fault tolerance – the ability to carry out arbitrarily long computations – depends on the size (and the character) of the errors, and on the duration of the computation, but when error probability is smaller than the threshold, that number of layers is finite. Overviews of fault tolerant computation are already at hand (Preskill, 1999; Nielsen and Chuang, 2000, and references therein).

An interesting subject related to the above discussion is quantum process tomography, anticipated by Jones (1994), and described in the context of quantum information processing by Chuang and Nielsen (1997) and by Poyatos, Cirac and Zoller (1997). The aim here is to characterize completely a process – such as a quantum logical gate – and not just a state. First deliberate implementation of this procedure (Nielsen, Knill, and Laflamme, 1998) has also demonstrated experimentally that einselection is indeed equivalent to an unread measurement of the pointer basis by the environment, and can be regarded as such from the standpoint of applications (i.e., NMR teleportation in the example above).

21.9 Concluding Remarks

Decoherence, einselection, pointer states, and even predictability sieve have become familiar concepts to many in the past decade. The first goal of this paper was to review these advances and to survey, and – where possible, to address – the remaining difficulties. The second related aim was to "preview" the future developments. This has led to considerations involving information, as well as to the operational, physically motivated discussions of seemingly esoteric concepts such as objectivity. Some of the material presented (including the 'Darwinian' view of the emergence of objectivity through redundancy, as well as the discussion of envariance and probabilities) are rather new, and a subject of research, hence the word "preview" applies here.

New paradigms often take a long time to gain ground. Atomic theory of matter (which, until early XX century, was 'just an interpretation') is the case in point. Some of the most tangible applications and consequences of new ideas are difficult to recognize immediately. In the case of atomic theory, Brownian motion is a good example: Even when the evidence is out there, it is often difficult to decode its significance.

Decoherence and einselection are no exception. They have been investigated for about two decades. They are the only explanation of classicality that does not require modifications of quantum theory, as do the alternatives (Bohm, 1952; Leggett, 1980, 1988, 2002; Penrose, 1986, 1989; Holland, 1993; Goldstein, 1998; Pearle, 1976; 1993; Ghirardi, Rimini, and Weber, 1986; 1987, Gisin and Percival, 1992; 1993a-c). Ideas based on the immersion of the system in the environment have recently gained enough support to be described (by sceptics!) as "the new orthodoxy" (Bub, 1997). This is a dangerous characterization, as it suggests that the interpretation based on the recognition of the role of the environment is both complete and widely accepted. Neither is certainly the case.

Many conceptual and technical issues (such as what constitutes 'a system') are still open. As for the breadth of acceptance, "the new orthodoxy" seems to be an optimistic (mis-)characterization of decoherence and einselection, especially since this explanation of the transition from quantum to classical has (with very few exceptions) not made it to the textbooks. This is intriguing, and may be as much a comment on the way in which quantum physics has been taught, especially on the undergraduate level, as on the status of the theory we have reviewed and its level of acceptance among the physicists.

Quantum mechanics has been to date, by and large, presented in a manner that reflects its historical development. That is, Bohr's planetary model of atom is still often the point of departure, Hamilton-Jacobi equations are used to "derive" Schrödinger equation, and an oversimplified version of the quantum - classical relationship (attributed to Bohr, but generally not doing justice to his much more sophisticated views) with the correspondence principle, kinship of commutators and Poisson brackets, Ehrenfest theorem, some version of the Copenhagen interpretation, and other evidence that quantum theory is really not all that different from classical – especially when systems of interest become macroscopic, and all one cares about are averages – is presented.

The message seems to be that the there is really no problem and that quantum mechanics can be "tamed" and confined to the microscopic domain. Indeterminacy and double slit experiment are of course discussed, but to prove peaceful coexistence within the elbow room assured by the Heisenberg's principle and complementarity. Entanglement is rarely explored. This is quite consistent with the aim of the introductory quantum mechanics courses, which has been (only slightly unfairly) summed up by the memorable phrase "shut up and calculate". Discussion of measurement is either dealt with through models based on the CI "old orthodoxy", or not at all. An implicit (and sometime explicit) message is: Those who ask questions that do not lend themselves to an answer through laborious, preferably perturbative calculation are "philosophers", and should be avoided.

The above description is of course a caricature. But given that the calculational techniques

of quantum theory needed in atomic, nuclear, particle, or condensed matter physics are indeed difficult to master, and given that – to date – most of the applications had nothing to do with the nature of quantum states, entanglement, and such, the attitude of avoiding the most flagrantly quantum aspects of quantum theory is easy to understand.

Novel applications force one to consider questions about the information content, the nature of "the quantum", and the emergence of the classical much more directly, with a focus on states and correlations, rather than on the spectra, cross sections and the expectation values. Hence, problems that are usually bypassed will come to the fore: It is hard to brand Schrödinger cats and entanglement as "exotic" and make them a centerpiece of a marketable device. I believe that as a result decoherence will become a part of the textbook lore. Indeed, at the graduate level there are already some notable exceptions among monographs (Peres, 1993) and specialized texts (Walls and Milburn, 1994; Nielsen and Chuang, 2000).

Moreover, the range of subjects already influenced by decoherence and einselection – by the ideas originally motivated by the quantum theory of measurements – is beginning to extend way beyond its original domain. In addition to the atomic physics, quantum optics, and quantum information processing (which were all mentioned throughout this review) it stretches from material sciences (Karlsson, 1998; Dreismann, 2000), surface science, where it seems to be an essential ingredient explaining emission of electrons (Brodie, 1995; Durakiewicz et al., 2001) through heavy ion collisions (Krzywicki, 1993) to quantum gravity and cosmology (Zeh, 1986, 1988, 1992; Kiefer, 1987; Kiefer and Zeh, 1995; Halliwell, 1989; Brandenberger, Laflamme and Mijic, 1990; Barvinsky and Kamenshchik, 1990, 1995; Paz and Sinha, 1991, 1992; Castagnino et al., 1993, Mensky and Novikov, 1996). Given the limitations of space we have not done justice to most of these subjects, focusing instead on issues of principle. In some areas reviews already exist. Thus, Giulini et al. (1996) is a valuable collection of essays, where, for example, decoherence in field theories is addressed. Dissertation of Wallace (2002) offers a good (if somewhat philosophical) summary of the role of decoherence with a rathe different emphasis on similar field-theoretic issues. Conference proceedings edited by Blanchard et al. (2000) and, especially, an extensive historical overview of the foundation of quantum theory from the modern perspective by Auletta (2000) are also recommended. More specific technical issues with implications for decoherence and einselection have also been reviewed. For example, on the subject of master equations there are several reviews with very different emphasis including Alicki and Lendi (1987), Grabert, Schramm, and Ingold (1988), Namiki and Pascazio (1993), as well as – more recently – Paz and Zurek (2001). In some areas – such as atomic BEC's – the study of decoherence has only started (Anglin, 1997; Dalvit, Dziarmaga, and Zurek, 2001). In many situations (e.g, quantum optics) a useful supplement to the decoherence view of the quantum - classical interface is afforded by 'quantum trajectories' – a study of the state of the system inferred from the intercepted state of the environment (see Carmichael, 1993; Wiseman and Milburn, 1993; Gisin and Percival, 1993a-c). This approach "unravels" evolving density matrices of open systems into trajectories conditioned upon the measurement carried out on the environment, and may have – especially in quantum optics – intriguing connections with the "environment as a witness" point of view (see Dalvit, Dziarmaga, and Zurek, 2001). In other areas – such condensed matter – decoherence phenomena have so many variations and are so pervasive that a separate "decoherent review" may be in order, especially as intriguing experimental puzzles seem to challenge the theory (Mohanty and Webb, 1997; Kravtsov and Altshuler, 1999).

Physics of information and computation is a special case. Decoherence is obviously a key obstacle in the implementation of information processing hardware that takes advantage of the superposition principle. While we have not focused on quantum information processing, the discussion was often couched in the language inspired by the information theory. This is no accident: It is the belief of this author that many of the remaining gaps in our understanding of

quantum physics and its relation to the classical domain – such as the definition of systems, or the still mysterious details of the "collapse" – shall follow pattern of the "predictability sieve" and shall be expanded into new areas investigation by considerations that simultaneously elucidate nature of "the quantum" and of "the information".

Figure Captions

Fig. 1. Snapshots of the quantum ($\hbar = 0.16$) Wigner function (a-c) and the classical probability distribution in phase space (d) for the chaotic evolution generated from the same initial Gaussian by the Hamiltonian:

$$H \ = \ p^2/2m \ - \ \kappa \cos(x - l \sin t) \ + \ ax^2/2$$

For $m = 1$, $\kappa = 0.36$, $l = 3$ and $a = 0 - 0.01$ it exhibits chaos with Lyapunov exponent $\Lambda = 0.2$. Quantum (a) and classical (d) are obtained at the same instant $t = 20$. They exhibit some similarities (i.e., the shape of the regions of significant probability density, "ridges" in the topographical maps of (a) and (d)), but the difference – the presence of the interference patterns with $W(x, p)$ assuming negative values (marked with blue) is striking. Saturation of the size of the smallest patches is anticipated already at this early time, as the ridges of the classical probability density are narrower than in the corresponding quantum features. Saturation is even more visible in (c) taken at $t = 60$ and (d), $t = 100$ (note change of scale). Sharpness of the classical features makes simulations going beyond $t = 20$ unreliable, but quantum simulations can be effectivelly carried out much further, as the necessary resolution can be anticipated in advance from Eqs. (3.15) - (3.16).

Fig. 2. Difference between the classical and quantum average of the dispersion of momentum $\Delta^2 = \langle p^2 \rangle - \langle p \rangle^2$ is plotted in (a) for the same initial condition, but three different values of $\hbar$ in the model defined in Fig. 1, but with the parameter $a = 0$. The instant when the departure between the classical and quantum averages becomes significant varies with $\hbar$ in a manner anticipated from Eqs. (3.5) and (3.6) for the Ehrenfest time, as is seen in the inset. Figure (b) shows the behaviors for the same value of $\hbar$, but for four different initial conditions. Inset appears to indicate that the typical variance difference δ varies only logarithmically with $\hbar$, although the large error bars (tied to the large systematic changes of behavior for different initial conditions) preclude one from arriving at a firmer conclusion. (See Karkuszewski, Zakrzewski, and Zurek, 2002, for further details and discussion).

Fig. 3. Schematic representation of the effect of decoherence on the Bloch sphere. When the interaction with the environment singles out pointer states located on the poles of the Bloch sphere, pure states (which lie on its surface) will evolve towards the vertical axis. This classical core is a set of all the mixtures of the pointer states.

Fig. 4. Information transfer in a `c-not` caricature of measurement, decoherence, and decoherence with noise. Bit-by-bit measurement is shown on the top. It is the fundamental logical circuit used to represent decoherence affecting the apparatus. Note that the direction of the information flow in decoherence – from the decohering apparatus and to the environment – differs from the information flow associated with noise. In short, as a result of decoherence environment is perturbed by the state of the system. Noise is – by contrast – perturbation inflicted by the environment. Preferred pointer states are selected so as to minimize the effect of the environment – to minimize the number of `c-not`s pointing from the environment at the expense of these pointing towards it.

Fig. 5. Time-dependent coefficients of the perturbative master equation for quantum Brownian motion. The parameters used in these plots (where the time is measure in units of Ω^{-1}) are $\gamma/\Omega = 0.05$, $\Gamma/\Omega = 100$, $k_B T/\hbar\Omega = 10, 1, 0.1$. Plots on the right show the initial portion of the

plots on the left – the initial transient – illustrating its independence of temperature (although higher temperatures produce higher final values of the coefficients). Plots on the right show that the final values of the coefficients strongly depend on temperature, and that the anomalous diffusion is of importance only for very low temperatures.

Fig. 6. Evolution of the Wigner function of the decohering harmonic oscillator. Note the difference between the rate at which the interference term disappears for the initial superposition of two minimal uncertainty Gaussians in position and in momenta.

Fig. 7. Predictability sieve in action. The plot shows purity $Tr\rho^2$ for mixtures that have evolved from initial minimum uncertainty wavepackets with different squeeze parameters s in an underdamped harmonic oscillator with $\gamma/\omega = 10^{-4}$. Coherent states – which have the same spread in position as in momentum, $s = 1$ – are clearly most predictable.

Fig. 8. Snapshots of a chaotic system with a double-well potential: $H = p^2/2m + Ax^4 - Bx^2 + Cx\cos(ft)$. In the example discussed here $m = 1$, $A = 0.5$, $B = 10$, $f = 6.07$ and $C = 10$ yielding the Lyapunov exponent $\Lambda \approx 0.45$ (see Habib, Shizume, and Zurek, 1998). All figures were obtained after approximately eight periods of the driving force. The evolution started from the same minimum uncertainty Gaussian, and proceeded according to the quantum Moyal bracket (a), the Poisson bracket (b), and (c) the Moyal bracket with decoherence (constant $D = 0.025$ in Eq. (5.64)). In the quantum cases $\hbar = 0.1$, which corresponds to the area of the rectangle in the image of the Wigner function above. Interference fringes are clearly visible in (a), and the Wigner function shown there is only vaguely reminiscent of the classical probability distribution in (b). Even modest decoherence ($D = 0.25$ used to get (c) corresponds to coherence length $\ell_c = 0.3$) dramatically improves the correspondence between the quantum and the classical. The remaining interference fringes appear on relatively large scales, which implies small scale quantum coherence.

Fig. 9. Classical and quantum expectation values of position $\langle x \rangle$ as a function of time for an example of Fig. 8. Evolution started from a minimum uncertainty Gaussian. Noticeable discrepancy between the quantum and classical averages appears on a timescale consistent with the Ehrenfest time $t_\hbar$. Decoherence – even in modest doses – dramatically decreases differences between the expectation values.

Part VI
Experiments for Quantum Information Theory

22 Experimental Realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A New Violation of Bell's Inequalities by Aspect, Grangier, et al. (1981)

Abstract

The linear-polarization correlation of pairs of photons emitted in a radiative cascade of calcium has been measured. The new experimental scheme, using two-channel polarizers (i.e., optical analogs of Stern-Gerlach filters), is a straightforward transposition of Ein-stein-Podolsky-Rosen-Bohm gedankenexperiment. The present results, in excellent agreement with the quantum mechanical predictions, lead to the greatest violation of generalized Bell's inequalities ever achieved.

In the well-known Einstein-Podolsky-RosenBohm gedankenexperiment [1] (Fig. 1), a source emits pairs of spin- $\frac{1}{2}$ particles, in a singlet state (or pairs of photons in a similar nonfactorizing state). After the particles have separated, one performs correlated measurements of their spin components along arbitrary directions $\vec{a}$ and $\vec{b}$. Each measurement can yield two results, denoted

$$E(\vec{\mathrm{a}}, \vec{\mathrm{b}}) = P_{++}(\vec{\mathrm{a}}, \vec{\mathrm{b}}) + P_{--}(\vec{\mathrm{a}}, \vec{\mathrm{b}}) - P_{+-}(\vec{\mathrm{a}}, \vec{\mathrm{b}}) - P_{-+}(\vec{\mathrm{a}}, \vec{\mathrm{b}})$$

is the correlation coefficient of the measurements on the two particles. Bell [2] considered theories explaining such correlations as due to common properties of both particles of the same pair; adding a locality assumption, he showed that they are constrained by certain inequalities that are not always obeyed by the predictions of quantum mechanics. Such theories are called [3] "realistic local theories" and they lead to the generalized Bell's inequalities [4]

$$-2 \leqslant S \leqslant 2, \tag{2}$$

where

$$S = E(\vec{\mathrm{a}}, \vec{\mathrm{b}}) - E\left(\vec{\mathrm{a}}, \vec{\mathrm{b}}'\right) + E\left(\vec{\mathrm{a}}', \vec{\mathrm{b}}\right) + E\left(\vec{\mathrm{a}}', \vec{\mathrm{b}}'\right)$$

involves four measurements in four various orientations. On the other hand, for suitable sets of orientations, [4] the quantum mechanical predictions can reach the values $S = \pm 2\sqrt{2}$, in clear contradiction with (2): Quantum mechanics cannot be completed by an underlying structure such as "realistic local theories."

Several experiments with increasing accuracy have been performed, and they clearly favor quantum mechanics. [3,5] Unfortunately, none allowed a direct test using inequalities (2), since none followed the scheme of Fig. 1 closely enough. Some experiments were performed with pairs of pho-

± 1; for photons, a measurement along $\vec{a}$ yields the result +1 if the polarization is found parallel to $\vec{a}$, and -1 if the polarization is found perpendicular. For a singlet state, quantum mechanics predicts some correlation between such measurements on the two particles. Let us denote by $P_{\pm\pm}(\vec{\mathrm{a}}, \vec{\mathrm{b}})$ the probabilities of obtaining the result ± 1 along $\vec{a}$ (particle 1) and ± 1 along $\vec{b}$

(particle 2). The quantity
tons (or of protons). But no efficient analyzers are available at such energies, and the results that would have been obtained with ideal polarizers are deduced indirectly from Compton scattering experiments. The validity of such a procedure in the context of Bell's theorem has been criticized. [3,6]
There are also experiments with pairs of lowenergy photons emitted in atomic radiative cascades. True polarizers are available in the visible range. However, all previous experiments involved single-channel analyzers, transmitting one polarization ($\vec{a}$ or $\vec{b}$) and blocking the orthog-

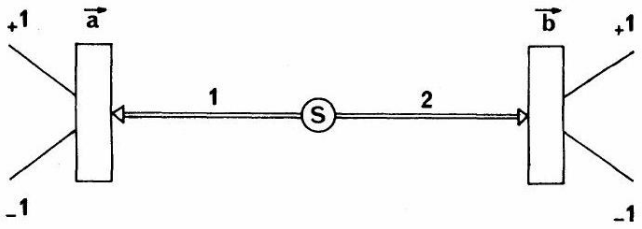


FIG. 1. Einstein-Podolsky-Rosen-Bohm gedankenexperiment. Two-spin- $\frac{1
{2}$ particles (or photons) in a singlet state (or similar) separate. The spin components (or linear polarizations) of 1 and 2 are measured along $\overrightarrow{\mathrm{a}}$ and $\overrightarrow{\mathrm{b}}$. Quantum mechanics predicts strong correlations between these measurements.}

onal one. The measured quantities were thus only the coincidence rates in $+1$ channels: $R_{++}(\overrightarrow{\mathrm{a}}, \vec{b})$. Several difficulties then arise [3] as a result of the very low efficiency of the detection system (the photomultipliers have low quantum efficiencies and the angular acceptance is small). The measurements of polarization are inherently incomplete: When a pair has been emitted, if no count is obtained at one of the photomultipliers, there is no way to know whether it has been missed by the (low-efficiency) detector or whether it has been blocked by the polarizer (only the latter case would be a real polarization measurement). Thus, coincidence counting rates such as $R_{+-}(\overrightarrow{\mathrm{a}}, \overrightarrow{\mathrm{b}})$ or $R_{--}(\overrightarrow{\mathrm{a}}, \overrightarrow{\mathrm{b}})$ cannot be measured directly. It is nevertheless possible to derive from the experimental data numerical quantities which can (according to quantum mechanics) possibly violate Bell-type inequalities. For this purpose, one has to resort to auxiliary experiments, where coincidence rates are measured with one or both polarizers removed. Some reasoning, with a few additional-and very natural -assumptions (such as the "no-enhancement" assumption of Clauser and Horne [7]), then allows one to obtain actually operational inequalities.
In this Letter, we report the results of an experiment following much more closely the ideal

scheme of Fig. 1. True dichotomic polarization measurements on visible photons have been performed by replacing ordinary polarizers by twochannel polarizers, separating two orthogonal linear polarizations, followed by two photomultipliers (Fig. 2). The polarization measurements then become very similar to usual SternGerlach measurements for spin- $\frac{1}{2}$ particles. [8]

Using a fourfold coincidence technique, we measure in a single run the four coincidence rates $R_{\pm\pm}(\overrightarrow{\mathrm{a}}, \overrightarrow{\mathrm{b}})$, yielding directly the correlation coefficient for the measurements along $\vec{a}$ and $\vec{b}$:

$$E(\overrightarrow{\mathrm{a}}, \overrightarrow{\mathrm{b}}) = \frac{R_{++}(\overrightarrow{\mathrm{a}}, \overrightarrow{\mathrm{b}}) + R_{--}(\overrightarrow{\mathrm{a}}, \overrightarrow{\mathrm{b}}) - R_{+-}(\overrightarrow{\mathrm{a}}, \overrightarrow{\mathrm{b}}) - R_{-+}(\overrightarrow{\mathrm{a}}, \overrightarrow{\mathrm{b}})}{R_{++}(\mathrm{a}, \mathrm{b}) + R_{--}(\mathrm{a}, \mathrm{b}) + R_{+-}(\mathrm{a}, \mathrm{b}) + R_{-+}(\mathrm{a}, \mathrm{b})}. \quad (3)$$

It is then sufficient to repeat the same measurements for three other choices of orientations, and inequalities (2) can directly be used as a test of realistic local theories versus quantum mechanics. This procedure is sound if the measured values (3) of the correlation coefficients

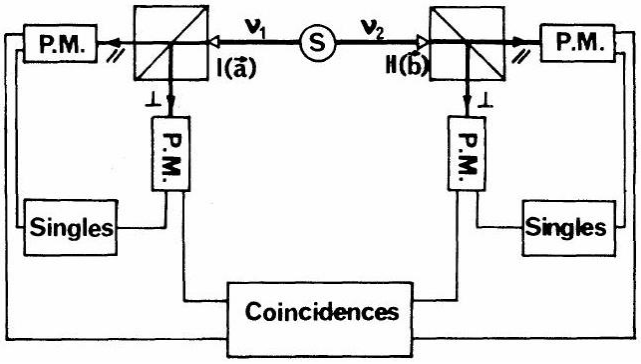


FIG. 2. Experimental setup. Two polarimeters I and II, in orientations $\overrightarrow{\mathrm{a}}$ and $\overrightarrow{\mathrm{b}}$, perform true dichotomic measurements of linear polarization on photons ν_1 and ν_2. Each polarimeter is rotatable around the axis of the incident beam. The counting electronics monitors the singles and the coincidences.}

can be taken equal to the definition (1), i.e., if we assume that the ensemble of actually detected pairs is a faithful sample of all emitted pairs. This assumption is highly reasonable with our very symmetrical scheme, where the two measurement results +1 and -1 are treated in the same way (the detection effiencies in both channels of a polarizer are equal). All data are collected in very similar experimental conditions, the only changes being rotations of the polarizers.
Such a procedure allows us not only to suppress possible systematic errors (e.g., changes occurring when removing the polarizers) but also to control more experimental parameters. For instance, we have checked that the sum of the coincidence rates of one photomultiplier with both
photomultipliers on the other side is constant. We have also observed that the sum of the four coincidence rates $R_{\pm\pm}(\overrightarrow{\mathrm{a}}, \overrightarrow{\mathrm{b}})$ is constant when changing the orientations; thus the size of the selected sample is found constant.
We have used the high-efficiency source previously described. [5] A $(J = 0) \rightarrow (J = 1) \rightarrow (J = 0)$ cas cade in calcium-40 is selectively excited by twophoton absorption, with use of two single-mode lasers. Pairs of photons (at wavelengths $\lambda_1 = 551.3$ nm and $\lambda_2 = 422.7$ nm) correlated in polarization are emitted at a typical rate of $5 \times 10^7 \mathrm{s}^{-1}$. The polarizers are polarizing cubes (Fig. 2) made of two prisms with suitable dielectric thin films on the sides stuck together; the faces are antirefelction coated. Cube I transmits light polarized in the incidence plane onto the active hypotenuse (parallel polarization, along $\vec{a}$) while it reflects the orthogonal polarization (perpendicular polarization). Cube II works similarly. For actual polarizers we define transmission and re-
flection coefficients: $T^{\|}$and $R^{\perp}$ are close to 1 , while $T^{\perp}$ and $R^{\|}$are close to 0 . The measured values of our devices are ${T_1}^I = {R_1}^I = 0.950$ and ${T_1}^{\perp} = {R_1}^{\mathrm{I}} = 0.007$ at λ_1; ${T_2}^{\mathrm{I}} = {R_2}^{\perp} = 0.930$ and ${T_2}^{\perp} = {R_2}'' = 0.007$ at λ_2 (all values are ± 0.005). Each polarizer is mounted in a rotatable mechanism holding two photomultipliers; we call the ensemble a polarimeter. The gains of the two photomultipliers are adjusted for the equality of the counting detection efficiencies in both channels of a polarimeter (2×10^{-3} at 422 nm, 10^{-3} at 551 nm). Typical single rates (over 10^4 s^{-1}) are high compared with dark rates (10^2 s^{-1}). Wavelength filters at 422 or 551 nm are mounted in front of each photomultiplier. The fourfold coincidence electronics includes four overlap-type coincidence circuits. Each coincidence window, about 20 ns wide, has been accurately measured. Since they are large compared to the lifetime of the intermediate state of the cascade (5 ns) all true coincidences are registered. We infer the accidental coincidence rates from the corresponding single rates, knowing the widths of the windows. This method is valid

with our very stable source, and it has been checked by comparing it with the methods of Ref. 5, using delayed coincidence channels and/or a time-to-amplitude converter. By subtraction of these accidental rates (about 10 s^{-1}) from the total rates, we obtain the true coincidence rates $R_{\pm\pm}(\vec{a}, \vec{b})$ (actual values are in the range $0 - 40$ s^{-1}, depending on the orientations). A run lasts 100 s , and $E(\vec{a}, \vec{b})$ derived from Eq. (3) is measured with a typical statistical accuracy of ± 0.02 (the sum of the four coincidence rates is typically 80 s^{-1}).
It is well known that the greatest conflict between quantum mechanical predictions and the inequalities (2) is expected for the set of orientations $(\vec{a}, \vec{b}) = \left(\vec{b}, \vec{a}'\right) = \left(\vec{a}', \vec{b}'\right) = 22.5°$ and $\left(\vec{a}, \vec{b}'\right) = 67.5°$. Five runs have been performed at each of these orientations; the average yields

$$S_{\text{expt}} = 2.697 \pm 0.015 \tag{4}$$

The indicated uncertainty is the standard deviation accounting for the Poisson law in photon counting. The impressive violation of inequalities (2) is 83% of the maximum violation predicted by quantum mechanics with ideal polarizers (the largest violation of generalized Bell's inequalities previously reported was 55% of the predicted violation in the ideal case [5]).
With symmetrical polarimeters, quantum mech-

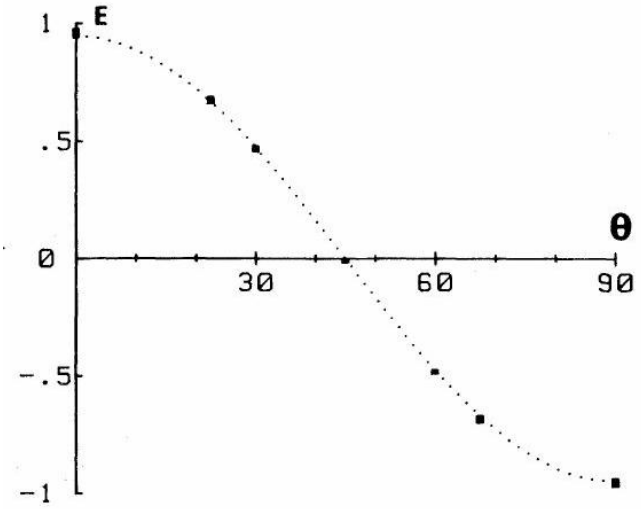


FIG. 3. Correlation of polarizations as a function of the relative angle of the polarimeters. The indicated errors are ± 2 standard deviations. The dotted curve is not a fit to the data, but quantum mechanical predictions for the actual experiment. For ideal polarizers, the curve would reach the values ± 1.

anics predicts

$$E(\vec{a}, \vec{b}) = F \frac{\left(T_1^{\parallel} - T_1^{\perp}\right)\left(T_2^{\parallel} - T_2^{\perp}\right)}{\left(T_1^{\parallel} + T_1^{\perp}\right)\left(T_2^{\parallel} + T_2^{\perp}\right)} \cos 2(\vec{a}, \vec{b}) \tag{5}$$

($F = 0.984$ in our case; it accounts for the finite solid angles of detection.) Thus, for our experiment,

$$S_{\text{QM}} = 2.70 \pm 0.05. \tag{6}$$

The indicated uncertainty accounts for a slight lack of symmetry between both channels of a polarimeter: We have found a variation of $\pm 1\%$ of the detection efficiencies when rotating the polarimeters. This spurious effect has been explained as small displacements of the light beam

impinging onto the photocathode. The effect of these variations on the quantum mechanical predictions has been computed, and cannot create a variation of S_{QM} greater than 2%.[9]

Figure 3 shows a comparison of our results with the predictions of quantum mechanics. Here, for each relative orientation $\theta = (\vec{a}, \vec{b})$, we have averaged several measurements in different absolute orientations of the polarimeters; this procedure averages out the effect of the slight variations of the detection efficiencies with orientation. The agreement with quantum mechanics is better than 1%.

In conclusion, our experiment yields the strongest violation of Bell's inequalities ever achieved, and excellent agreement with quantum mechanics. Since it is a straightforward transposition of the ideal Einstein-Podolsky -Rosen-Bohm scheme,
the experimental procedure is very simple, and needs no auxiliary measurements as in previous experiments with single-channel polarizers. We are thus led to the rejection of realistic local theories if we accept the assumption that there is no bias in the detected samples: Experiments support this natural assumption.
Only two loopholes remain open for advocates of realistic theories without action at a distance. [10] The first one, exploiting the low efficiencies of detectors, could be ruled out by a feasible experiment. [11] The second one, exploiting the static character of all previous experiments, could also be ruled out by a "timing experiment" with variable analyzers [12] now in progress.
The authors acknowledge many valuable discussions with F. Laloë about the principle of this experiment. They are grateful to C. Imbert who sponsors this work.

[1] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. 47, 777 (1935); D. J. Bohm, Quantum Theory (PrenticeHall, Englewood Cliffs, N.J., 1951).
[2] J. S. Bell, Physics (N.Y.) 1, 195 (1965).
[3] J. F. Clauser and A. Shimony, Rep. Prog. Phys. 41, 1981 (1978). This paper is an exhaustive review of this question.
[4] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. 23, 880 (1969).
[5] A. Aspect, P. Grangier, and G. Roger, Phys. Rev. Lett. 47, 460 (1981).
[6] M. Froissart, Nuovo Cimento B64, 241 (1981).
[7] J. F. Clauser and M. A. Horne, Phys. Rev. D 10, 526 (1974).
[8] Such an experimental scheme has been proposed and discussed by several authors: A. Shimony, in Foundations of Quantum Mechanics, edited by B. d'Espagnat (Academic, New York, 1972); F. Laloë, private communication; A. Garuccio and V. Rapisarda, Nuovo Cimento A65, 269 (1981); see also Ref. 7. A similar experiment has been undertaken by V. Rapisarda et al.
[9] Alternatively, this lack of symmetry can be taken into account in generalized Bell's inequalities similar to inequalities (2). (The demonstration will be published elsewhere.) In our case, the inequalities then become $|S| \leqslant 2.08$. The violation is still impressive.
[10] As in our previous experiments, the polarizers are separated by 13 m . The detection events are thus spacelike separated, and we eliminate the loophole considered by L. Pappalardo and V. Rapidarda, Lett. Nuovo Cimento 29, 221 (1980).
[11] T. K. Lo and A. Shimony, Phys. Rev. A 23, 3003 (1981).
[12] A. Aspect, Phys. Rev. D 14, 1944 (1976).

Part VII
Quantum Computing

(add from Nielson, Chang)

Part VIII
Creation of a Quantum Computer

(add from Nielson, Chang)

Part IX
Quantum Error Correction

(???? I'll write what is known about it)

Part X
Some Philosophical and Exotic Theories of Quantum Information

23 Quantum Theory and Measurement Edited by John Archibald Wheeler and Wojciech Hubert Zurek

23.0.1 Preface

Λ textbook on quantum theory and measurement does not exist, nor is this intended to be one. This is a reterence book, containing key papers on quantum theory as it relates to measurement. They are arranged in such a way, and accompanied by such supplementary references, that the collection can be used as a source book for a university course or seminar on the subject. It was so used by us in 1979-1980 and in 1980-1981 at the University of Texas. We have found that these materials are of interest to students and colleagues of all ages, not only in physics, but also in astronomy, philosophy, and mathematics.

We suppose that the reader already has some familiarity with quantum theory, preferably at least the equivalent of an undergraduate course in the subject.

Quantum theory has turned out to be the overarching principle of twentieth-century physics. It would be difficult to find a single subject among the physical sciences which is not affected in its foundations or in its applications by quantum theory. We may feel lost, to be sure, in the beginning stages of the study of the subject. Our supposed knowledge of a particle with its definite track through space and time dissolves into a wave, definiteness becomes indeterminism, and predictability of place is replaced by a predictability of the properties of nuclei, atoms, molecules, solids, liquids, and gases. We soon find ourselves armed with wonderful new tools. The more we use them, the more applications we find; and the more applications we find, the more uses of quantum theory we make.

Why there is no textbook on the measurement side of quantum theory is clear to anyone who participates in a seminar on the subject, and even clearer to one who gives a course on it: puzzlement! Beyond the probability interpretation of quantum mechanics, beyond all the standard analysis of idealized experiments, beyond the principle of indeterminacy and the limits it imposes, lie deep issues on which full agreement has not yet been reached in the physics community. They include questions like these: Does observation demand an irreversible act of amplification such as takes place in a grain of photographic emulsion or in the electron avalanche of a Geiger counter? And if so, what does one mean by "amplification"? And by "inteversible"? Does the quantum theory of observation apply in any meaningful way to the "whole universe"? Or is it restricted, even in principle, to the light cone? And if so, whose light cone? How are the observations made by different observers to be fitted into a single consistent picture in space-time? If these are some of the issues, they lead to other still deeper questions: What is the most productive meaning to assign to the term "reality"?

How are we to look at the subject, so mixed in its character, partly well-understood-and, as such, the un- reasoned that quantum mechanics is shakable foundation for all of modern incompatible with any reasonable idea physics-and partly still uncaptured of reality. In the next two papers, Bohr frontier territory? What else is it but replies, in effect, that the EPR concept an unfamiliar animal, confined to an animal house? And how else can one better capture its newness than by walking around, looking at it through one window after another, seeking to combine fragmentary views into a total picture? We here take two tours

around the subject. The first tour begins with Nicls Bohr's account of his famous 28-year dialog with Albert Einstein. That account is followed by a great trio: Max Born's epochal paper on the probability interpretation of quantum mechanics, Werner Heisenberg's on the principle of indeterminism, and Niels Bohr's Como lecture on what quantum mechanics permits one to know. These are followed by H. P. Robertson's general formulation of indeterminism or "uncertainty," then by Nevili Moit's analysis of the meaning of an α-ray track, which illustrates the principles expounded by Bohr and Born and others and shows the quantum theory of observation in action.

Had quantum mechanics stopped here, its deepest lesson would have escaped attention: "No elementary quantum phenomenon is a phenomenon until it is a registered (observed) phenomenon." The door to this in-sight-and all the questions that go with it-was opened a crack by the paper of Alhert Finstein, Richard Tolman, and Boris Podolsky, and opened wider by the idealized experiment proposed by Einstein, Podolsky, and Nathan Rosen. This EPR paper of reality is too limited. In contrast to Bohr, Erwin Schrödinger, in his famous paper on the "cat paradox," and Eugene Wigner, in a subsequent paper, tried to connect the concept "observation" as it is employed in quantum mechanics with "consciousness." This first tour around the animal house, looking through the various windows, concludes with "law without law," an attempt to assess the situation as it stands today and to evaluate the place of quantum mechanics in the larger scheme of physics.

The second tour of inspection (Sections $\overline{11} - \bar{V}\overline{1}$) looks into the old windows afresh and into some new ones. It is designed for the more advanced student of the subject. It too gives a view of what is clear and well-established, but also glimpses of what is problematic and mysterious. Section II begins with the classic treatise of Fritz Wolfgang Londion and Edmond Bauer on the quantum theory of observation and includes notes of Wigner's 1976 lectures on interpretation of quantum mechanics, not previously published. The reader who has mastered this material or the equivalent has in hand the solid foundation of the subject. This section ends with three papers on the problem of measurement within the framework of quantum theory: Hugh Everett's "Relative State" or "Many Worlds" interpretation, and papers of Wigner and H. D. Zeh.

The Einstein-Podolsky-Rosen exper- deals with the impossibility of meaiment (Section III) deals with a system suring the spin of an electron that which, once united in a definite quanis free rather than bound in an atom tum state, splits into two well-separated systems. It considers the correlation between the state observed for one system and the state observed for the other. It asks: Does the predicted correlation exist? And if so, how does it come about? There is an enormous literature on these questions. Out of the many possible papers we have selected thirteen for this part of our second tour around the subject. They deal with "hidden variables," John Bell's inequality designed to rule out "local hidden variables," the experiments themselves, and generalizations of such experiments.

U_p to this point, the statistical interpretation of quantum mechanics and the principle of indeterminacy have been applied to a particle or system of finitely many degrees of freedom. The next group of napers (Section IV), including one by Lev Landau and Rudolf Peierls, and two by Bohi and Leon Rosenfeld, deal with the measurement of the electromagnetic field, a system with infinitely many degrees of freedom.

What is the comection between entropy, information, ergodicity, irreversibility, thermodynamics, and quantum mechanics? The next seven selections (Section V) deal in one way or another with these topics.

The second tour concludes with Section VI, eight papers on the accuracy achievable in measurement as it is affected by quantum limitations. The first (N. F. Mott and H. S. Massey) or in some experimental combination of electric and magnetic fields. Even when a particle or an atom or a molecule admits of a measurement of its angular momentum, the measuring

equipment may be so light in mass that by this very reason its orientation is uncertain (papers of Huzihiro Araki and Mutsuo Yanase, and Yanase). Or the measurement of the time at which an interaction takes place may limit the accuracy with which one can determine the transfer of energy in that interaction (paper of David Bohm and Yakir Aharonov). Or a message may be sent through an amplifier or sent down a communication line and have quantum effects introduced into it along the way (papers of H. Heffner, H. A. Haus and J. A. Mullen, and John Pierce). Or in a measurement of a weak effect. like a gravitational wave from a supernova, can one circumvent quantum indeterminacy limits on the sensitivity of the measuring device? (paper of V. B. Braginsky, Y. I. Vorontsov and K. S. Thorne).

Anyone asking for the practical bearing of the quantum theory of measurement will think of measuring devices, their sensitivity, and the improvements in this sensitivity that can only be achieved by exploiting modern insights to the fullest. In no way do the advances of physics spread more widely to the community than in new and improved measuring devices, whose uses range from biology to
medicine, from chemistry to manufacturing. Not otherwise can one understand why the number of kinds of devices listed in the annual "Guide to Scientific Instruments" issued by the American Association for the Advancement of Science (AAAS, 1961, 1970, 1980) has steadily increased. There is at present a heavy push to measure at the Earth the fantastically weak gravitational wave produced by a supernova in the Virgo cluster of galaxies. Central to this enterprise are considerations of quantum theory that have already led to new ideas of optimal design. Achievements on this front will surely make their way from physics to many another field and supply important areas of science and technology with measuring devices of a sensitivity previously unattainable.

We regard as a welcome forerunner to the present collection an earlier collection of about half as many titles and a quarter as many pages issued for the exclusive use of members of the Physical Society of Japan. We have noi entered into various schemes for the aximatization of quantum theory and so-called "quantum logic," and therefore do not reproduce selections from such books as George W. Mackey's Mathematical Foundations of Quantum Mechanics (1963) and Josef M. Jauch's Foundations of Quantum Mchanics (1968), nor, for exampie, the work of Gnther Ludwig and his collaborators (1968) or P. Mittelstaedt (1978), or Beltrametti and Cassinelli (1981). Neither do we pretend to a proper historical perspective, such as surely someday will be possible thanks
to the wonderful collection of tape recordings, notebooks, and other materials inventoried in Kuhn, Heilbron, Forman, and Allen, Sources for the History of Quantum Physics (1967). The literature on quantum theory is so vast that one could fill a book this size with bibliography alone. In the annotated bibliographies for each section (located near the end of the book) we have had to content ourselves with a few especially important or representative works, seeking to provide in this way points of entry into the literature.

The reader will look in vain in these selections for any decailed exposition of the wealth of mechanisms that make physics such a rich subject. We leave out such topics as photoelectric eect, scattering, chemical binding, particle theory, the LambRetherford shift, the building up of atoms, angular momentum isomers, superconductivity, and dozens of others equally important for understanding what quantum theory means for the world of today, because we assume that the reader already knows something of "quantum mechanics in action."

If one already knows so much about the applications of quantum theory, what more is to be learned by the study of the quantum theory of measurement? Willis Lamb (1969), some years after receiving the Nobel Prize, wrote, " . . . A discussion of the interpretation of quantum mechanics on any level beyond this almost inevitably becomes rather vague. The major difficulty involves the concept of measurement,' which in quantum me-
chanics means determining the value of a physical observable for a dynamical system with as

much precision as is possible.
"I have taught graduate courses in quantum mechanics for over 20 years at Columbia, Stanford, Oxford and Yale, and for almost all of them have dealt with measurement in the following manner. On beginning the lectures I told the students, 'You must first learn the rules of calculation in quantum mechanics, and then I will tell you about the theory of measurement and discuss the meaning of the subject.' Almost invariably, the time allotted to the course ran out before 1 had to fulfill my promise."

No one who reads among the present selections can escape some contact with the deeper meaning of the subject –and with some of the issues. Is it true that "no elementary quantum phenomcnon is a phenomenon until it is a recorded phenomenon"? If so, what does "recording" demand? "Irreversibility"? If so, what does one mean by "irreversibility"? If the "arrow of time" is absent from Schrödinger's equation and from quantum theory generally, what brings it into the act of measurement along with all its ideological connectives, from statistical mechanics to ergodic theory, and from information theory to thermodynamics? Is it true that the result of a measurement must be expressed in classical terms, because only in such terms can one speak in plain language to oneselfand to others? What part does communication play in creating what is called "knowledge"? And from what
deeper principle arises the necessity of the quantum in a construction of the world?
With a good conscience we limit ourselves here to the measurement side of quantum theory, because the formalism of the subject is so well treated in so many outstanding texts. Moreover, historic papers in the development of that formalism have been collected in the wonderfully useful book by B. L. Van der Waerden (1967). We wish to express here our indebtedness to those books and above all to the book of Max Jammer (1974) which provides a wealth of historical commentary on the development of the subject to its present state. See also DeWitt and Graham (1971).

We take this opportunity to thank most heartily the many colleagues who have given us their advice in the preparation of this book and to acknowledge our indebtedness to the authors and publishers cited at the front for permission to reprint the selections. We could not have put the collection together without calling on the intelligence and helpfulness of Ruth Bentley, Zelda Davis, Adrienne Harding, Colleen Kieke, Jean F. Otto, Rebecca Stadtnci, and Gloria TalcoveWoodward. We appreciate the care given to the project by the staff of Princeton University Press, including especially Alice Calaprice and Judith May. We thank many a favorable chance, many a kind act of hospitality, and thank, too, the University of Texas, the Center for Theoretical Physics, the Center for Statistical Mechanics and Thermodynamics, and the Nation-
al Science Foundation (Grant PHY K. Kucha, G. Ludwig, G. Mackey, 7826592) for the colleagues that they L. Michel, C. W. Misner, P. Mithave brought our way who share telstaedt, Y. Ne'eman, A. Peres, C. our concern with the measurement side of quantum theory, among them L. Bartell, J. D. Bekenstein, D. Bohm, A. Bohr, V. B. Braginsky, E. Caianiello, P. Candelas, P. C. W. Davies, B. d'Espagnat, D. Deutsch, B. S. DeWitt, R. H. Dicke, F. Dyson, H. Everett III, L. Z. Fang, R. P. Feynman, E. S. Fry, U. Gerlach, A. M. Gleason, L. P. Horwitz, A. Jaffe, F. Jenc, J. Kalckar, J. R. Klauder, D. Kondepudi, and

Piron, I. Prigogine, A. Qadir, L. Radicati, D. Sciama, A. Shimony, H. P. Stapp, E. C. G. Sudarshan, C. Teitelboim, K. S. Thorne, F. Tipler, W. Unruh, E. P. Wigner, W. K. Wootters, and H. D. Zeh.

John Archibald Wheeler Wojciech Hubert Zurek Ausiin, Texuss
January 20, 1982

The editors gratefully acknowledge the permission of the Niels Bohr Library of the American Institute of Physics to reproduce here Ehrenfest's photographs of Bohr and Einstein, and the permissions received from authors, translators, and publishers to reprint the

following items.
I.i Commentary Based on Petersen (1968)
Extracts reprinted by permission from Quantum Physics and The Philosophical Tradition by Aage Petersen. Copyright 1968, Massachusetts Institute of Technology Press.

Commentaries

1.1 Commentary of Heisenberg (1967)

Extracts from "Quantum theory and its interpretations," by W. Heisenberg. Reprinted by permission from Niels Bohr: His Life and Work as Seen by His Friends and Colloagues, pp. 94 108, edited by S. Rozental. Copyright 1967, North Holland Publishing Company.
I. 2 Commentary of Rosenfeld (1971a)

Extracts from "Men and ideas in the history of atomic theory," by L. Rosenfeld. From Selected Papers of Lon Rosenfeld, pp. 266-296, edited by R. S. Cohen and J. J. Stachel. Copyright 1979, D. Reidel Publishing Company, reprinted by permission of the publisher.
I. 3 Commentary of Heisenberg (1967)

Extracts from "Quantum theory and its interpretations," by W. Heisenberg. Reprinted by permission from Niels Bohr: His Life and Work as Seen by His Friends and Colleagues, pp. 94-108, cdited by S. Rozental. Copy right 1967, North Holland Publishing Company.
I. 3 Commentary of Rosenfeld (1971a)

Extracts from "Men and ideas in the history of atomic theory," by L. Rosenfeld. From Selected Papers of Leon Rosenfeld, pp. 266-296, edited by R. S. Cohen and J. J. Stachel. Copyright 1979, D. Reidel Publishing Company, reprinted by permission of the publisher.
I. 4 Commentary of Rosenfeld (1963)

Extracts from "Niels Bohr's contribution to epistemology," by L. Rosenfeld. From Selected Papers of Lon Rosenfeld,
pp. 522-535, edited by R. S. Cohen and J. J. Stachel. Copyright 1979, D. Reidel Publishing Company, reprinted by permission of the publisher.
I. 4 Commentary of Rosenfeld (1971a)

Extracts from "Men and ideas in the history of atomic theory," by L. Rosenfeld. From Selected Papers of Lon Rosenfeld, pp. 266-296, edited by R. S. Cohen and J. J. Stachel. Copyright 1979, D. Reidel Publishing Company, reprinted by permission of the publisher.
I. 4 Commentary of Heisenberg (1967)

Extracts from "Quantum theory and its interpretations," by W. Heisenberg. Reprinted by permission from Niels Rohr: His Life and Work as Seen by His Friends and Colleagues, pp. 94-108, edited by S. Rozental. Copyright 1967, North Holland Publishing Company.
. 8 Commentary of Rosenfeid (1967)
Extracts from "Niels Bohr in the thirties: consolidation and extension of the conception of complementarity," by L. Rosenfeld. Reprinted by permission from Niels Bohr : His Life and Work as Seen by His Friends and Colleagues, pp. 114-136, edited by S. Rozental. Copyright 1967, North Holland Publishing Company.
I. 9 Commentary of Rosenfeld (1967)

Extracts from "Niels Bohr in the thirties: consolidation and extension of the conception of complementarity," by L. Rosenfeld. Reprinted by permission from Niels Bohr: His Life and Work as Seen by His Friends and Colleagues, pp. 114-136, edited by S. Rozental Copyright 1967, North Holland Publishing Company.
IV. 2 Commentary of Rosenfeld (1955)

Extracts from "On quantum electrodynamics," by L . Rosenfeld. Reprinted by permission from Niels Bohr and the Development of Physics, edited by W. Pauli. Copyright 1955, Pergamon, New York.

VI. 1 Commentary of Rosenfeld (1971b)

Extracts from "Quantum theory in 1929: recollections from the first Copenhagen conference," by L. Rosenfeld. Reprinted by permission from Selected Papers of Lon Rosenfeld, pp. 305-307, edited by R. S. Cohen and J. J. Stachel. Copyright 1979, D. Reidel Publishing Co.

I. 1 "Discussion with Einstein on epistemological problems in atomic physics," by Niels Bohr. Reprinted by permission

from Albert Einstein, Philosopher Scientist, pp. 200-241, edited by Paul Arthur Schilpp. Copyright 1949, currently handled jointly by Open Court Publishing Company and the American Friends of The Hebrew University, Inc.

I. 2 "On the quantum mechanics of collisions," by M. Born. By permission from Zeitschrift fr Physik 37, pp. 863867. Copyright 1926, Springer-Verlag.

1.3 "The physical content of quantum kinematics and mechanics," by W. Heisenberg. Reprinted by permission from Zeitschrift fiir Physik 43, pp. 172-198. Copyright (C) 1927 by Springer-Verlag. Reprinted in Dokumente der Naturuivsenschaft, Vol. 4. pp. 9-35. Copyright 1935.

I. 4 "The quantum postulate and the recent development of atomic theory," by Niels Bohr. Reprinted by permission from Nature, Voi. 121, pp. 580-590. Copyright (C) 1928, Macmillian Journals Limited.

I. 5 "The uncertainty principle," by H. P. Robertson. Reprinted by permission from Physical Review 34, pp. i3-i4. Copyright 1929, American Physical Sucity.

I. 6 "The wave mechanics of α-ray tracks," by N. F. Mott. Reprinted by permission from Proceedings A126, pp. 79-84. Copyright 1929, The Royal Society, London.

1.7 "Knowledge of past and future in quantum mechanics," by A. Finstein, R. C. Tolman, and B. Podolsky. Reprinted by permission from Physical Review 37, pp. 780-781. Copyright 1931, currently handled jointly by American Physical Society and the American Friends of the Hebrew University, Inc.

I. 8 "Can quantum-mechanical description of physical reality be considered complete?" by A. Einstein, B. Podolsky and N. Rosen. Reprinted by permission from Physical Review 47, pp. 777-780. Copyright 1935, currently handled jointly by American Physical Society and the American Friends of The Hebrew University, Inc.

1.9 "Quantum mechanics and physical reality," by Nicls Bohin. Reprinted by permission from Nature, Vol. 136, pp. 65. Copyright 1935, Macmillian Journals Limited.

I. 10 "Can quantum-mechanical description of physical reality be considered complete?" by Niels Bohr. Reprinted by permission from Physical Review 48, pp. 696-702. Copyright 1935, American Physical Society.

I. 11 "Die gegenwrtige Situation in der Quantenmechanik," by E. Schrödinger. By permission from Die Naturuissenschaften 23, pp. 807-812, 823-828, 844-849. Copyright 1935, Springer-Verlag New York, Inc. English translation: "The present situation in quantum mechanics: a translation of Schrödinger's 'cat paradox' paper," by John $\overline{\text{D}}$. Irimmer. Reprinted by permission from Proceedings of the American Philosophical Society, Vol. 124, pp. 323-338. Copyright 1980. American Philosophical Society.

i.i2 "Remarks on the mind-body question," pp. 171-184, from Symmetries and Reflections, science essay by E. P. Wigner. Copyright 1967, Indiana University Press, reprinted by permission of the publisher.

I. 13 "Law without law," excerpts as follows:

"Frontiers of time" by John A. Wheeler. Reprinted by permission from Problems in the Foundations of Physics. Proceedings of the International School of Physics "Enrico Fermi," Course 72, pp. 395-407. Copyright 1979, Italian Physical Society.

"Beyond the Black Hole," from H. Woolf, ed., Some Strangeness in the Proportion: A Centennial Symposium to Celebrate the Achievements of Albert Einstein, Copyright 1980, Addison-Wesley, Reading, Massachusetts, pp. 362-363. Reprinted with permission.

II. 1 "The theory of observation in quantum mechanics," by F. W. London and E. Bauer. No. 775 of Actualits scientifiques et industrielles: Exposs de physique gnraie, edited by Paul Langevin, Hermann et Compagnie, 1939. English translations done independently by Abner Shimony, by J. A. Wheeler and W. H. Zurek, and by James H. McGrath and Susan Mclean MicGrath; the editors have drawn on aill three translations to produce the version here.
II. 2 "Interpretation of quantum mechanics," by Eugene P. Wigner. By permission from lecture notes of Eugene P. Wigner, tevised and printed here for the first time.
II. 3 "Relative state formulation of quantum mechanics," by Hugh Everett III. Reprinted by permission from Reviews of Modern Physics, Vol. 29, pp. 454-462. Copyright 1957, American Physical Socicty.
II. 4 "The problem of measurement," by Eugene P. Wigner. Reprinted by permission from American Journal of Physics, Vol. 31, pp. 6-15, edited by John S. Rigden.

Copyright 1963, American Association of Physics Teachers.

II. 5 "On the interpretation of measurement in quantum theory," by H. D. Zeh. Reprinted by permission from Foundations of Physics, Vol. 1, pp. 69-76. Copyright 1970, Plenum Publishing Corporation.
III. 1 "Polyelectrons" by John A. Wheeler. Reprinted by permission from Annals of the New York Academy of Sciences, Vol. 48, pp. 219-238, edited by Bill M. Boland. Copyright 1946, New York Academy of Science.
III. 2 "The paradox of Einstein, Rosen and Podolsky," by David Bohm. Reprinted by permission from Quantum Theory, Chapter 22, Sections 15-19. Copyright 1951, Prentice Hall.
III. 3 "A suggested interpretation of the quantum theory in terms of 'hidden' variables, $\overline{\mathbf{I}}$ and $\overline{\mathbf{II}}$,'" by David Bohm. Reprinted by permission from Physical Review 85, pp. 166-179. Copyright 1952, American Physical Society.
III. 4 "On the problem of hidden variables in quantum mechanics," by John S. Bell. Keprinted by permission from Reviews of Modern Physics, Vol. 38, pp. 447-452. Copyright 1966, American Physical Society.
III. 5 "On the Einstein Podolsky Rosen paradox," by John S. Bell. Reprinted by permission of J. S. Bell. Originally appeared in Physics I, pp. 195 200. Copyright 1964, Physics Publishing Co.
III. 6 "Proposed experiment to test local hidden-variable theories," by John F. Clauser, Michael A. Horne, Richard A. Holt, and Abner Shimony. Reprinted by permission from Physical Review Letters 23, pp. 880-884. Copyright 1969, American Physical Society.
IIII. 7 "Experimental test of local hidden-variable theories," by Stuart J. Freedman and John F. Clauser. Reprinted by permission from Physical Review Letters 28, pp. 938-941. Copyright 1972, American Physical Society.
Iiii. 8 "Experimental test of local hidden-variable theories," by Edward S. Fry and Randall C. Thompson. Reprinted by permission from Physical Review Letters 37, pp. 465-468. Copyright 1976, American Physical Society.
III. 9 "Quantum mechanics and hidden variables: A test of Bell's inequality by the measurement of the spin correlation in low-energy proton-proton scattering." by M. LamehiRachti and W. Mittig. Reprinted by permission from

Physical Review D14, pp. 2543-2555. Copyright 1976, American Physical Society.
III. 10 "Proposed experiment to test the nonseparability of quantum mechanics," by Alain Aspect. Reprinted by permission from Physical Review D14, pp. 1944-1951. Copyright 1976, American Physical Society.
III. 11 "Complementarity in the double-slit experiment: Quantum nonseparability and a quantitative statement of Bohr's principle," by W. K. Wootters and W. H. Zurek. Reprinted by permission from Physical Review D19, pp. 473-484. Copyright 1979, American Physical

Society.
III. 12 "Complementarity in the double-slit experiment: On simple realizable systems for observing intermediate particle-wave behavior," by L. S. Bartell. Reprinted by permission from Physical Review D21, pp. 1698-1699. Copyright 1980, American Physical Society.
III. 13 "A 'delayed-choice' quantum mechanics experiment," hy William C. Wickes, C. O. Alley, and O. Jakubowicz. Printed here for the first time by permission of the autiors.
IV. 1 "Erweiterung des Umbestimmtheitsprinzips fr die relativistische Quantentheorie," by L. Landau and Rudolf Peierls. By permission from Zeitschrift fr Physik 69, p. 56. Copyright 1931 Springer-Verlag. English translation: "Extension of the uncertainty principle to relativistic quantum theory," translated and edited by Dirk ter Haar. Reprinted by permission from Collected Papers of L. D. Landau, pp. 4-51. Copyright 1965, Gordon and Breach
IV. 2 "On the question of the measurability of electromagnetic field quantities," by Niels Bohr and Lon Rosenfeld. By permission from Maiematisk-Fysiske Mduelelser Kongelige Danske Videnskabernes Selskah 12, No. 8. Copyright 1933, Det Kongelige Danske Videnskabernes Selskab. English translation by Aage Petersen. Reprinted by permission from Seiected Papers of Lon Rosenfeid, pp. 357412, edited by R. S. Cohen and J. J. Stachel. Copyright 1979, D. Reidel Publishing Co.
IV. 3 "Field and charge measurements in quantum electrodynamics," by Niels Bohr and Lon Rosenfeld. Reprinted by permission from Physical Review 78, pp. 794-798. Copyright 1950, American Physical Society.
V. 1 "Uber die Entropieverminderung in einen thermodynamischen System bei Eingriffen intelligenter Wesen," by Leo Szilard. By permission from Zcitschrift fr Pliysik 53, pp. 840 856. Copyright 1929. SpringerVerlag. English translation: "On the decrease of entropy in a thermodynamic system by the intervention of intelligent beings," by Anatol Rapoport and Mechthilde Knoller, revised by Carl Eckart. Reprinted by permission from Rehavioral Science 9, pp. 301-310. Copyright 1964, Society for General Systems Research.
V. 2 "Measurement and Reversibility" and "The Measuring Process," by John von Neumann. By permission from Mathematische Grundlagen der Quantenmechanik, Chap ters V and VI. Copyright 1932, Springer-Verlag. English translation reprinted by permission from J. von Neumann, Mathematical Foundations of Quantum Mechanics, trans. Robert T. Beyer, pp. 347-445. Copy right 1955, Princeton University Press.
V. 3 "The ergodic behaviour of quantum many-body systems," by Leon Van Hove. Reprinted by permission from Physica 25, pp. 268-276. Copyright 1959, North Holland Publishing Company.
V. 4 "Quantum theory of measurement and ergodicity conditions," by A. Daneri, A. Loinger, and G. M. Prosperi. Reprinted by permission from Nuclear Physics 33, pp. 297. Copyright 1962, North Holland Publishing Company.
V. 5 -lime symmetry in the quantum process of measurement," by Yakir Aharonov, Peter G. Rergmann, and Joel L. Lebowitz. Reprinted by permission from Physical Review 134, pp. B1410. Copyright 1964, American Physical Society.
V. 6 "Lyapounov variable: Entropy and measurement in quantum mechanics," by B. Misra, I. Prigogine, and M. Courbage. Reprinted by permission from Proceedings of Tile National Academy of Sciences 76. pp. 47684772. Copyright 1979, The National Academy of Sciences.
V. 7 "Can we undo quantum measurements?" by Asher Peres. Reprinted by permission from Physical Review D22, pp. 879-883. Copyright (C) 1980, American Physical Society.
VI. 1 "Magnetic moment of the electron," by N. F. Mott and
H. S. W. Massey. Reprinted by permission of Oxford University Press from The Theory of Atomic Collisions, 3rd ed., pp. 214-219, Section 2, Chapter IX. Copyright 1965, Oxford University Press.
VI. 2 "Measurement of quantum mechanical operators," by H. Araki and M. M. Yanase.

Reprinted by permission from Physical Review 120, pp. 622-626. Copyright 1960, American Physical Society.
VI. 3 "Optimal measuring apparatus," by M. M. Yanase. Reprinted by permission from Physical Review 123, pp. 666-668. Copyright 1961, American Physical Society.
VI. 4 "Time in the quantum theory and the uncertainty relation for time and chergy," by Y. Aharonov and D. Bohm. Reprinted by permission from Physical Review 122, pp. 1649-1658. Copyright 1961, American Physical Society.
VI. 5 "The fundamental noise limit of linear amplifiers," by J. Heffner. Reprinted from Proceedings of the Institute of Radio Engineers 50, pp. 1604-1608. Copyright 1962, The Institute of Radio Engineers.
VI. 6 "Quantum noise in linear amplifiers," by Herman A. Haus and James A. Mullen. Reprinted by permission from Physical Review 128, pp. 2407-2413. Copyright 1962, American Physical Society.
Vi. 7 "Opical chamels. Practical limits with photon counting," by J. R. Pierce. Reprinted from the Institute of Electrical and Electronics Engineers Transactions on Communications Com-26, pp. 1819-1821. Copyright 1978, Institute of Electrical and Electronics Engineers.
VI. 8 "Quantum nondemolition measurements," by V. B. Braginsky, Y. I. Vorontsov, and K. S. Thorne. Reprinted from Science 209, pp. 547-557. Copyright 1980, The American Association for the Advancement of Science.

24 I. Questions of Principle

24.1 1.1 The Bohr-einstein Dialogue

Bohr in Brief

Complementarity: any given application of classical concepts precludes the simultaneous use of other classical concepts which in a different connection are equally necessary for the elucidation of the phenomena.

Bohr (1934), p. 10

The discovery of the quantum of action shows us, not only the natural iimitation of classical physics, but, by throwing a new light upon the old philosophical problem of the objective existence of phenomena independently of our observations, confronts us with a situation hitherto unknown in natural science. As we have seen, any observation necessitates an interference with the course of the phenomena, [and] of such a nature that it deprives us of the foundation underlying the causal mode of description. The limit, which nature herself has thus imposed upon us, of the possibility of speaking about phenomena as existing objectively finds its expression, as far as we can judge, just in the formulation of quantum mechanics.

BOHR (1934), p. 115

. . . atomic phenomena under different experimental conditions, must be termed complementary in the sense that cach is welldefined and that together they exhaust all definable knowledge about the objects concerned. The quantum-mechanical formalism . . . gives . . . an exhaustive complementary account of a very large domain of experience.

Вонк (1958), p. 90

... one sometimes speaks of "disturbance of phenomena by observation" or "creation of physical attributes to atomic objects by measurements." Such phrases, however, arc apt to causc confusion, since words like phenomena and observation, just as attributes and measurements, are here used in a way incompatible with common language and practical definition. On the lines of objective description, [I advocate using] the word phenomenon to refer only to observations obtained under circumstances whose description includes an account of the whole experimental

arrangement. In such terminology, the observational problem in quantum physics is deprived of any special intricacy and we are, moreover, directly reminded that every atomic phenomenon is closed in the sense that its observation is based on registrations obtained by means of suitable amplification
devices with irreversible functioning such as, for example, permanent marks on a photographic plate, caused by the penetration of electrons into the emulsion. In this connection, it is important to realize that the quantum-mechanical formalism permits well-defined applications referring only to such closed phenomena.

BOHR (1958), p. 73

. . . the finite magnitude of the quantum of action prevents altogether a sharp distinction being made between a phenomenon and the agency by which it is observed . . . . BOHR (1934), p. 11

. . . it . . . can make no difference, as regards observable effects obtainable hy a definite experimental arrangement, whether our plans for constructing or handling the instruments are fixed beforehand or whether we prefer to postpone the completion of our planning until a later moment when the particle is already on its way from one instrument to another. Bohr in Schilpp (1949), p. 230

. . . a subsequent measurement to a certain degree deprives the information given by a previous measurement of its significance for predicting the future course of the phenomena. Obviously, these facts not only set a limit to the extent of the information obtainable by measurements, but they also set a limit to the meaning which we may attribute to such information. We meet here in a new light the old truth that in our description of nature the purpose is not to disclose the real essence of the phenomena but only to track down, so far as it is possible, relations between the manifold aspects of our experience.

BOHR (1934), p. 18

The experimental conditions can be varied in many ways, but the point is that in each case we must be able to communicate to others what we have done and what we have learned, and that therefore the functioning of the measuring instruments must be described within the framework of classical physical ideas.

Bohr (1958), p. 89

the conscious analysis of any concept stands in a relation of exclusion to its immediate application. BOHR (1934), p. 96

I am quite prepared to talk of the spiritual life of an electronic computer; to say that it is considering or that it is in a bad mood.

What really matters is the unambiguous description of its behaviour, which is what we observe. The question as to whether the machine really feels, or whether it merely looks as though it did, is absolutely as meaningless as to ask whether light is "in reality" waves or particles. We must never forget that "reality" too is a human word just like "wave" or "consciousness." Our task is to learn to use these words correctiy-that is, unambiguousiy and consistentiy.

Bohr as quoted by Kalckar (1967), p. 234

We are suspended in language in such a way that we cannot say what is up and what is down.

Bohr as quoted by Petersen (1968), p. 188

Commentary Based on

Petersen (1968)

Aage Petersen was already working had previously considered: "One of the on his book, his Copenhagen doctoral most important issues in the measurethesis, while he was assisting Bohr (†18 November 1962) in preparing of his last lectu The thesis is philoracter. It is concerned It is not intended to be sional history of science, nor a cumentation of stages in Bohr's thinking.

However, some of the sections allow one to get an impression of stages in Bohr's development of the concepts of "complementarity," "closure," and "phenomenon." The book states more sharply than Bohr does in his writings the points on which Bohr disagreed with others, explaining, for example, why Bohr introduced the term "complementarity" when Heisenherg had already employed the term "indeterminism."

Petersen (pp. 110-111 and 145) notes that Bohr insisted upon an analysis of the "possibilities of definition" over and above those "possibilities of observation" that he and Heisenberg together ment analysis is the question of the nature and origin of the uncertainties involved in the determination of conjugate variables. According to Heisenberg, these uncertainties were due to discontinuous changes, imposed by the quantum on one such variable during the measurement of the other. However, as Bohr pointed out, 'a discontinuous change of energy and momentum during observation could not prevent us from ascribing accurate values to the space-time coordinates, as well as to the momentum-cnergy components before and after the process.' To clarify the issue it is necessary to consider closely the possibilities of definition. . . . Bohr pointed out that the conditions of description in quantum physics not only 'set a limit to the extent of the information obtainable by measurement, but they also set a limit to the meaning which we may attribute to such information.' More specifically, the reciprocal
uncertainties are '. . . essentially an outcome of the limited accuracy with which changes in energy and momentum can be defined."

Petersen goes on to say (p. 120), "Einstein's criticism showed the need for a more nigotous formulation of the Copenhagen interpretation, and Bohr's many attempts to improve the terminology illuminate the development of his attitude to the interpretation question. [How could one] make explicit the conditions set by the formalism for applying the physical concepts unambiguously in the quantum domain? [For this purpose the] shift from 'intuitive understanding' to 'unambiguous communication' [was] an important step."

Petersen adds (pp. 120 and 122 23), "Terminologically, the principal result of Bohr's analysis of Einstein's imaginary experiments was the concept of a quantum phenomenon [which first appeared in Bohr (1939)]. Bohr came to regard it as the basic element of the quantal description. ... To specify a phenomenon it is not enough to state the initial characteristics of the object, like the momentum with which it emerges from the source. The predictions depend on the whole experimental arrangement and are only well defined if the whole arrangement is specified. To be able to predict the interference pattern we must be given the whole geometry of the optical bench. In other words, 'all unambiguous interpretation of the quantum mechanical formalism involves the fixation of the external conditions, defining the initial state of the atomic system concerned and the
character of the possible predictions as regards subsequent observable properties of that system. Any measurement in quantum theory can in fact only refer either to a fixation of the initial state or to the test of such predictions, and it is . . . the combination of measurements of both kinds which constitutes a welldefined phenomenon . . . .' [A phenomenon] is 'indivisible.' In electron interference, the physical process' starting at the electron's emergence from the gun and ending at its impact on the plate has no definable course. It cannot be broken up into physically welldefined steps. Unlike a classical phenomenon, a quantum phenomenon is not a sequence of physical events, but a new kind of individual entity. [3].

Petersen (p. 164) recalls Bohr's state ment (1934, pp. 19-20): "An interesting example of ambiguity in our use of language is provided by the phrase used to express the failure of the causal modc of description, namely, that one speaks of a free choice on the part of nature. Indeed, properly speaking, such a phrase requires the idea of an extennal chooser, the existence of which, however, is denied already by the use of the word nature." Petersen adds (p. 172) "... Boht often stressed in discussions that 'reality' is a word in our language and that this word is no different from other words in that we must learn to use it correctly ...." Petersen continues

(ρ. 173), "Indivisibility and closure are the two principal characteristics of a quantum phenomenon.... The phenomenon's 'interior' is . . . physically inscrutable. . . . In a classical physical process each infinitesimal step is 'closed', i.e. it
is a definite physical event. . . . In quantum physics the object's 'behavior' is not a sequence of 'closed' steps." Here Petersen might have quoted from Bohr (1958, p. 73):"... Every atomic phenomenon is closed in the sense that its observation is based on registrations obtained by means of suitable amplification devices with irreversible functioning such as, for example, permanent marks on a photographic plate, caused by the penetration of electrons into the emulsion." But Petersen adds (p. 17779), ". . . It is clear that Bohr considered the closure of fundamental significance not only in quantum physics but in the whole description of nature. Classical physics did not call attention to the role of this concept because classical processes have, so to say, maximal closure. In quantum mechanics the physically describable aspects of a phenomenon are closed, but the phenomenon's physically inscrutable 'interior' is not. ... [The] question suggests itself as to whether it is possible to dispense with the classical concepts in the quantum domain or at least supplement them with new physical concepts that are less directly tied to the structure of classical theories and more adapted to the typical quantal parts of quantum mechanics. Bohr gave a negative answer to this question. He held that 'it would be a misconception to believe that the difficultics of the atomic theory may be evaded by eventually replacing the concepts of classical physics by new conceptual forms.""

Bohr was remarkably categorical about the question at issue. 'It lies in the nature of physical observation...
that all experience must ultimately be expressed in terms of classical concepts the unambiguous interpretation of any measurement must be essentially framed in terms of the classical physical theories, and we may say that in this sense the language of Newton and Maxwell will remain the language of physicists for all time.' 'Even when the phenomena transcend the scope of classical physical theories, the account of the experimental arrangement and the recording of observations must be given in plain language, suitably supplemented by technical physical terminology. This is a clear logical demand, since the very word experiment refers to a situation where we can tell others what we have done and what we have icanned.'"

Commentary of Heisenrfrg (1967)

The Solvay Conference in Brussels in the autumn of 1927 closed this marvellous period in the history of atomic theory. Planck, Einstein, Lorentz, Bohr, de Broglie, Born, and Schrödingci, and from the younger generation Kramers, Pauli, and Dirac, were gathered here and the discussions were soon focussed to a duel between Einstein and Bohr on the question as to what extent atomic theory in its present form could be considered to be the final solution of the difficulties which had becn discussed for several decades. We generally met already at breakfast in the hotel, and Einstein began to describe an ideal experiment in which he thought the inner contradictions of the Copenhagen interpretation were particularly
clearly visible. Einstein, Bohr and I walked together from the hotel to the congress building, and I listened to the lively discussion between these two people whose philosophical attitudes were so different, and from time to time I added a remark on the structure of the mathematical formalism. During the meeting and particularly in the pauses we younger people, mostly Pauli and I, tried to analyze Einstein's experiment, and at lunch time the discussions continued between Bohr and the others from Copenhagen. Bohr had usually finished the complete analysis of the ideal experiment late in the afternoun and showed it to Finstein at the supper table. Einstein had no good objection to this analysis, but in his heart he was not convinced. Bohr's friend Ehrenfest, who was also a close friend of Einstein, said to him, "I'm ashamed of you, Einstein. You put yourself here just in the same position as your opponents in their futile attempts to refute your relativity theory." These discussions continued even at the next Solvay

meeting in 1930, and it was probably on this occasion that Einstein at breakfast proposed the famous experiment (discussed in Bohr's article on the occasion of Einstein's 70th birthday) in which the colour of a light quantum is to be determined by weighing the source before and after the quantum's emission. As this problem involved gravity, one had to include the theory of gravity, in other words, general relativity theory in
the analysis. It was a particular triumph for Bohr that he was able to show that evening, by using just Einstein's own formulae from general rclativity, that even in this experiment the uncertainty relations are valid, and that Einstein's objections were unfounded. With this the Copenhagen interpretation of quantum theory seemed from now on to stand on solid ground.

Commentary of Einstein (1936)

There is no doubt that quantum mechanics has seized hold of a beautiful element of truth, and that it will be a test stone for any future theoretical basis, in that it must be deducible as a limiting case from that basis, just as electrostatics is deducible from the Maxwell equations of the electromagnetic field or as thermodynamics is deducible from classical mechanics. However, I do not believe that quantum mechanics will be the starting point in the search for inis basis, jusi as, vice versa one could not go from thermodynamics (resp. statistical mechanics) to the foundations of mechanics.

Commentary of Einstein (BEFORE 1953)

That the Lord should play with dice, all right; but that He should gamble according to definite rules, that is beyond me.

24.2 I. 1 Discussion with Einstein on Epistemological Problems in Atomic Physics

WHEN invited by the Editor of the series, "Living Philosophers," to write an article for this volume in which contemporary scientists are honouring the epoch-making contributions of Albert Einstein to the progress of natural philosophy and are acknowledging the indebtedness of our whole generation for the guidance his genius has given us, I thought much of the best way of explaining how much I owe to him for inspiration. In this connection, the many occasions through the years on which I had the privilege to discuss with Einstein epistemological problems raised by the modern development of atomic physics have come back vividly to my mind and I have felt that I could hardly attempt anything better than to give an account of these discussions which, even if no complete concord has so far been obtained, have been of greatest value and stimulus to me. I hope also that the account may convey to wider circles an impression of how essential the open-minded exchange of ideas has been for the progress in a field where new experience has time after time demanded a reconsideration of our views.

From the very beginning the main point under debate has been the attitude to take to the departure from customary principles of natural philosophy characteristic of the novel development of physics which was initiated in the first year of this century by Planck's discovery of the universal quantum of action. This discovery, which revealed a feature of atomicity in the laws of nature going far beyond the old doctrine of the limited divisibility of matter, has indeed taught us that the classical theories

of physics are idealizations which can be unambiguously applied only in the limit where all actions involved are large compared with the quantum. The question at issue has been whether the renunciation of a causal mode of description of atomic processes involved in the

[8]Originally published in Albert Einstein: Philosopher-Scientist, P. A. Schilpp, ed., pp. 200-41, The Library of Living Philosophers, Evanston (1949).

endeavours to cope with the situation should be regarded as a temporary departure from ideals to be ultimately revived or whether we are faced with an irrevocable step towards obtaining the proper harmony between analysis and synthesis of physical phenomena. To describe the background of our discussions and to bring out as clearly as possible the arguments for the contrasting viewpoints, I have felt it necessary to go to a certain length in recalling some main features of the development to which Einstein himself has contributed so decisively.

As is well known, it was the intimate relation, elucidated primarily by Boitzmann, between the laws of thermodynamics and the statistical regularitics exhibited by mechanical systems with many degrees of freedom, which guided Planck in his ingenious treatment of the problem of thermal radiation, leading him to his fundamental discovery. While, in his work, Planck was principally concerned with considerations of essentially statistical character and with great caution refrained from definite conclusions as to the extent to which the existence of the quantum implied a departure from the foundations of mechanics and electrodynamics, Einstein's great original contribution to quantum theory (1905) was just the recognition of how physical phenomena like the photo-effect may depend directly on individual quantum effects. [1] In these very same years when, in developing his theory of relativity, Einstein laid a new foundation for physical science, he explored with a most daring spirit the novel features of atomicity which pointed beyond the whole framework of classical physics.

With unfailing intuition Einstein thus was led step by step to the conclusion that any radiation process involves the emission or absorption of individual light quanta or "photons" with energy and momentum

$$E = hv \quad \text{and} \quad P = h\sigma \tag{I}$$

[1] A. Einstein, Ann. d. Phys., 17, 132, (1905).

respectively, where h is Planck's constant, while v and σ are the number of vibrations per unit time and the number of waves per unit length, respectively. Notwithstanding its fertility, the idea of the photon implied a quite unforeseen dilemma, since any simple corpuscular picture of radiation would obviously be irreconcilable with interference effects, which present so essential an aspect of radiative phenomena, and which can be described only in terms of a wave picture. The acuteness of the dilemma is stressed by the fact that the interference effects offer our only means of defining the concepts of frequency and wavelength entering into the very expressions for the energy and momentum of the photon.

In this situation, there could be no question of attempting a causal analysis of radiative phenomena, but only, by a combined use of the contrasting pictures, to estimate probabilities for the occurrence of the individual radiation processes. However, it is most important to realize that the recourse to probability laws under such circumstances is essentially different in aim from the familiar application of statistical considerations as practical means of accounting for the properties of mechanical systems of great structural complexity. In fact, in quantum physics we are presented not with intricacies of this kind, but with the inability of the classical frame of concepts to comprise the peculiar feature of indivisibility, or "individuality," characterizing the elementary processes.

The failure of the theories of classical physics in accounting for atomic phenomena was further accentuated by the progress of our knowledge of the structure of atoms. Above all, Rutherford's discovery of the atomic nucleus (1911) revealed at once the inadequacy of classical mechanical and electromagnetic concepts to explain the inherent stability of the atom. Here again the quantum theory offered a clue for the elucidation of the situation and especially it was found possible to account for the atomic stability, as well as for the empirical laws governing the spectra of the elements, by assuming that any reaction of the atom resulting in a change of its energy involved a complete transition between two so-called stationary quantum states and that, in particular, the spectra were emitted by a step-like pro-

cess in which each transition is accompanied by the emission of a monochromatic light quantum of an energy just equal to that of an Einstein photon.

These ideas, which were soon confirmed by the experiments of Franck and Hertz (1914) on the excitation of spectra by impact of electrons on atoms, involved a further renunciation of the causal mode of description, since evidently the interpretation of the spectral laws implies that an atom in an excited state in general will have the possibility of transitions with photon emission to one or another of its lower energy states. In fact, the very idea of stationary states is incompatible with any directive for the choice between such transitions and leaves room only for the notion of the relative probabilities of the individual transition processes. The only guide in estimating such probabilities was the so-called correspondence principle which originated in the search for the closest possible connection between the statistical account of atomic processes and the consequences to be expected from classical theory, which should be valid in the limit where the actions involved in all stages of the analysis of the phenomena are large compared with the universal quantum.

At that time, no general self-consistent quantum theory was yet in sight, but the prevailing attitude may perhaps be illustrated by the following passage from a lecture by the writer from 1913: [2]

I hope that I have expressed myself sufficiently clearly so that you may appreciate the extent to which these considerations confict with the admirably consistent scheme of conceptions which has been rightly termed the classical theory of electrodynamics. On the other hand, I have tried to convey to you the impression that-just by emphasizing so strongly this conflict-it may also be possible in course of time to establish a certain coherence in the new ideas.

Important progress in the development of quantum theory was made by Einstein himself in his famous article on radiative equilibrium in 1917, [3] where he showed that Planck's law for thermal radiation could be simply deduced from assumptions

[2] N. Bohr, Fysisk Tidsskrift, 12, 97, (1914). (English version in The Theory of Spectra and Atomic Constitution, Cambridge, University Press, 1922). [3] A. Einstein, Phys. Zs., 18, 121, (1917).

conforming with the basic ideas of the quantum theory of atomic constitution. To this purpose, Einstein formulated general statistical rules regarding the occurrence of radiative transitions between stationary states, assuming not only that, when the atom is exposed to a radiation field, absorption as well as emission processes will occur with a probability per unit time proportional to the intensity of the irradiation, but that even in the absence of external disturbances spontaneous emission processes will take place with a rate conesponding to a certain a priori probability. Regarding the latter point, Finstein emphasized the fundamental character of the statistical description in a most suggestive way by drawing attention to the analogy between the assumptions regarding the occurrence of the spontaneous radiative transitions and the well-known laws governing transformations of radioactive substances.

In connection with a thorough examination of the exigencies of thermodynamics as regards radiation problems, Einstein stressed the dilcmma still further by pointing out that the argumentation implied that any radiation process was "unidirected" in the sense that not only is a momentum corresponding to a photon with the direction of propagation transferred to an atom in the absorption process, but that also the emitting atom will receive an equivalent impulse in the opposite direction, although there can on the wave picture be no question of a preference for a single direction in an emission process. Einstein's own attitude to such startling conclusions is expressed in a passage at the end of the article (loc. cit., p. 127 f.), which may be translated as follows:

These features of the elementary processes would seem to make the development of a proper quantum treatment of radiation almost unavoidable. The weakness of the theory lies in the fact that, on the one hand, no closer connection with the wave concepts is obtainable and that,

on the other hand, it leaves to chance (Zufall) the time and the direction of the elementary processes; nevertheless, I have full confidence in the reliability of the way entered upon.

When I had the great experience of meeting Einstein for the first time during a visit to Derlin in 1920, these fundamental
questions formed the theme of our conversations. The discussions, to which I have often reverted in my thoughts, added to all my admiration for Einstein a deep impression of his detached attitude. Certainly, his favoured use of such picturcsquc phrases as "ghost waves (Gespensterfelder) guiding the photons" implied no tendency to mysticism, but illuminated rather a profound humour behind his piercing remarks. Yet, a certain difference in attitude and outlook remained, since, with his mastery for co-ordinating apparently contrasting experience without abandoning continuity and causality, Einstein was perhaps more reluctant to renounce such ideals than someone for whom renunciation in this respect appeared to be the only way open to procced with the immediate task of co-ordinating the multifarious evidence regarding atomic phenomena, which accumulated from day to day in the exploration of this new field of knowledge.

In the following years, during which the atomic problems attracted the attention of rapidly increasing circles of physicists, the apparent contradictions inherent in quantum theory were felt ever more acutely. Illustrative of this situation is the discussion raised by the discovery of the Stern-Gerlach effect in 1922. On the one hand, this effect gave striking support to the idea of stationary states and in particular to the quantum theory of the Zeeman effect developed by Sommerfeld; on the other hand, as exposed so clearly by Einstcin and Ehrenfest, [4] it presented with unsurmountable difficulties any attempt at forming a picture of the behaviour of atoms in a magnetic field. Similar paradoxes were raised by the discovery by Compton (1924) of the change in wave-length accompanying the scattering of X-rays by electrons. This phenomenon afforded, as is well known, a most direct proof of the adequacy of Einstein's view regarding the transfer of energy and momentum in radiative processes; at the same time, it was equaliy clear that no simple picture of a corpuscular collision could offer an exhaustive description of the phenomenon. Under the impact of such difficulties, doubts
[6] A. Einstein and P. Ehrenfest, Zs. f. Phys., 11, 31, (1922).
were for a time entertained even regarding the conservation of energy and momentum in the individual radiation processes; [5] a view, however, which very soon had to be abandoned in face of more refined experiments bringing out the correlation between the deflection of the photon and the corresponding electron recoil.

The way to the clarification of the situation was, indeed, first to be paved by the development of a more comprehensive quantum theory. A first step towards this goal was the recognition by de Broglie in 1925 that the wave-corpuscle duality was not confined to the properties of radiation, but was equally unavoidable in accounting for the behaviour of material particles. This idea, which was soun convincingly confinmed by experiments on electron interference phenomena, was at once greeted by Einstein, who had already envisaged the deep-going analogy between the properties of thermal radiation and of gases in the so-called degenerate state. [9] The new line was pursued with the greatest success by Schrödinger (1926) who, in particular, showed how the stationary states of atomic systems could be represented by the proper solutions of a wave-equation to the establishment of which he was led by the formal analogy, originally traced by Hamilton, between mechanical and optical problems. Still, the paradoxical aspects of quantum theory were in no way ameliorated, but even emphasized, by the apparent contradiction between the exigencies of the general superposition principle of the wave description and the feature of individuality of the elementary atomic processes.

At the same time, Heisenberg (1925) had laid the foundation of a rational quantum mechanics, which was rapidly developed through important contributions by Born and Jordan as well as by Dirac. In this theory, a formalism is introduced, in which the kinematical and dynamical variables of classical mechanics are replaced by symbols subjected to a non-commutative

algebra. Notwithstanding the renunciation of orbital pictures, Hamilton's canonical cquations of mechanics are kept unaltered and

[5] N. Bohr, H. A. Kramers and J. C. Slater, Phil. Mag., 47, 785, (1924).

[6] A. Einstein, Berl. Ber., (1924), 261, and (1925), 3 and 18.

Planck's constant enters only in the rules of commutation

$$qp - pq = \mathrm{V} = \mathrm{I}\frac{h}{2\pi} \tag{2}$$

holding for any set of conjugate variables q and p. Through a representation of the symbols by matrices with elements referring to transitions between stationary states, a quantitative formulation of the correspondence principle became for the first time possible. It may here be recalled that an important preliminary step towards this goal was reached through the establishment, especially by contributions of Kramers, of a quantum theory of dispersion making basic use of Einstein's general rules for the probability of the occurrence of absorption and emission processes.

This formalism of quantum mechanics was soon proved by Schrödinger to give results identical with those obtainable by the mathematically often more convenient methods of wave theory, and in the following years general methods were gradually established for an essentially statistical description of atomic processes combining the features of individuality and the requirements of the superposition principle, equally characteristic of quantum theory. Among the many advances in this period, it may especially be mentioned that the formalism proved capable of incorporating the exclusion principle which governs the states of systems with several electrons, and which already before the advent of quantum mechanics had been derived hy Pauli from an analysis of atomic spectra. The quantitative comprehension of a vast amount of empirical evidence could leave no doubt as to the fertility and adequacy of the quantum-mechanical formalism, but its abstract character gave rise to a widespread feeling of uneasiness. An elucidation of the situation should, indeed, demand a thorough examination of the very observational problem in atomic physics.

This phase of the development was, as is well known, initiated in 1927 by Heisenherg, [7] who pointed out that the knowledge obtainable of the state of an atomic system will always involve a peculiar "indeterminacy." Thus, any measurement of the position of an electron by means of some device,

[7] W. Heisenberg, Zs. f. Phys., 43, 172, (1927).

like a microscope, making use of high frequency radiation, will, according to the fundamental relations (i), be connected with a momentum exchange between the electron and the measuring agency, which is the greater the more accurate a position measurement is attempted. In comparing such considerations with the exigencies of the quantum-mechanical formalism, Heisenberg called attention to the fact that the commutation rule (2) imposes a reciprocal limitation on the fixation of two conjugate variables, q and p, expressed by the relation

$$\Delta_q \cdot \Delta_p \approx h, \tag{3}$$

where Δq and Δp are suitably defined latitudes in the determination of these variables. In pointing to the intimate connection between the statistical description in quantum mechanics and the actual possibilities of measurement, this so-called indeterminacy relation is, as Heisenberg showed, most important for the elucidation of the paradoxes involved in the atiempts of analyzing quantum effects with reference to customary physical pictures.

The new progress in atomic physics was commented upon from various sides at the International Physical Congress held in September 1927, at Como in commemoration of Volta. In a lecture on that occasion, [8] I advocated a point of view conveniently termed "complementarity," suited to embrace the characteristic features of individuality of quantum phenomena, and at

the same time to clarify the peculiar aspects of the observational problem in this field of experience. For this purpose, it is decisive to recognize that, however far the phenomena transcend the scope of classical physical explanation, the account of all evidence must be expressed in classical terms. The argument is simply that by the word "experiment" we refer to a situation where we can tell others what we have done and what we have learned and that, therefore, the account of the experimental arrangement and of the resuits of the observations must be expressed in unambiguous language with suitable application of the terminology of classical physics.

This crucial point, which was to become a main theme of the

[8] Atti del Congresso Internazionale dei Fisici, Como, Settembre 1927 (reprinted in Nature, 121, 78 and 580, 1928).

discussions reported in the following, implies the impossibility of any sharp separation between the behaviour of atomic objects and the interaction with the measuring instruments which serve to define the conditions under which the phenomena appear. In fact, the individuality of the typical quantum effects finds its proper expression in the circumstance that any attempt of subdividing the phenomena will demand a change in the experimental arrangement introducing new possibilities of interaction between objects and measuring instruments which in principle cannot be controlled. Consequently, evidence obtained under different experimental conditions cannot be comprehended within a single picture, but must be regarded as complementary in the sense that only the totality of the phenomena exhausts the possible information about the objects.

Under these circumstances an essential element of ambiguity is involved in ascribing conventional physical attributes to atomic objects, as is at once evident in the dilemma regarding the corpuscular and wave properties of electrons and photons, where we have to do with contrasting pictures, each referring to an essential aspect of empirical evidence. An illustrative example, of how the apparent paradoxes are removed by an examination of the experimental conditions under which the complementary phenomena appear, is also given by the Compton effect, the consistent description of which at first had presented us with such acute difficulties. Thus, any arrangement suited to study the exchange of energy and momentum between the electron and the photon must involve a latitude in the spacetime description of the interaction sufficient for the definition of wave-number and frequency which enter into the relation (I). Conversely, any attempt of locating the collision between the photon and the electron more accurately would, on account of the unavoidable interaction with the fixed scales and clocks defining the space-time reference frame, exclude all closer account as regards the balance of momentum and energy.

As stressed in the lecture, an adequate tool for a complementary way of description is offered precisely by the quantummechanical formalism which represents a purely symbolic scheme permitting only predictions, on lines of the correspondencc principlc, as to results obtainable under conditions specified

by means of classical concepts. It must here be remembered that even in the indeterminacy relation (3) we are dealing with an implication of the formalism which defies unambiguous expression in words suited to describe classical physical pictures. Thus, a sentence like "we cannot know both the momentum and the position of an atomic object" raises at once questions as to the physical reality of two such attributes of the object, which can be answered only by referring to the conditions for the unambiguous use of space-time concepts, on the one hand, and dynamical conservation laws, on the other hand. While the combination of these concepts into a single picture of a causal chain of events is the essence of classical mechanics, room for regularities beyond the grasp of such a description is just afforded by the circumstance that the study of the complementary phenomena demands mutually exclusive experimental arrangements.

I he necessity, in atomic physics, of a renewed examination of the foundation for the un-

ambiguous use of elementary physical ideas recalls in some way the situation that led Einstein to his original revision on the basis of all application of space-time concepts which, by its emphasis on the primordial importance of the observational problem, has lent such unity to our world picture. Notwithstanding all novelty of approach, causal description is upheld in relativity theory within any given frame of reference, but in quantum theory the uncontrollable interaction between the objects and the measuring instruments forces us to a renunciation even in such respect. This recognition, however, in no way points to any limitation of the scope of the quantum-mechanical description, and the trend of the whole argumentation presented in the Como lecture was to show that the viewpoint of complementarity may be regarded as a rational generalization of the very ideal of causality.

At the general discussion in Como, we all missed the presence of Einstein, but soon after, in October 1927, I had the opportunity to meet him in Brussels at the Fifth Physical Conference of the Solvay Institute, which was devoted to the theme "Electrons and Photons." At the Solvay meetings, Einstein had from their beginning been a most prominent figure, and several
of us came to the conference with great anticipations to learn his reaction to the latest stage of the development which, to our view, went far in clarifying the problems which he had himself from the outset elicited so ingeniously. During the discussions, where the whole subject was reviewed by contributions from many sides and where also the arguments mentioned in the preceding pages were again presented, Einstein expressed, however, a deep concern over the extent to which causal account in space and time was abandoned in quantum mechanics.

To illustrate his attitude, Einstein referred at one of the sessions to the simple example, illustrated by Fig. i, of a particle (electron or photon) penetrating through a hole or a narrow slit in a diaphragm placed at some distance before a photographic plate. On account of the diffraction of the wave con-

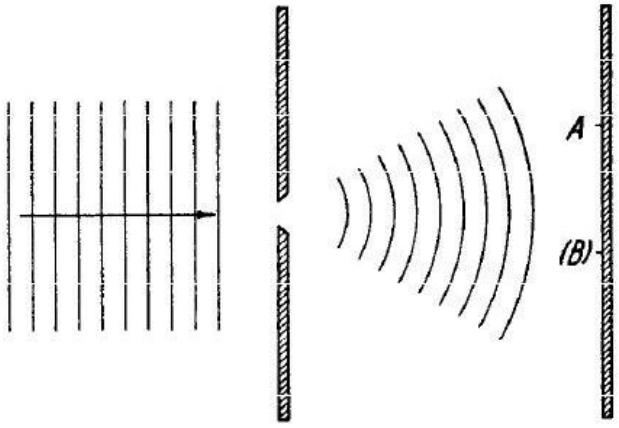


FIG. 1

nected with the motion of the particle and indicated in the figure by the thin lines, it is under such conditions not possible to predict with certainty at what point the electron will arrive at the photographic plate, but only to calculate the probability that, in an experiment, the electron will be found within any given region of the plate. The apparent difficulty, in this description, which Einstein felt so acutely, is the fact that, if in the experiment the electron is recorded at one point $\hat{A}$ of the piate,

[9] Institut International de Physique Solvay, Rapport et discussions du 5^6 Conseil, Paris : 9:9, a5, 5 ff.

then it is out of the question of ever observing an effect of this electron at another point (B), although the laws of ordinary wave propagation offer no room for a correlation between two such events.

Einstein's attitude gave rise to ardent discussions within a small circle, in which Ehrenfest, who through the years had been a close friend of us both, took part in a most active and

helpful way. Surely, we all recognized that, in the above example, the situation presents no analogue to the application of statistics in dealing with complicated mechanical systems, but rather recalled the background for Einstein's own early conclusions about the unidirection of individual radiation effects which contrasts so strongly with a simple wave picture (cf. p. 205). The discussions, however, centered on the question of whether the quantum-mechanical description exhausted the possibilities of accounting for observable phenomena or, as Einstein maintained, the analysis could be carried further and, especially, of whether a fuller description of the phenomena could be obtained by bringing into consideration the detailed balance of energy and momentum in individual processes.

To explain the trend of Einstein's arguments, it may be illustrative here to consider some simple features of the momentum and energy balance in connection with the location of a particle in space and time. For this purpose, we shall examine the simple case of a particle penetrating through a hole in a diaphragm without or with a shutter to open and close the hole, as indicated in Figs. 2a and 2b, respectively. The equidistant parallel lines to the left in the figures indicate the train of plane waves corresponding to the state of motion of a particle which, before reaching the diaphragm, has a momentum P related to the wave-number σ by the second of equations (i). In accordance with the diffraction of the waves when passing through the hole, the state of motion of the particle to the right of the diaphragm is represented by a spherical wave train with a suitably defined angular aperture ϑ and, in case of Fig. 2b, also with a limited radial extension. Consequently, the description of this state involves a certain latitude Δp in the momentum component of the particle paraliel to the diaphragm and, in the case of a
diaphragm with a shutter, an additional latitude ΔE of the kinetic energy.

Since a measure for the latitude Δq in location of the particle in the plane of the diaphragm is given by the radius a of the hole, and since $\vartheta \approx (1/oa)$, we get, using (1), just $\Delta_p \approx \hat{\vartheta} P \approx (h/\Lambda q)$, in accordance with the indeterminacy rela-

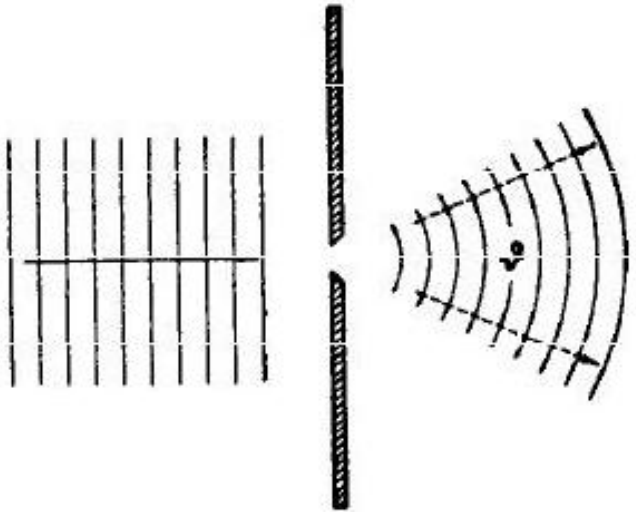


Fig. 2a

tion (3). This result could, of course, also be obtained directly by noticing that, due to the limited extension of the wave-field at the place of the slit, the component of the wave number parallcl to the plane of the diaphragm will involve a latitude

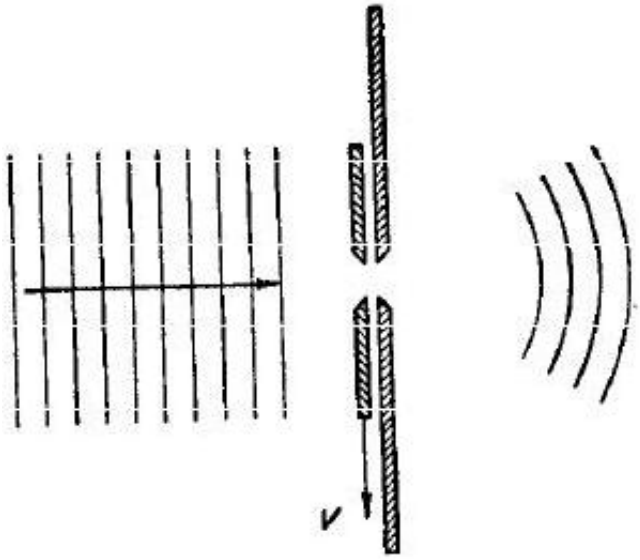


Fig. 2b

$\Delta_0 \approx (\mathrm{I}/a) \approx (\mathrm{I}/\Delta q)$. Similarly, the spread of the frequencies
of the harmonic components in the limited wave-train in Fig. 2b is evidently $\Delta v \approx (\mathrm{I}/\Delta t)$, where Δt is the time interval during which the shutter leaves the hole open and, thus, represents the latitude in time of the passage of the particle through the diaphragm. From (I), we therefore get

$$\Delta E \cdot \Delta t \approx h, \tag{4}$$

again in accordance with the relation (3) for the two conjugated variables E and t.

From the point of view of the laws of conservation, the origin of such latitudes entering into the description of the state of the particle after passing through the hole may be traced to the possibilities of momentum and energy exchange with the diaphragm
or the shutter. In the reference system considered in Figs. 2a and 2 b , the velocity of the diaphragm may be disregarded and only a change of momentum Δp between the particle and the diaphragm needs to be taken into consideration. The shutter, however, which leaves the hole opened during the time Δt, moves with a considerable velocity $v \approx (a/\Delta t)$, and a momentum transfer Δp involves therefore an energy exchange with the particle, amounting to $v\Delta_p \approx (1/\Delta t)\Delta_q\Delta_p \approx (h/\Delta t)$, being just of the same order of magnitude as the latitude ΔE given by (4) and, thus, allowing for momentum and energy balance.

The problem raised by Einstein was now to what extent a control of the momentum and energy transfer, involved in a location of the particle in space and time, can be used for a further specification of the state of the particle after passing through the hole. Here, it must be taken into consideration that the position and the motion of the diaphragm and the shutter have so far been assumed to be accurately co-ordinated with the space-time reference frame. This assumption implies, in the description of the state of these bodies, an essential latitude as to their momentum and energy which need not, of course, noticeably affect the velocities, if the diaphragm and the shutter are sufficiently heavy. However, as soon as we want to know the momentum and energy of these parts of the measuring arrangement with an accuracy sufficient to control the momentum and energy exchange with the particle under investigation, we shall, in accordance with the general indeterminacy relations, lose the possibility of their accurate location in space and time. We have, therefore, to examine how far this circumstance will affect the intended use of the whole arrangement and, as we shall see, this crucial point clearly brings

out the complementary character of the phenomena.

Returning for a moment to the case of the simple arrangement indicated in Fig. 1, it has so far not been specified to what use it is intended. In fact, it is only on the assumption that the diaphragm and the plate have well-defined positions in space that it is impossible, within the frame of the quantum-mechanical formalism, to make more detailed predictions as to the point of the photographic plate where the particle will be recorded. If, however, we admit a sufficiently large latitude in the knowledge of the position of the diaphragm it should, in principle, be possible to control the momentum transfer to the diaphragm and, thus, to make more detailed predictions as to the direction of the electron path from the hole to the recording poirt. As regards the quantum-mechanical description, we have to deal here with a two-body system consisting of the diaphragm as well as of the particle, and it is just with an explicit application of conservation laws to such a system that we are concerned in the Compton effect where, for instance, the observation of the recoil of the electron by means of a cloud chamber allows us to predict in what direction the scattered photon will eventually be observed.

The importance of considerations of this kind was, in the course of the discussions, most interestingly illuminated by the examination of an arrangement where between the diaphragm with the slit and the photographic plate is inserted another

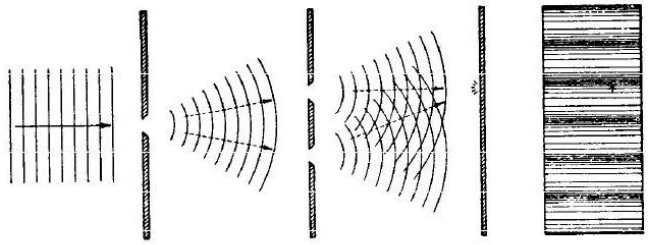


FIG. 3

diaphragm with two parallel slits, as is shown in Fig. 3. If a parallel beam of electrons (or photons) falls from the left on the first diaphragm, we shall, under usual conditions, observe on the plate an interference pattern indicated by the shading of the photographic plate shown in front view to the right of the figure. With intense beams, this pattern is built up by the accumulation of a large number of individual processes, each giving rise to a small spot on the photographic plate, and the distribution of these spots follows a simple law derivable from the wave analysis. The same distribution should also be found in the statistical account of many experiments performed with beams so faint that in a single exposure only one electron (or photon) will arrive at the photographic plate at some spot shown in the figure as a small star. Since, now, as indicated by the broken arrows, the momentum transferred to the first diaphragm ought to be different if the electron was assumed to pass through the upper or the lower slit in the second diaphragm, Einstein suggested that a control of the momenium transfer would permit a closer analysis of the phenomenon and, in particular, to decide through which of the two slits the electron had passed before arriving at the plate.

Λ closer examination showed, however, that the suggested control of the momentum transfer would involve a latitude in the knowledge of the position of the diaphragm which would exclude the appearance of the interference phenomena in question. In fact, if ω is the smail angle between the conjectured paths of a particle passing through the upper or the lower slit, the difference of momentum transfer in these two cases will, according to (1), be equal to $h\sigma\omega$ and any control of the momentum of the diaphragm with an accuracy sufficient to measure this difference will, due to the indeterminacy relation, involve a minimum latitude of the position of the diaphragm, comparable with $1/\sigma\omega$. If, as in the figure, the diaphragm with the two slits is placed in the middle between the first diaphragm and the photographic plate, it will be seen that the number of fringes per unit length will be just equal to $\sigma\omega$ and, since an uncertainty in the position of the first diaphragm of the amount of $1/\sigma\omega$ will cause an equal uncertainty in the positions of the fringes, it follows that no interference effect can appear. The same result is

easily shown to hold for any other placing of the second diaphragm between the first diaphragm and the plate, and would also be obtained if, instead of the first diaphragm, another of these three bodies were used for the control, for the purpose suggested, of the momentum transfer.

This point is of great logical consequence, since it is only the circumstance that we are presented with a choice of either tracing the path of a particle or observing interference effects, which
allows us to escape from the paradoxical necessity of concluding that the behaviour of an electron or a photon should depend on the presence of a slit in the diaphragm through which it could be proved not to pass. We have here to do with a typical example of how the complementary phenomena appear under mutually caclusive experimental arrangements (cf. p. 210) and are just faced with the impossibility, in the analysis of quantum effects, of drawing any sharp separation between an independent behaviour of atomic objects and their interaction with the measuring instruments which scrve to define the conditions under which the phenomena occur.

Our talks about the attitude to be taken in face of a novel situation as regards analysis and synthesis of experience touched naturally on many aspects of philosophical thinking, but, in spitc of all divergencies of approach and opinion, a most humorous spirit animated the discussions. On his side, Einstein mockingly asked us whether we could really believe that the providential authorities took recourse to dice-playing (". . . ob der lieve Gout wrfel,"), to which I replied by pointing at the great caution, already called for by ancient thinkers, in ascribing attributes to Providence in every-day language. I remember also how at the peak of the discussion Ehrenfest, in his affectionate manner of teasing his friends, jokingly hintcd at the apparent similarity between Einstein's attitude and that of the opponents of relativity theory; but instantly Ehrenfest added that he would not be able to find relief in his own mind before concord with Einstein was reached.

Einstein's concern and criticism provided a most valuable incentive for us all to reexamine the various aspects of the situation as regards the description of atomic phenomena. To me it was a welcome stimulus to clarify still further the rle played by the measuring instruments and, in order to bring into strong relief the mutually exclusive character of the experimental conditions under which the complementary phenomena appear, I tried in those days to sketch various apparatus in a pseudorealistic style of which the following figures are examples. Thus, for the study of an interference phenomenon of the type
indicated in Fig. 3, it suggests itself to use an experimental arrangement like that shown in Fig. 4, where the solid parts of the apparatus, serving as diaphragms and plate-holder, are

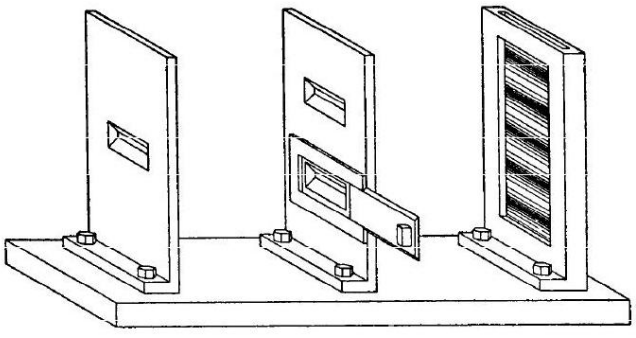


Fig. 4

firmly bolted to a common support. In such an arrangement, where the knowledge of the relative positions of the diaphragms and the photographic plate is secured by a rigid connection, it is obviously impossible to control the momentum exchanged between the particle and the separate parts of the apparatus. The only way in which, in such an arrangement, we could insure that the particle passed through one of the slits in the second diaphragm is to cover the other slit by a lid, as indicated in the figure; but if the slit is covered, there is of course no question of any interference phenomenon, and on the plate we shall simply observe a continuous distribution

as in the case of the single fixed diaphragm in Fig. i.

In the study of phenomena in the account of which we are dealing with detailed momentum balance, certain parts of the whole device must naturally be given the freedom to move independently of others. Such an apparatus is sketched in Fig. 5, where a diaphragm with a slit is suspended by weak springs from a solid yoke bolted to the support on which also other immobile parts of the arrangement are to be fastened. The scale on the diaphragm together with the pointer on the bearings of
the yoke refer to such study of the motion of the diaphragm, as may be required for an estimate of the momentum transferred to it, permitting one to draw conclusions as to the deflection suffered by the particle in passing through the slit. Since, however, any reading of the scale, in whatever way performed, will

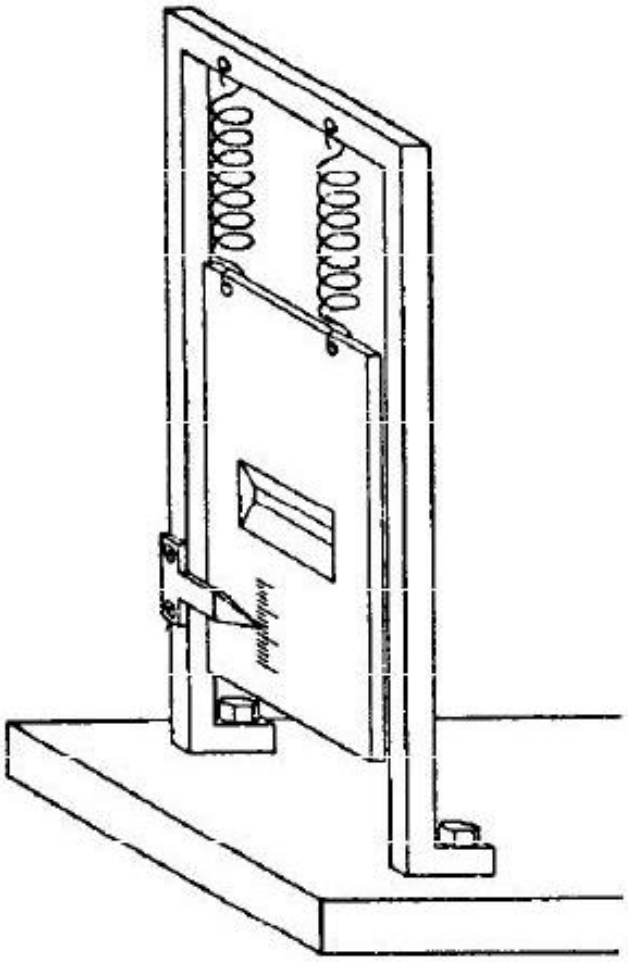


Fig. 5

involve an uncontrollable change in the momentum of the diaphragm, there will always be, in conformity with the indeterminacy principle, a reciprocal relationship between our knowledge of the position of the slit and the accuracy of the momentum control.

In the same semi-serious style, Fig. 6 represents a part of an arrangement suited for the study of phenomena which, in contrast to those just discussed, involve time co-ordination explicitly. It consists of a shutter rigidly connected with a robust clock resting on the support which carries a diaphragm and on which further parts of similar character, regulated by the same clock-work or by other clocks standardized relatively to it, are also to be fixed. The special aim of the figure is to underline that a clock is a piece of machinery, the working of

which can completely be accounted for by ordinary mechanics and will be
affected neither by reading of the position of its hands nor by the interaction between its accessories and an atomic particle. In securing the opening of the hole at a definite moment, an apparatus of this type might, for instance, be used for an accurate measurement of the time an electron or a photon takes to come from the diaphragm to some other place, but evidently, it would leave no possibility of controiling the energy transfer to

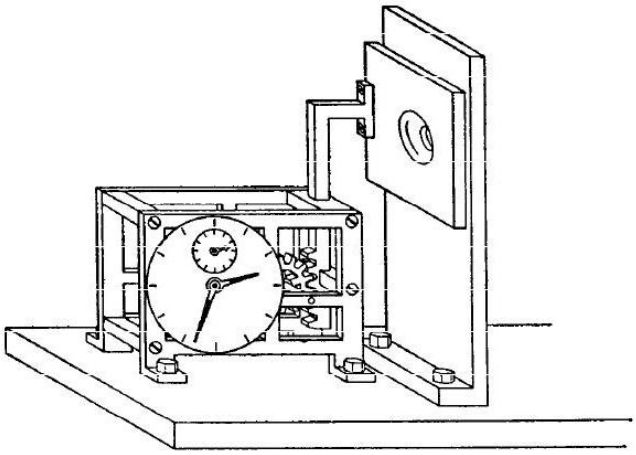


Fig. 6

the shutter with the aim of drawing conclusions as to the encrgy of the particle which has passed through the diaphragm. If we are interested in such conclusions we must, of course, use an arrangement where the shutter devices can no longer serve as accurate clocks, but where the knowledge of the moment when the hole in the diaphragm is open involves a latitude connected with the accuracy of the energy measurement by the general relation (4).

The contemplation of such more or less practical arrangements and their morc or less fictitious use proved most instructive in directing attention to essential features of the problems. The main point here is the distinction between the objects under investigation and the measuring instruments which serve to define, in classical terms, the conditions under which the phenomena appear. Incidentally, we may remark that, for the illustration of the preceding considerations, it is not relevant that experiments involving an accurate control of the momentum or energy transfer from atomic particles to heavy bodies like diaphragms and shutters would be very difficult to perform, if practicable at all. It is only decisive that, in contrast to the proper measuring instruments, these bodies together with the particles would in such a case constitute the system to which the quantum-mechanical formalism has to be applied. As regards the specification of the conditions for any well-defined application of the formalism, it is moreover essential that the whole experimental arrangement be taken into account. In fact, the introduction of any further piece of apparatus, like a mirror, in the way of a particle might imply new interference effects essentially influencing the predictions as regards the results to be eventually recorded.

The extent to which renunciation of the visualization of atomic phenomena is imposed upon us by the impossibility of their subdivision is strikingly illustrated by the following example to which Einstein very early called attention and often has reverted. If a semi-reflecting mirror is placed in the way of a photon, leaving two possibilities for its direction of propagation, the photon may either be recorded on one, and only one, of two photographic plates situated at great distances in the two directions in question, or else we may, by replacing the plates by minors, observe effects exhibiting an interference between the two reflected wave-trains. In any attempt of a pictorial representation of the behaviour of the photon we would, thus, meet with

the difficulty: to be obliged to say, on the one hand, that the photon always chooses one of the two ways and, on the other hand, that it behaves as if it had passed both ways.

It is just arguments of this kind which recall the impossibility of subdividing quantum phenomena and reveal the ambiguity in ascribing customary physical attributes to atomic objects. In particular, it must be realized that-besides in the account of the placing and timing of the instruments forming the experimental arrangement-all unambiguous use of space-time concepts in the description of atomic phenomena is confined to the
recording of observations which refer to marks on a photographic plate or to similar practically irreversible amplification effects like the building of a water drop around an ion in a cloud-chamber. Although, of course, the existence of the quantum of action is ultimately responsible for the properties of the materials of which the measuring instruments are built and on which the functioning of the recording devices depends, this circumstance is not relevant for the problems of the adequacy and completeness of the quantum-mechanical description in its aspects here discussed.

These problems were instructively commented upon from different sides at the Solvay meeting, [10] in the same session where Einstein raiscd his gencral objections. On that occasion an interesting discussion arose also about how to speak of the appearance of phenomena for which only predictions of statistical character can be made. The question was whether, as to the occurrence of individual effects, we should adopt a terminology proposed by Dirac, that we were concerned with a choice on the part of "nature" or, as suggested by Heisenberg, we should say that we have to do with a choice on the part of the "observer" constructing the measuring instruments and reading their recording. Any such terminology would, however, appear dubious since, on the one hand, it is hardly reasonable to endow nature with volition in the ordinary sense, while, on the other hand, it is certainly not possible for the observer to influence the events which may appear under the conditions he has arranged. To my mind, there is no other alternative than to admit that, in this field of experience, we are dealing with individual phenomena and that our possibilities of handling the measuring instruments allow us only to make a choice between the different complementary types of phenomena we want to study.

The epistemological problems touched upon here were more explicitly dealt with in my contribution to the issue of Naturwissenschaften in celebration of Planck's 70th birthday in 1929. In this article, a comparison was also made between the lesson derived from the discovery of the universal quantum of action

and the development which has followed the discovery of the finite velocity of light and which, through Einstein's pioneer work, has so greatly clarified basic principles of natural philosophy. In relativity theory, the emphasis on the dependence of all phenomena on the reference frame opened quite new ways of tracing general physical laws of unparalleled scope. In quantum theory, it was argued, the logical comprehension of hitherto unsuspected fundamental regularities governing atomic phenomena has demanded the recognition that no sharp separation can be made between an independent behaviour of the objects and their interaction with the measuring instruments which define the reference frame.

In this respect, quantum theory presents us with a novel situation in physical science, but attention was called to the very close analogy with the situation as regards analysis and synthesis of experience, which we meet in many other fields of human knowledge and interest. As is well known, many of the difficulties in psychology originate in the different placing of the separation lines between object and subject in the analysis of various aspects of psychical experience. Actually, words like "thoughts" and "sentiments," equally indispensable to illustrate the variety and scope of conscious life, are used in a similar complementary way as are space-time coordination and dynamical conservation laws in atomic physics. A precise formulation of such analogies involves, of course, intricacies of terminology, and the writer's position is perhaps best

[8][10] Ibid., 248 ff .

indicated in a passage in the article, hinting at the mutually exclusive relationship which will always exist between the practical use of any word and attempts at its strict definition. The principal aim, however, of these considerations, which were not least inspired by the hope of influencing Einstein's attitude, was to point to perspectives of bringing general epistemological problems into relief by means of a lesson derived from the study of new, but fundamentally simple physical experience.

At the next meeting with Einstein at the Solvay Conference in 1930, our discussions took quite a dramatic turn. As an objection to the view that a control of the interchange of momentum and energy between the objects and the measuring instruments was excluded if these instruments should serve their purpose of defining the space-time frame of the phenomena, Einstein brought forward the argument that such control should be possible when the exigencies of relativity theory were taken into consideration. In particular, the general relationship between energy and mass, expressed in Einstein's famous formula

$$E = mc^2 \tag{5}$$

should allow, by means of simple weighing, to measure the total energy of any system and, thus, in principle to control the energy transferred to it when it interacts with an atomic object.

As an arrangement suited for such purpose, Einstein proposed the device indicated in Fig. 7, consisting of a box with

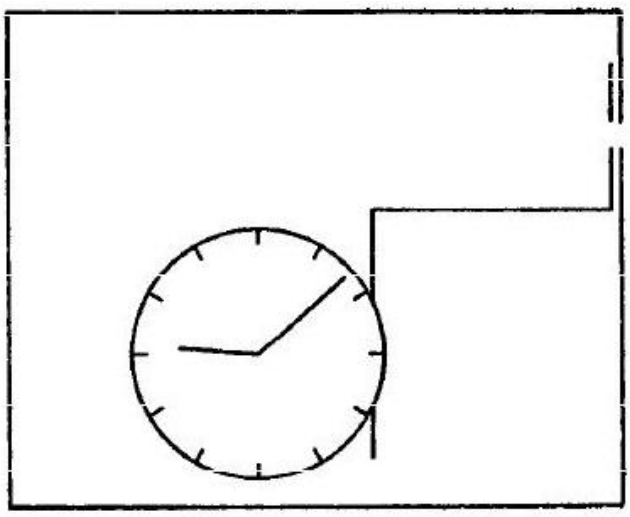


Fig. 7

a hole in its side, which could be opened or closed by a shutter moved by means of a clockwork within the box. If, in the beginning, the box contained a certain amount of radiation and the clock was set to open the shutter for a very short interval at a chosen time, it could be achieved that a single photon was released through the hole at a moment known with as great accuracy as desired. Moreover, it would apparently also be possible, by weighing the whole box before and after this event, to measure the energy of the photon with any accuracy wanted, in definite contradiction to the reciprocal indeterminacy of time and energy quantities in quantum mechanics.

This argument amounted to a serious challenge and gave rise to a thorough examination of the whole problem. At the outcome of the discussion, to which Einstein himself contributed effectively, it became clear, however, that this argument could not be upheld. In fact, in the consideration of the problem, it was found necessary to look closer into the consequences of the identification of inertial and gravitational mass implied in the application of relation (5).

Fspecially, it was essential to take into account the relationship between the rate of a clock and its position in a gravitational field-well known from the red-shift of the lines in the sun's spectrum-following from Einstein's principle of equivalence between gravity effects and the phenomena observed in accelerated reference frames.

Our discussion concentrated on the possible application of an apparatus incorporating Einstein's device and drawn in Fig. 8 in the same pseudo-realistic style as somc of the preceding figures. The box, of which a section is shown in order to exhibit its interior, is suspended in a spring-balance and is furnished with a pointer to read its position on a scale fixed to the balance support. The weighing of the box may thus be performed with any given accuracy Δm by adjusting the balance to its zero position by means of suitable loads. The essential point is now that any determination of this position with a given accuracy Δq will involve a minimum latitude Δp in the control of the momentum of the box connected with Δ_q by the relation (3). This latitude must obviously again be smaller than the total impulse which, during the whole interval T of the balancing procedure, can be given by the gravitational field to a body with a mass Δm, or

$$\Delta_p \approx \frac{h}{\Delta q} < T \cdot g \cdot \Delta m \tag{6}$$

where g is the gravity constant. The greater the accuracy of the reading q of the pointer, the longer must, consequently, be the balancing interval T, if a given accuracy Δm of the weighing of the box with its content shall be obtained.

Now, according to general relativity theory, a clock, when displaced in the direction of the gravitational force by an amount of Δq, will change its rate in such a way that its reading

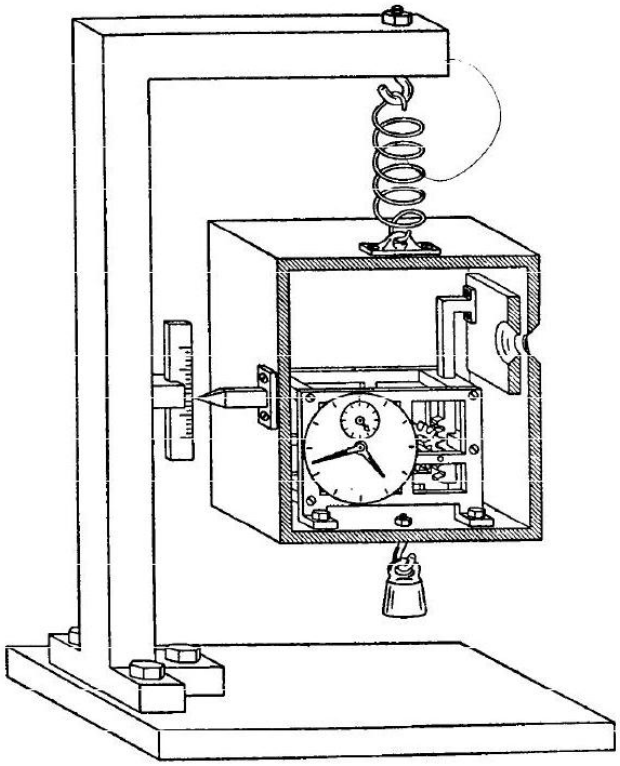


FIG. 8

in the course of a time interval T will differ by an amount ΔT given by the relation

$$\frac{\Delta T}{T} = \frac{1}{c^2} g \Delta_q \tag{7}$$

By comparing (6) and (7) we see, therefore, that after the weighing procedure there will in our knowledge of the adjustment of the clock be a latitude

$$\Delta T > \frac{h}{c^2 \Delta m}$$

Together with the formula (5), this relation again leads to

$$\Delta T \cdot \Delta E > h$$

in accordance with the indeterminacy principle. Consequently, a use of the apparatus as a means of accurately measuring the energy of the photon will prevent us from controlling the moment of its escape.

The discussion, so illustrative of the power and consistency of relativistic arguments, thus emphasized once more the necessity of distinguishing, in the study of atomic phenomena, between the proper measuring instruments which serve to define the reference frame and those parts which are to be regarded as objects under investigation and in the account of which quantum effects cannot be disregarded. Notwithstanding the most suggestive confirmation of the soundness and wide scope of the quantum-mechanical way of description, Einstein nevertheless, in a following conversation with me, expressed a feeling of disquietude as regards the apparent lack of firmly laid down principles for the explanation of nature, in which all could agree. From my viewpoint, however, I could only answer that, in dealing with the task of bringing order into an entirely new field of experience, we could hardly trust in any accustomed principles, however broad, apart from the demand of avoiding logical inconsistencics and, in this respect, the mathematical formalism of quantum mechanics should surely meet all requirements.

The Solvay meeting in 1930 was the last occasion where, in common discussions with Einstein, we could benefit from the stimulating and mediating influence of Ehrenfest, but shortly before his deeply deplored death in 1933 he told me that Einstein was far from satisfied and with his usual acuteness had discerned new aspects of the situation which strengthened his critical attitude. In fact, by further examining the possibilities for the application of a balance arrangement, Einstein had perceived alternative procedures which, even if they did not allow the use he originally intended, might seem to enhance
the paradoxes beyond the possibilities of logical solution. Thus, Einstein had pointed out that, after a preliminary weighing of the box with the clock and the subsequent escape of the photon, one was still left with the choice of either repeating the weighing or opening the box and comparing the reading of the clock with the standard time scale. Consequently, we are at this stage still free to choose whether we want to draw conclusions either about the energy of the photon or about the moment when it left the box. Without in any way interfering with the photon between its escape and its later interaction with other suitable measuring instruments, we are, thus, able to make accurate predictions pertaining either to the moment of its arrival or to the amount of energy liberated by its absorption. Since, however, according to the quantum-mechanical formalism, the specification of the state of an isolated particle cannot involve both a well-defined connection with the time scale and an accurate fixation of the energy, it might thus appear as if this formalism did not offer the means of an adequate description.

Once more Einstein's searching spirit had elicited a peculiar aspect of the situation in quantum theory, which in a most striking manner illustrated how far we have here transcended customary explanation of natural phenomena. Still, I could not agree with the trend of his remarks as reported by Ehrenfest. In my opinion, there could be no other way to deem a logically consistent mathematical formalism as inadequate than by dem onstrating the departure of its consequences from experience or by proving that its predictions did not exhaust the possibilities of observation, and Einstein's argumentation could be directed to neither of these ends. In fact, we must realize that in the problem in question we are not dealing with a single specified experimental arrangement, but are referring to two different, mutually exclusive arrangements. In the one, the balance together with another piece of apparatus like a spectrometer is used for

the study of the energy transfer by a photon; in the other, a shutter regulated by a standardized clock together with another apparatus of similar kind, accurately timed relatively to the clock, is used for the study of the time of propagation of a photon over a given distance. In both these cases, as also assumed by Einstein, the observable effects are expected to be in complete conformity with the predictions of the theory.

The problem again emphasizes the necessity of considering the whole experimental arrangement, the specification of which is imperative for any well-defined application of the quantum-mechanical formalism. Incidentally, it may be added that paradoxes of the kind contemplated by Einstein are encountered also in such simple arrangements as sketched in Fig. 5. In fact, after a preliminary measurement of the momentum of the diaphragm, we are in principle offered the choice, when an electron or photon has passed through the slit, either to repeat the momentum measurement or to control the position of the diaphragm and, thus, to make predictions pertaining to alternative subsequent observations. It may also be added that it obviously can make no difference as regards observable effects obtainable by a definite experimental arrangement, whether our plans of constructing or handling the instruments are fixed beforehand or whether we prefer to postnone the completion of our planning until a later moment when the particle is already on its way from one instrument to another.

In the quantum-mechanical description our freedom of constructing and handling the experimental arrangement finds its proper expression in the possibility of choosing the classically defined parameters entering in any proper application of the formalism. Indeed, in all such respects quantum mechanics exhibits a correspondence with the state of affairs familiar from classical physics, which is as close as possible when considering the individuality inherent in the quantum phenomena. Just in helping to bring out this point so clearly, Einstein's concern had therefore again been a most welcome incitement to explore the essential aspects of the situation.

The next Solvay meeting in 1933 was devoted to the problems of the structure and properties of atomic nuclei, in which field such great advances were made just in that period due to the experimental discoveries as well as to new fruitful applications of quantum mechanics. It need in this connection hardly be recalled that just the evidence obtained by the study of artificial nuclear transformations gave a most direct test of Einstein's fundamental law regarding the equivalence of mass and energy, which was to prove an evermore important guide for researches in nuclear physics. It may also be mentioned how Einstein's intuitive recognition of the intimate relationship between the law of radioactive transformations and the probability rules governing individual radiation effects (cf. p. 205) was confirmed by the quantum-mechanical explanation of spontaneous nuclear disintegrations. In fact, we are here dealing with a typical example of the statistical mode of description, and the complementary relationship between energy-momentum conservation and time-space co-ordination is most strikingly exhibited in the well-known paradox of particle penetration through potential barriers.

Einstein himself did not attend this meeting, which took place at a time darkened by the tragic developments in the political world which were to influence his fate so decply and add so greatly to his burdens in the service of humanity. A few months earlier, on a visit to Princeton where Einstein was then guest of the newly founded Institute for Advanced Study to which he soon after became permanently attached, I had, however, opportunity to talk with him again about the epistemological aspects of atomic physics, but the difference between our ways of approach and expression still presented obstacles to mutual understanding. While, so far, relatively few persons had taken part in the discussions reported in this article, Einstein's critical attitude towards the views on quantum theory adhered to by many physicists was soon after brought to public attention through a paper [11] with the title "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?," published in 1935 by Finstein,

Podolsky and Rosen.

The argumentation in this paper is based on a criterion which the authors express in the following sentence: "If, without in any way disturbing a system, we can predict with certainty (i.e., with probability equal to unity) the value of a physical quantity, then there exists an element of physical reality correspond-

ing to this physical quantity." By an elegant exposition of the consequences of the quantum-mechanical formalism as regards the representation of a state of a system, consisting of two parts which have been in interaction for a limited time interval, it is next shown that different quantities, the fixation of which cannot be combined in the representation of one of the partial systems, can nevertheless be predicted by measurements pertaining to the other partial system. According to their criterion, the authors therefore conclude that quantum mechanics does not "provide a complete description of the physical reality," and they express their belief that it should be possible to develop a more adequate account of the phenomena.

Due to the lucidity and apparently incontestable character of the argument, the paper of Einstein, Podolsky and Rosen created a stir among physicists and has played a large rle in general philosophical discussion. Certainly the issue is of a very subtle character and suited to emphasize how far, in quantum theory, we are beyond the reach of pictorial visualization. It will be seen, however, that we are here dealing with problems of just the same kind as those raised by Einstein in previous discussions, and, in an article which appeared a few months later, [12] I tried to show that from the point of view of complementarity the apparent inconsistencies were completely removed. The trend of the argumentation was in substance the same as that exposed in the foregoing pages, but the aim of recalling the way in which the situation was discussed at that time may be an apology for citing certain passages from my article.

Thus, after referring to the conclusions derived by Einstein, Podolsky and Rosen on the basis of their criterion, I wrote:
Such an argumentation, however, would hardly seem suited to affect the soundness of quantum-mechanical description, which is based on a coherent mathcmatical formalism covering automatically any procedure of measurement like that indicated. The apparent contradiction in fact discloses only an essential inadequacy of the customary viewpoint of natural philosophy for a rational account of physical phenomena of the type with which we are concerned in quantum mechanics. Indeed the finite interaction between object and measuring agencies conditioned

by the very existence of the quantum of action entails-because of the impossibility of controlling the reaction of the object on the measuring instruments, if these are to serve their purpose-the necessity of a final renunciation of the classical ideal of causality and a radical revision of our attitude towards the problem of physical reality. In fact, as we shall see, a criterion of reality like that proposed by the named authors containshowever cautious its formulation may appear-an essential ambiguity when it is applied to the actual problems with which we are here concerned.

As regards the special problem treated by Einstein, Podolsky and Rosen, it was next shown that the consequences of the formalism as regards the representation of the state of a system consisting of two interacting atomic objects correspond to the simple arguments mentioned in the preceding in connection with the discussion of the experimental arrangements suited for the study of complementary phenomena. In fact, although any pair q and p, of conjugate space and momentum variables obeys the rule of non-commutative multiplication expressed by (2), and can thus only be fixed with reciprocal latitudes given by (3), the difference $q_1 - q_2$ between two space-co-ordinates referring to the constituents of the system will commute with the sum $p_1 + p_2$ of the corresponding momentum components, as follows directly from the commutability of q_1 with p_2 and q_2 with p_1. Both $q_1 - q_2$ and $p_1 + p_2$ can, therefore, be accurately fixed in a state of

[811] A. Einctein, R. Podolsky and N. Rosen, Phys. Req., 47, 777, (1935).
[812] N. Bohr, Phys. Rev., 48, 696, (1935).

the complex system and, consequently, we can predict the values of either q_1 or p_1 if either q_2 or p_2, respectively, are determined by direct measurements. If, for the two parts of the system, we take a particle and a diaphragm, like that sketched in Fig. 5, we see that the possibilities of specifying the state of the particle by measurements on the diaphragm just correspond to the situation described on p. 220 and further discussed on p. 230, where it was mentioned that, after the particle has passed through the diaphragm, we have in principle the choice of measuring either the position of the diaphragm or its momentum and, in each case, to make predictions as to subsequent observations pertaining to the particle. As repeatedly stressed, the principal point is here that such measurements demand mutually exclusive experimental arrangements.

The argumentation of the article was summarized in the following passage:
From our point of view we now see that the wording of the abovementioned criterion of physical reality proposed by Einstein, Podolsky, and Rosen contains an ambiguity as regards the meaning of the expression 'without in any way disturbing a system.' Of course there is in a case like that just considered no question of a mechanical disturbance of the system under investigation during the last critical stage of the measuring procedure. But even at this stage there is essentially the question of an influence on the very conditions which define the possible types of predictions regarding the future behaviour of the system. Since these conditions constitute an inherent element of the description of any phenomenon to which the term "physical reality" can be properly attached, we see that the argumentation of the mentioned authors does not justify their conclusion that quantum-mechanical description is essentially incomplete. On the contrary, this description, as appears from the preceding discussion, may be characterized as a rational utilization of all possibilities of unambiguous interpretation of measurements, compatible with the finite and uncontrollable interaction between the objects and the measuring instruments in the field of quantum theory. In fact, it is only the mutual exclusion of any two experimental procedures, permitting the unambiguous definition of complementary physical quantities, which provides room for new physical laws, the coexistence of which might at first sight appear irreconcilable with the basic principles of science. It is just this entirely new situation as regards the description of physical phenomona that the notion of complementarity aims at characterizing.

Rereading these passages, I am deeply aware of the incfficiency of expression which must have made it very difficult to appreciate the trend of the argumentation aiming to bring out the essential ambiguity involved in a reference to physical attributes of objects when dealing with phenomena where no sharp distinction can be made between the behaviour of the objects themselves and their interaction with the measuring instruments. I hope, however, that the present account of the discussions with Einstein in the foregoing years, which contributed so greatly to make us familiar with the situation in quantum physics, may give a clearer impression of the necessity of a radical revision of basic principles for physical explanation in order to restore logical order in this field of experience.

Einstein's own views at that time are presented in an article "Physics and Reality," published in 1936 in the Journal of the Franklin Institute. [13]." Starting from a most illuminating exposition of the gradual development of the fundamental principles in the theories of classical physics and their relation to the problem of physical reality, Einstein here argues that the quan-tum-mechanical description is to be considered merely as a means of accounting for the average behaviour of a large number of atomic systems and his attitude to the belief that it should offer an exhaustive description of the individual phenomena is expressed in the following words: "To believe this is logically possible without contradiction; but it is so very contrary to my scientific instinct that I cannot forego the search for a more complete conception."

Even if such an attitude might seem well-balanced in itself, it nevertheless implies a rejection of the whole argumentation exposed in the preceding, aiming to show that, in quantum

mechanics, we are not dealing with an arbitrary renunciation of a more detailed analysis of atomic phenomena, but with a recognition that such an analysis is in principle excluded. The peculiar individuality of the quantum effects presents us, as regards the comprehension of weil-defined evidence, with a novel situation unforeseen in classical physics and irreconcilable with conventional ideas suited for our orientation and adjustment to ordinary experience. It is in this respect that quantum theory has called for a renewed revision of the foundation for the unambiguous use of elementary concepts, as a further step in the development which, since the advent of relativity theory, has been so characteristic of modern science.

In the following years, the more philosophical aspects of the situation in atomic physics aroused the interest of ever larger circles and were, in particular, discussed at the Second International Congress for the Unity of Science in Copenhagen in July 1936. In a lecture on this occasion, [14] I tried especially to

stress the analogy in epistemological respects between the limitation imposed on the causal description in atomic physics and situations met with in other fields of knowledge. A principal purpose of such parallels was to call attention to the necessity in many domains of general human interest to face problems of a similar kind as those which had arisen in quantum theory and thereby to give a more familiar background for the apparently extravagant way of expression which physicists have developed to cope with their acute difficultics.

Besides the complementary features conspicuous in psychology and already touched upon (cf. p. 224), examples of such relationships can also be traced in biology, especially as regards the comparison between mechanistic and vitalistic viewpoints. Just with respect to the observational problem, this last question had previously been the subject of an address to the International Congress on Light Therapy held in Copenhagen in 1932, [15] where it was incidentalily pointed out that even the psycho-physical parallelism as envisaged by Lcibniz and Spinoza has obtained a wider scope through the development of atomic physics, which forces us to an attitude towards the problem of explanation recalling ancient wisdom, that when searching for harmony in life one musi never forget that in the drama of existence we are ourselves both actors and spectators.

Utterances of this kind would naturally in many minds evoke the impression of an underlying mysticism foreign to the spirit of science; at the above mentioned Congress in 1936 I therefore tried to clear up such misunderstandings and to explain that the only question was an endeavour to clarify the conditions, in each field of knowledge, for the analysis and synthesis of experience. [14] Yet, I am afraid that I had in this respect only little success in convincing my listeners, for whom the dissent among the physicists themselves was naturally a cause of scepticism as to the necessity of going so far in renouncing customary demands as regards the explanation of natural phenomena. Not least through a new discussion with Einstein in Princeton in 1937, where we did not get beyond a humourous contest con-

[15] II [e] Congrs international de la Lumire, Copenhague 1933 (reprinted in Nature, 131, 421 and 457, 1933).

cerning which side Spinoza would have taken if he had lived to see the development of our days, I was strongly reminded of the importance of utmost caution in all questions of terminology and dialectics.

These aspects of the situation were especially discussed at a meeting in Warsaw in 1938, arranged by the International Institute of Intellectual Co-operation of the League of Nations. [16] The preceding years had seen great progress in quantum physics due to a number of fundamental discoveries regarding the constitution and properties of atomic nuclei as well as due to important developments of the mathematical formalism taking the requirements of relativity theory into account. In the last respect, Dirac's ingenious quantum theory of the electron of-

[811] A. Einstein, Journ. Frankl. Inst., 221, 349, (1936).

[14] N. Bohr, Erkenntnis, 6, 293, (1937), and Philosophy of Science, 4, 289, (1937).

fered a most striking illustration of the power and fertility of the general quantum-mechanical way of description. In the phenomena of creation and annihilation of electron pairs we have in fact to do with new fundamental features of atomicity, which are intimately connected with the non-classical aspects of quantum statistics expressed in the exclusion principle, and which have demanded a still more far-reaching renunciation of explanation in terms of a pictorial representation.

Mieanwhile, the discussion of the epistemological problems in atomic physics attracted as much attention as ever and, in commenting on Einstein's views as regards the incompleteness of the quantum-mechanical mode of description, I entered more directly on questions of terminology. In this connection I warned especially against phrases, often found in the physical literature, such as "disturbing of phenomena by ohservation" or "creating physical attributes to atomic objects by measurements." Such phrases, which may serve to remind of the apparent paradoxes in quantum theory, are at the same time apt to cause confusion, since words like "phenomena" and "observations," just as "attributes" and "measurements," are used in a way hardly compatible with common language and practical definition.

As a more appropriate way of expression I advocated the ap-
"New Theories in Physics (Paris 1938), 11.
plication of the word phenomenon exclusively to refer to the observations obtained under specified circumstances, including an account of the whole experimental arrangement. In such terminology, the observational problem is free of any special intricacy since, in actual experiments, all observations are expressed by unambiguous statements referring, for instance, to the registration of the point at which an electron arrives at a photographic plate. Moreover, speaking in such a way is just suited to emphasize that the appropriate physical interpretation of the symbolic quantum-mechanical formalism amounts only to predictions, of determinate or statistical character, pertaining to individual phenomena appearing under conditions defined by classical physical concepts.

Notwithstanding all differences between the physical problems which have given rise to the development of relativity theory and quantum theory, respectively, a comparison of purely logical aspects of relativistic and complementary argumentation reveals striking similarities as regards the renunciation of the absolute significance of conventional physical attributes of objects. Also, the neglect of the atomic constitution of the measuring instruments themselves, in the account of actual experience, is equally characteristic of the applications of relativity and quantum theory. Thus, the smallness of the quantum of action compared with the actions involved in usual experience, including the arranging and handling of physical apparatus, is as essential in atomic physics as is the enormous number of atoms composing the world in the general theory of relativity which, as often pointed out, demands that dimensions of apparatus for measuring angles can be made small compared with the radius of curvature of space.

In the Warsaw lecture, I commented upon the use of not directly visualizable symbolism in relativity and quantum theory in the following way:
Even the formalisms, which in both theories within their scope offer adequate means of comprehending all conceivable experience, exhibit deepgoing analogics. In fact, the astounding simplicity of the generalization of classical physical theories, which are obtained by the use of multidimensional geometry and non-commutative algebra, respectively, rests in both
cases essentially on the introduction of the conventional symbol $\sqrt{-1}$. The abstract character of the formalisms concerned is indeed, on closer examination, as typical of relativity theory as it is of quantum mechanics, and it is in this respect purely a matter of tradition if the former theory is considered as a completion of classical physics rather than as a first fundamental step in the thoroughgoing revision of our conceptual means of comparing observations, which the modern development of physics has forced upon us.
It is, of course, true that in atomic physics we are confronted with a number of unsolved

fundamental problems, especialiy as regards the intimate relationship between the elementary unit of electric charge and the universal quantum of action; but these problems are no more connected with the epistemological points here discussed than is the adequacy of relativistic argumentation with the issue of thus far unsolved problems of cosmology. Both in relativity and in quantum theory we are concerned with new aspects of scientific analysis and synthesis and, in this comection, it is interesting to note that, even in the great epoch of critical philosophy in the former century, there was only question to what extent a priori arguments could be given for the adequacy of space-time co-ordination and causal connection of experience, but never question of rational generalizations or inherent limitations of such categories of human thinking.

Although in more recent years I have had several occasions of meeting Einstein, the continued discussions, from which I always have reccived new impulses, have so far not lied to a common view about the epistemological problems in atomic physics, and our opposing views are perhaps most clearly stated in a recent issue of Dialectica, [17] bringing a general discussion of these problems. Realizing, however, the many obstacles for mutual understarding as regards a matter where approach and background must influence everyone's attitude, I have welcomed this opportunity of a broader exposition of the development by which, to my mind, a veritable crisis in physical science has been overcome. The lesson we have hereby received would seem to have brought us a decisive step further in the never-

[17] N. Bohr, Dialectica, 1, 312 (1948).

ending struggle for harmony between content and form, and taught us once again that no content can be grasped without a formal frame and that any form, however useful it has hitherto proved, may be found to be too narrow to comprehend new experience.

Surely, in a situation like this, where it has been difficult to reach mutual understanding not only between philosophers and physicists but even between physicists of different schools, the difficulties have their root not seldom in the preference for a certain use of language suggesting itself. from the different lines of approach. In the Institute in Copenhagen, where through those years a number of young physicists from various countries came together for discussions, we used, when in trouble, often to comfort ourselves with jokes, among them the old saying of the two kinds of truth. To the one kind belong statements so simple and clear that the opposite assertion obviously could not be defended. The other kind, the so-calied "deep truths," are statements in which the opposite also contains deep truth. Now, the development in a new field will usually pass through stages in which chaos becomes gradually replaced by order; but it is not least in the intermediate stage where deep truth prevails that the work is really exciting and inspires the imagination to search for a firmer hold. For such endeavours of seeking the proper balance between seriousness and humour, Einstein's own personality stands as a great example and, when expressing my belief that through a singularly fruitful co-operation of a whole gencration of physicists we are nearing the goal where logical order to a large extent allows us to avoid deep truth, I hope that it will be taken in his spirit and may serve as an apology for several utterances in the preceding pages.

The discussions with Einstein which have formed the theme of this article have extended over many years which have witnessed great progress in the field of atomic physics. Whether our actual meetings have been of short or long duration, they have always left a deep and lasting impression on my mind, and when writing this report I have, so-to-say, been arguing with Einstein all the time even when entering on topics ap-

parently far removed from the special problems under debate at our meetings. As regards the account of the conversations I am, of course, aware that I am relying only on my own memory, just as I am prepared for the possibility that many features of the development of quantum theory, in which Einstein has played so large a part, may appear to himself in a different light. I trust, however, that I have not failed in conveying a proper impression of how much it has

meant to me to be able to benefit from the inspiration which we all derive from every contact with Einstein.

Niels Bohr
Universitetets Institut
for Teoretisk Fysik
Copenhagen, Denmark

24.3 I. 2 Born's Probabilistic Interpretation

COMMENTARY OF ROSENFELD (1971A)

that the proper quantal concepts can be altogether dispensed with? Far from it, Heisenberg had at once seen that this Schrödinger made no secret of his contention was untenable: Schrödinintention to substitute simple classical pictures for the strange conceptions of quantum mechanics, for whose abstract character he expressed deep "aversion"; he was conscious that this last sentiment was shared by all the older generation of physicists, who had not accepted the necessity of giving up their habitual ways of thinking when dealing with phenomena on the atomic scale. Significantly, he turned towards the chevroned peers of the classical eraLorentz, Planck, Einstein-who did not grudge him praise and encouragement, and shunned the founders of quantum mechanics. The latter, however, who had taken no notice of de Broglie, looked into Schrödnger's ideas mosi critically; he had indeed enforced the claim to be taken seriously by solving the wave equation for the hydrogen atom and obtaining Rydberg's formula by a calculation much simpler and more elegant than Pauli's quantum algebra. This could hardly be a fortuitous coincidence, and indeed both Pauli and Schrödinger soon discovered that the two theories so different in conception, were mathematically equivalent: for instance, the quantum amplitude governing the transition between two stationary states could be readily computed with the help of the wave amplitudes corresponding to these states. Would this formal equivalence clinch the issue in favor of Schrödinger's contention ger's way of treating the charge density as a classical source of radiation would even prevent him from obtaining Planck's law for the distribution of thermal radiation. How could such an eiementary, but fatal objection have escaped, not only Schrödinger himself, but above all the creators of the quantum theory of radiation, who gave him such uncritical support? Almost regretting to have ushered in ideas whose revolutionary consequences they had not foreseen, these great masiers desperately clung to the "sound philosophy" of classical physics, without realizing its limitations; an emotional resistance dimmed their judgment. The pioneers of quantum mechanics, on their side, were now confronted with a new challenge: Schrodinger's wave theory of matter clearly provided another formal approach to the consistent description of atomic phenomena they were striving for, but its physical content still eluded them.

It did not last long, however, before they realized that wave mechanics was just the appropriate technique they wanted for dealing with the aperiodic phenomena intractable by the quantum aigebra. This was explicitly demonstrated by Born, who showed how to treat atomic collisions by a transposition of the mathematical methods applied to the analogous classical problem
of the scattering of light waves by a waves and the associated atomic parpolarizable medium. Born's argument, ticles. He accordingly proposed to moreover, embodied an essentially new interpret the wave intensity, not as the feature, of decisive importance, with regard to the physical interpretation of the intensity of the matter waves. The optical analogy suggested a comparison of this intensity with that of a classical light wave, which the quantum theory of radiation interprets as the density of the statistical distribution of the associated photons. Born pointed out that the usual particle description of the atomic collision process could be maintained if one adopted a similar statistical relationship between the matter density of an

actual distribution of matter, as Schrödinger imagined, but as a density of probability for the presence of a particle. Thus, the formal equivalence of wave mechanics and Heisenberg's quantum mechanics became physically meaningful: it established a complete harmony between the statistical meaning of the wave intensity and the statistical character of the rules of quantum algebra for the calculation of transition probabiiities.

24.4 1.2 On the Quantum Mechanics of Collisions by Max Born

Through the investigation of collisions it is argued that quantum mechanics in the Schrödinger form allows one to describe not only stationary states but also quantum jumps.

Heisenberg's quantum mechanics has so far been applied exclusively to the calculation of stationary states and vibration amplitudes associated with transitions (I purposely avoid the word "transition probabilities"). In this connection the formalism, further developed in the meantime, seems to be well validated. However, questions of this kind deal with only one aspect of quantum theory. Beside them there shows up as equally important the question of the nature of the "transitions" themselves. On this point opinions seem to be divided. Many assume that the problem of transitions is not encompassed by quantum mechanics in its present form, but that here new conceptual developments will be necessary. I myself, impressed with the closed character of the logical nature of quantum mechanics, came to the presumption that this theory is complete and that the problem of transitions must be contained in it. I believe that I have now succeeded in proving this.

Bohr has already directed attention to the fact that all difficulties of principle associated with the quantum approach which meet us in the emission and absorption of light by atoms also occur in the interaction of atoms at short distances and consequently in collision processes. In collisions one deals not with mysterious wave fields, but exclusively with systems of material particles, subject to the formalism of quantum mechanics. I therefore attack the problem of investigating more closely the interaction of the free particle (α-ray or electron) and an arbitrary atom and of determining whether a description of a collision is not possible within the framework of existing theory.

Of the different forms of the theory only Schrödinger's has proved suitable for this process, and exactly for this reason I might regard it as the deepest formulation of the quantum laws. The course of my reasoning is the following.

If one wishes to calculate quantum mechanically the interaction of two systems,

† This report was originally intended for die Naturwissenschaften, but could not be accepted there for lack of space. I hope that its publication in this journal [Zcitschrift fr Physik] does not seem out of place [M.B.].

Originally published under the title, "Zur Quantenmechanik der Stossvorgnge," Zeitschrift fr Physik, 37, 863-67 (1926), icpinted in Dhumente der Naturnissenschaft, 1,4852 (1962) and in M. Born (1963); translation into English by J.A.W. and W.H.Z., 1981.

then, as is well known, one cannot, as in classical mechanics, pick out a state of the one system and determine how this is influenced by a state of the other system, since all states of both systems are coupled in a complicated way. This is true also in an aperiodic process, such as a collision, where a particle, let us say an electron, comes in from infinity and then goes off to infinity. There is no escape from the conclusion that, as well before as after collision, when the electron is far enough away and the coupling is small enough, a definite state must be specifiable for the atom and likewise a definite rectilinear motion for the electron. The problem is to formulate mathematically this asymptotic behavior of the coupled particles. I did not succeed in doing this with the matrix form of guantum mechanics, but did with the Schrödinger formulation.

According to Schrödinger, the atom in its nth quantum state is a vibration of a state function

of fixed frequency W_n^0/h spread over all of space. In particular, an electron moving in a straight line is such a vibratory phenomenon which corresponds to a plane wave. When two such waves interact, a complicated vibration arises. However, one sees immediately that one can determine it through its asymptotic behavior at infinity. Indeed one has nothing more than a "diffraction problem" in which an incoming plane wave is refracted or scattered at an atom. In place of the boundary conditions which one uses in optics for the description of the diffraction diaphragm, one has here the potential energy of interaction between the atom and the electron.

The task is clear. We have to solve the Schrödinger wave equation for the system atom-plus-electron subject to the boundary condition that the solution in a preselected direction of electron space goes over asymptotically into a plane wave with exactly this direction of propagation (the arriving electron). In a thus selected solution we are further interested principally in a behavior of the "scattered" wave at infinity, for it describes the behavior of the system after the collision. We spell this out a little further. Let $\psi_1^0(q_k), \psi_2^0(q_k), \ldots$ be the eigenfunctions of the unperturbed atom (we assume that there is only a discrete spectrum). The unperturbed electron, in straight-line motion, corresponds to eigenfunctions $\sin(2\pi/\lambda)(\alpha x + \beta y + \gamma z + \delta)$, a continuous manifold of plane waves. Their wavelength, according to de Broglie, is connected with the energy of translation τ by the relation $\tau = h^2/(2\mu\lambda^2)$. The eigenfunction of the unperturbed state in which the electron arrives from the $+z$ direction, is thus

$$\psi_{n,\tau}^0(q_k, z) = \psi_n^0(q_k)\sin(2\pi z/\lambda).$$

Now let $V(x, y, z; a_k)$ be the potential energy of interaction of the atom and the electron. One can then show with the help of a simple perturbation calculation that there is a uniquely determined solution of the Schrödinger equation with a potential V, which goes over asymptotically for $z \to +\infty$ into the above function.
The question is now how this solution behaves "after the collision."

The calculation gives this result: The scattered wave created by this perturbation has asymptotically at infinity the form:
$\psi_{n\tau}^1(x, y, z; q_k) = \sum_m \iint_{\alpha x+\beta y+\gamma z>0} d\omega \Phi_{n_\tau m}(\alpha, \beta, \gamma)\sin k_{n_\tau m}(\alpha x + \beta y + \gamma z + \delta)\psi_m^0(q_k)$.
This means that the perturbation, analyzed at infinity, can be regarded as a superposition of solutions of the unperturbed problem. If one calculates the energy belonging to the wavelength $\lambda_{n_\tau m}$ according to the de Broglie formula, one finds

$$W_{n_\tau m} = h\nu_{nm}^0 + \tau$$

where the ν_{nm}^0 are the frequencies of the unperturbed atom.
If one translates this result into terms of particles, only one interpretation is possible. $\Phi_{n_t m}(\alpha, \beta, \gamma)$ gives the probability* for the electron, arriving from the z direction, to be thrown out into the direction designated by the angles α, β, γ, with the phase change δ. Here its energy τ has increased by one quantum $h\nu_{nm}^0$ at the cost of the energy of the atom (collision of the first kind for $W_n^0 < W_m^0, h\nu_{nm}^0 < 0$; collision of the second kind $W_n^0 > W_m^0, h\nu_{nm}^0 > 0$).

Schrödinger's quantum mechanics therefore gives quite a definite answer to the question of the effect of the collision; but there is no question of any causal description. One gets no answer to the question, "what is the state after the collision," but only to the question, "how probable is a specificd outcome of the collision" (where naturally the quantum mechanical energy relation must be fulfilled).

Here the whole problem of determinism comes up. From the standpoint of our quantum mechanics there is no quantity which in any individual case causally fixes the consequence of the collision; but also experimentally we have so far no reason to believe that there are some inner properties of the atom which condition a definite outcome for the collision. Ought we to hope

later to discover such properties (like phases or the internal atomic motions) and determine them in individual cases? Or ought we to believe that the agreement of theory and experiment-as to the impossibility of prescribing conditions for a causal evolution-is a preestablished harmony founded on the nonexistence of such conditions? I myself am inclined to give up determinism in the world of atoms. But that is a philosophical question for which physical arguments alone are not decisive.

In practical terms indeterminism is present for experimental as well as for theoretical physicists. The "yield function" Φ so much investigated by experimentalists is now also sharply defined theoretically. One can determine it from the potential energy of interaction, $V(x, y, z; q_k)$. However, the calculations required

- Addition in proof: More careful consideration shows that the probability is proportional to the square of the quantity $\Phi_{n_\tau m}$.
  for this purpose are too complicated to communicate here. I will only clarify briefly the meaning of the function $\Phi_{n_c m}$. If, for example, the atom before the collision is in the normal state $n = 1$, then it follows from the equation

$$\tau + h\nu_{1m}^0 = \tau - h\nu_{m1}^0 = W_{1_\tau m} > 0$$

that, for an electron with less energy than the lowest excitation energy of the atom, the final state is also necessarily $m = 1$, or that $W_{1_\tau 1}$ must be equal to τ. Then we have "elastic reflection" of the electron with the yield function Φ_{y_τ}. If τ increases beyond the first excitation level, then there occurs, besides refledtion, also excitation with the yield $\Phi_{1_\tau 2}$, etc. If the target atom is in the excited state $n = 2$ and $\tau < h\nu_{21}^0$, then there occur reflection with yield $\Phi_{2\tau_2}$ and collisions of the second kind with the yield $\Phi_{2,1}$. If the kinetic energy $\tau > h\nu_{21}^0$, then further excitation is also possible.

The formulas thus reproduce completely the qualitative character of collisions. The quantitative predictions of the formulas for particular cases require extensive investigation.

I do not exclude the possibility that the strict connection of mechanics and statistics as it comes to light here will demand a revision of basic ideas of thermodynamics and statisticai mechanics.

I also believe that the problem of radiation of light-and irradiation-has to be handled in a way entirely analogous to the "boundary value problem" of the wave equation, and will lead to a rational theory of radiation damping and linebreadths in agreement with the theory of light quanta.

An extended treatment will appear shortly in this journal.

Commentary of Heisenberg (1967)

In July [1926] I visited my parents in Munich and on this occasion I heard a lecture given by Schrödinger for the physicists in Munich about his work on wave mechanics. It was thus that I first became acquainted with the interpretation Schrödinger wanted to give his mathematical formalism of wave mechanics, and I was very disturbed about the confusion with which I believed this would burden atomic theory. Unfortunately, nothing came of my atiempt during the discussion to put things in order. My argument that one could not even understand Planck's radiation law on the basis of Schrödinger's interpretation convinced no one. Wilhelm Wien, who held the chair of experimental physics at the University of Munich, answered rather sharply that one must really put an end to quantum jumps and the whole atomic mysticism, and the difficulties I had mentioned would certainly soon be solved by Schrödinger. I no longer remember whether or not I wrote to Bohr of this encounter in Munich. Be that as it may, Bohr shortly afterwards invited Schrödinger to Copenhagen and asked him not only to lecture on his

wave mechanics, but also to stay in Copenhagen so long that there would be adequate time to discuss the interpretation of quantum theory.

As far as I remember these discussions took place in Copenhagen around September 1926 and in particular they left me with a very strong impression of

24.5 I. 3 the Principle of Indeterminacy

Bohr's personality. For though Bohr was an unusually considerate and obliging person, he was abie in such a discussion, which concerned epistemological problems which he considered to be of vital importance, to insist fanatically and with almost terrifying relentlessness on complete clarity in all arguments. He would not give up, even after hours of struggling, before Schrodinger had admitted that this interpretation was insufficient, and could not even explain Planck's law. Every attempt from Schrödinger's side to get round this bitter result was slowly refuted point by point in infinitely laborious discussions. It was perhaps from over-exertion that after a few days Schrödinger became ill and had to lie abed as a guest in Bohr's home. Even here it was hard to get Bohr away fiom Schiödinget's bed and the phrase, "But, Schrödinger, you must at least admit that . . ." could be heard again and again. Once Schrödinger burst out almost desperately, "If one has to go on with these damned quantum jumps, then I'm sorry that I ever started to work on atomic theory." To which Bohr answered, "But the rest of us are so grateful that you did, for you have thus brought atomic physics a decisive step forward." Schrödinger finally left Copenhagen rather discouraged, while we at Bohr's Institute felt ihat at leasi Schröonger's interpretation of quantum theory, an interpretation rather too hastily arrived at using the classical wave-theories as models, was now disposed of, but that we still
lacked some important ideas before we could really reach a full understanding of quantum mechanics.

From now on the discussions between Bohr and his co-workers in Copenhagen became more and more concentrated on the central problem in quantum theory: how the mathematical formalism was to be applied to each individual problem, and thus how the frequently discussed paradoxes, such as e.g. the apparent contradiction between the wave and particle models, could be cleared up. Ever new imaginary experiments were thought up, each displaying the paradoxes in a more clear-cut way than its predecessors, and we tried to guess what answer nature would probably give to each experiment.

Left alone in Copenhagen [when Bohr went on vacation at the end of February 1927] I too was able to give my thoughts freer play, and I decided to make the above uncertainty the central point in the interpretation. Remembering a discussion I had had long before with a fellow student in Göttingen, I got the idea of investigating the possibility of determining the position of a particle with the aid of a gamma-ray microscope, and in this way soon arrived at an interpretation which I believed to be coherent and free of contradictions. I then wrote a long letter to Pauli, more or less the draft of a paper, and Pauli's answer was decidedly positive and encouraging. When Bohr returned from Norway, I was already able to present him with the first version of a paper along with the letter from

Pauli. At first Bohr was rather dissatisfied. He pointed out to me that certain statements in this first version were still incorrectly founded, and as he always insisted on relentless clarity in every detail, these points offended him deeply. Further, he had probably already grown familiar, while he was in Norway, with the concept of complementarity which would make it possible to take the dualism between the wave and particle picture as a suitable starting point för an interpretation. This concept of complementarity fitted well the fundamental philosophical attitude which he had always had, and in which the limitations of our means of expressing ourselves entered as a central philosophical problem. He therefore took objection to the fact that I had not started from the dualism between particles and waves. After several weeks

of discussion, which were not devoid of stress, we soon concluded, not least thanks to Oskar Klein's participation, that we really meant the same, and that the uncertainty relations were just a special case of the more general complementarity principle. Thus, I sent my improved paper to the printer and Bohr prepared a detailed publication on complementarity.

Commentary of Rosenfeld (1971a)

Bohr was now impatient to come to grips with the outstanding epistemological issue. He was convinced that in the quantum theory of matter just as in that of radiation, one faced an irreducible particle-wavedualisin, anditseemed to him that the way was clear to the
lucidation of its epistemological sigificance. The emphasis must be laid here on the role of a scientific theory as a means of unambiguous communication of experience. In atomic theory it is found convenient to use for this purpose, according to the circumstances, either the language appropriate to the description of wave phenomena, or the language of particle mechanics, both modes of description being subject to essential limitations: it is a necessary task of the theory to formulate these limitations so as to fix the conditions of validity of each type of idealized description. Night after night in the first months of 1927, Bohr and Heisenberg pondered together over these questions; again, they were at loggerheads over the strategy: Bohr expected the answer would follow from a direct analysis of the definition of the idealized concepts, Heisenberg argued that the answer was hidden in the formal structure of the theory and that a closer scrutiny of this structure should bring it to light.

Towards the end of February, they parted, after a last fruitless discussion, Bohr having decided to seek a much needed recreation in the snowy hills of Norway. On the same night, however, Heisenberg had an inspiration that put him on the right track. He vividly remembered a discussion he had with Einstein a year before about the new quantum mechanics; his attempt at arguing that a good theory ought only to operate with observable quantities had elicited from Einstein the pointed retort, which had made a strong impression on him: "Only the theory itself can decide what is and is not observable."

This remark, he thought, was the key to the whole problem: all one had to do was to investigate, for each given phenomenon, which conclusions one could draw from its theoretical analysis, according to the principles of quantum mechanics, about possible limitations to its observability.

Heisenberg based his argumentation on very general "indeterminacy relations" which he had shown to be deeply rooted in the formal structure of quantum mechanics. The mechanical variables are always associated in "conjugate" pairs . . . .

Heisenberg naturally wanted to clinch the argument by analyzing particular examples of idealized experimental situations which could illustrate the application of the indeterminacy relations. He was anxious, in particular, to demonstrate the impossibility of assigning a trajectory to a moving electron: let us imagine we should attempt to localize the electron by means of a microscope: in order to achieve sufficient resolution, we should have to illuminate it with radiation of very high frequency, in the range of the gamma-rays emitted by radioactive substances; the scattering of such photons by the electron, according to the theory of the Compton effect, would throw the electron completely out of the path prescribed by its previous velocity. Bohr's reaction to these considerations was very characteristic: he at once realized that Heisenberg again had forged the weapon that was needed io master the problem, but was soon dissatisfied with the smart way in
which he was wielding it. The idea of bringing out the origin of the limitations of classical description by analyzing imaginary processes of observation was of the type that would appeal to Bohr, and he took it up eageriy, but in his own infinitely patient manner, examining the argument from all sides, leaving no point in the shadow. He was not long to discover that Heisenberg's discussion of the gamma-ray microscope touched only one aspect of the question-

the role of the frequency of the radiation, but did not really go to the heart of the matter: the Compton recoil of the electron could only be a source of indeterminacy for its momentum to the extent to which the scattering process itself is not completely determined. Now, he pointed out, the formation of an image in a microscope requires a bundle of rays of finite aperture, and it is this latitude in the direction of the photons impunging on the electron that implies a corresponding latitude in the electron recoil. On the other hand a large aperture increases the accuracy of the electron's localization; and a simple computation shows that the two contrary effects of the aperture on the indeterminacies of position and momentum are such as to impose on their product the lower limit given by the relation (2), independently of the aperture and of the frequency of the radiation.

Bohr looked upon such imaginary experiments in a rather different spirit from Heisenberg. The later was satisfied with the knowledge that he had now established a complete correspondence between the mathematical structure of the theory and the usual physical concepts describing the various aspects of experience; the indeterminacy relations were part of this correspondence, their physical content could be exhibited by the discussion of appropriate experiments. Bohr wanted to pursue the epistemological analysis one step further, and in particular to understand the logical nature of the mutual exclusion of the two aspects opposed in the particle-wave dualism. From this point of view the indeterminacy relations appear in a new light. The conjugate variables for which they hold refer, respectively, to the two mutually exclusive classical pictures centered on the idealized concepts of particle and wave: to the former are attached the momentum and energy variables, to the latter the coordinates of space and time. The particle concept is used to describe the exchanges of momentum and energy between atomic systems, and between such systems and radiation: it is the physical support, so to speak, of the conservation laws governing such exchanges, irrespectively of any spacetime localization. The wave concept, or rather the derived density function, describes the localization of atomic systems and the distribution of radiation in space and time; it excludes the specification of momentum and energy, since only a wave of infinite spatial and temporal extension can have a sharply defined periodicity, necessary for a sharp definition of momentum and encrgy. The odd situation we meet in atomic theory is the necessity of making use of these two conflicting pictures in order io deal with all the conditions under which we can observe the atomic phenomena. The indeterminacy relations are therefore essential to ensure the consistency of the theory, by assigning the limits within which the use of classical concepts belonging to the two extreme pictures may be applied without contradiction. For this novel logical relationship, which called in Bohr's mind echoes of his philosophical meditations over the duality of our mental activity, he proposed the name "complementarity," conscious that he was here breaking new ground in epistemology.

The solemnity of the occasion did not dawn immediately upon Heisenberg. He was not well-disposed toward the idea of a particle-wave dualism, and Bohr was himself still struggling to find the right expression for the new ideas that were taking shape in his mind. However eager he was to let Heisenberg share his elation at the prospects they disclosed, his eagerness was not sufficiently matched by clarity to make impression on a reluctant interlocutor. The memory of the fruitless discussions with Schrödinger still lingered in Heisenberg's mind, and he regarded with deep suspicion any attempt to make more than formal use of the concept of matter wave. He stressed, quite rightly, that according to the correspondence principle, it is the particle concept that has a direct physical meaning with respect to atomic constituents, whereas matter waves are merely mathematical auxiliaries. To this Bohr would oppose the case of radiation, where the correspondence principle, on the contrary, points to the electromagnetic waves as the fundamental classical concept, and leaves only a symbolic part to the photons. Moreover, Oskar

Klein, who was then Bohr's assistant, had carefully discussed the relation of matter waves to the correspondence principle, and shown how the latter gave as reliable a guidance for the physical interpretation of wave mechanics as for that of the quantum algebra: but Klein's paper had not found grace with Heisenberg. He stuck obstinately to the view that his own scheme of quantum mechanics formed a sufficient basis for a complete description of the phenomena.

Matters did not improve when Bohr was shown the hastily written paper in which Heisenberg had developed his arguments. Bohr started handling the manuscript as he would have done one of his own, namely as a rough draft which could eventually lead to an acceptable iexi; and with his usual optimism, he expected Heisenberg to welcome this scrutiny: the latter was simply annoyed to find Bohr raising so many objections to the inaccuracios and careless statements of the paper, and proposing new formulations with which he was in no mood to agree. There is no telling how things would have ended if Pauli's arrival on the scene had not relieved the tension. Heisenberg had informed Pauli of his ideas and received from him approval and encouragement; now, Pauli was in a position both to lend Bohr a dispassionate ear and to gain a hearing from Heisenberg. He was able to explain to the latter that there was no disagreement between his and Bohr's ways of analyzing the physical content of atomic theory, but that Bohr
had gone further and deeper in the analysis of its logical structure. Even so, all Heisenberg could be persuaded to do about his paper was to append to it a "remark added on the proof," in which he declared in substance that he had missed essential points, whose clarification would be found in a forthcoming paper by Bohr. This addendum must
have puzzled many readers: it is not often that the announcement of a decisive progress in our insight into the workings of nature is qualified by such a warning.

As to Bohr's "forthcoming" publication, more than a year elapsed before it appeared in print...

24.6 I. 3 the Physical Content of Quantum Kinematics and Mechanics

Werner Heisenberg

First we define the terms velocity, energy, etc. (for example, for an electron) which remain valid in quantum mechanics. It is shown that canonically conjugate quantities can be deter-nained simultaneously only with a characteristic indeterminacy (§1). This indeterminacy is the real basis for the occurrence of statistical relations in quantum mechanics. Its mathematical formulation is given by the Dirac-Jordan theory (§2). Starting from the basic principles thus obtained, we show how microscopic processes can be understood by way of quantum mechanics (§3). To illustrate the theory, a few special gedankenexperiments are discussed ($\widehat{8}4$).

We believe we understand the physical content of a theory when we can see its qualitative experimental consequences in all simple cases and when at the same time we have checked that the application of the theory never contains inner contradictions. For example, we believe that we understand the physical content of Einstein's concept of a closed 3-dimensional space because we can visualize consistently the experimental consequences of this concept. Of course these consequences contradict our everyday physical concepts of space and time. However, we can convince ourselves that the possibility of employing usual space-time concepts at cosmolog-ical distances can be justified neither by logic nor by observation. The physical interpretation of quantum mechanics is still full of internal discrepancies, which show themselves in arguments about continuity versus discontinuity and particle versus wave. Already from this circumstance one might conclude that no interpretation of quantum mechanics is possible which uses ordi-nary kinematical and mechanical concepts. Of course, quantum mechanics arose exactly out of the attempt to break with all ordinary kinematic concepts and to put in their place relations

between concrete and experimentally determinable numbers. Moreover, as this enterprise seems to have succeeded, the mathematical scheme of quantum mechanics needs no revision. Equally unnecessary is a revision of space-time geometry at small distances, as we can make the quantummechanical laws approximate the classical ones arbitrarily closely by choosing sufficiently great masses, even when arbitrarily small distances and times come into question. But that a revision of kinematical and mechanical concepts is necessary

Originally published under the title, "lher den anschanlichen Inhalt der quantentheoretischen Kinematik und Mechanik," Zeitschrift fiir Physik, 43, 172-98 (1927); reprinted in Dokumente der Naturwissenscheft, 4,9-35 (1963); translation into English by J.A.W. und W.H.Z., 1981.

seems to follow directly from the basic equations of quantum mechanics. When a definite mass m is given, in our everyday physics it is perfectly understandable to speak of the position and the velocity of the center of gravity of this mass. In quantum mechanics, however, the relation $\mathbf{pq} - \mathbf{qp} = -i\hbar$ between mass, position, and velocity is believed to hold. Therefore we have good reason to become suspicious every time uncritical use is made of the words "position" and "yelocity." When one admits that discontinuities are somehow typical of processes that take place in small regions and in short times, then a contradiction between the concepts of "position" and "velocity" is quite plausible. If one considers, for example, the motion of a particle in one dimension, then in continuum theory one will be able to draw (Fig. 1) a worldline $x(t)$ for the track of the particle (more precisely, its center of gravity), the tangent of which gives the velocity at every instant. In contrast, in a theory based on discontinuity there might be in place of this curve a series of points at finite separation (Fig. 2) In this case it is clearly meaningless to speak about one velocity at one position (1) because one velocity can only be defined by two positions and (2), conversely, because any one point is associated with two velocities.

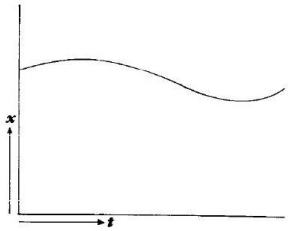


FIGURE 1

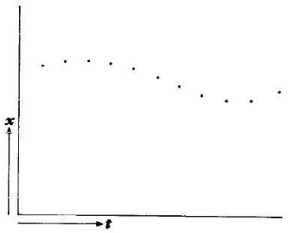


FIGURE 2

The question therefore arises whether, through a more precise analysis of these kinematic and mechanical concepts, it might be possible to clear up the contradictions evident up to now in the physical interpretations of quantum mechanics and to arrive at a physical understanding of the quantum-mechanical formulas.*

- The present work has arisen from efforts and desires to which other investigators have already given clear expression, before the development of quantum mechanics. I call attention here especially to Bohr's papers on the basic postulates of quantum theory (for example, Zeits. f. Physik, 13, 117 [1923]) and Einstion's discussions on the connection between wave field and light quanta The problems dealt with here are discussed most clearly in recent times, and the problems arising are partly answered, by W. Pauli ("Quantentheorie," Handbuch der Physik, Vol. XXIII, cited hereafter as l.c.); quantum mechanics has changed only slightly the formulation of these problems as given by Pauli It is also a special pleasure to thank here Herrn Pauli for the repeated stimulus 1 have received from our oral and written discussions, which have contributed decisively to the present work.

§1. Concepts: Position, Path, Velocity, Energy

In order to be able to follow the quantum-mechanical behavior of any object one has to know the mass of this object and its interactions with any fields and other objects. Only then can

the Hamiltonian function be written down for the quantummechanical system. (The following considerations ordinarily refer to nonrelativistic quantum mechanics, as the laws of quantum electrodynamics are still very incompletely known.)* About the "Gestalt" (construction) of the object any further assumption is unnecessary; one most usefully employs the word "Gestalt" to designate the totality of these interactions.

When one wants to be clear about what is to be understood by the words "position of the object," for example of the electron (relative to a given frame of reference), then one must specify definite experiments with whose help one plans to measure the "position of the electron"; otherwise this word has no meaning. There is no shortage of such experiments, which in principle even aiiow one to determine the "position of the electron" with arbitrary accuracy. For example, let one illuminate the electron and observe it under a microscope. Then the highest attainable accuracy in the measurement of position is governed by the wavelength of the light. However, in principle one can build, say, a γ-ray microscope and with it carry out the determination of position with as much accuracy as one wants. In this measurement there is an important feature, the Compton effect. Every observation of scattered light coming from the electron presupposes a photoelectric cffect (in the eye, on the photographic plate, in the photocell) and can therefore also be so interpreted that a light quantum hits the electron, is reflected or scattered, and then, once again bent by the lens of the microscope, produces the photoeffect. At the instant when position is determined–therefore, at the moment when the photon is scattered by the electron-the electron undergoes a discontinuous change in momentum. This change is the greater the smaller the wavelength of the light employed - that is, the more exact the determination of the position. At the instant at which the position of the electron is known, its momentum therefore can be known up to magnitudes which correspond to that discontinuous change. Thus, the more precisely the position is determined, the less precisely the momentum is known, and conversely. In this circumstance we see a direct physical interpretation of the equation $\mathbf{pq} - \mathbf{qp} = -i\hbar$. Let q_1 be the precision with which the value q is known (q_1 is, say, the mean error of q), therefore here the wavelength of the light. Let p_1 be the precision with which the value p is determinable; that is, here, the discontinuous change of p in the Compton effect. Then, according to the elementary laws of the Compton effect p_1 and q_1 stand in the relation

- Quite recently, however, great advances in this domain have been made in the papers of P. Dirac [Proc. Roy. Soc. A114, 243 (1927) and papers to appear subscquently].

$$p_1 q_1 \sim h. \tag{1}$$

That this relation (1) is a straightforward mathematical consequence of the rule $\mathbf{pq} - \mathbf{qp} = -i\hbar$ will be shown below. Here we can note that equation (1) is a precise expression for the facts which one earlier sought to describe by the division of phase space into cells of magnitude h. For the determination of the position of the electron one can also do other experiments-for example, collision experiments. A precise measurement of the position demands collisions with very fast particles, because for slow electrons the diffraction phenomena-which, according to Einstein, are consequences of de Broglie waves (as, for example, in the Ramsauer effect)-prevent a sharp specification of location. In a precise measurement of position the momentum of the electron again changes discontinuously. An elementary estimate of the precision using the formulas for de Broglie waves leads once more to relation (1).

Throughout this discussion the concept of "position of the electron" seems well enough defined, and only a word need be added about the "size" of the electron. When two very fast particles hit the electron one after the other within a very short time interval Δt, then the positions of the electron defined by the two particles lie very close together at a distance Δl.

From the regularities which are observed for α-particles we conclude that Δl can be pushed down to a magnitude of the order of 10^{-12} cm if only Δt is sufficiently small and particles a re selected with sufficiently great velocity. This is what we mean when we say that the electron is a corpuscle whose radius is not greater than 10^{-12} cm.

We turn now to the concept of "path of the electron." By path we understand a series of points in space (in a given reference system) which the electron takes as "positions" one after the other. As we already know what is to be understood by "position at a definite iime," no new difficulties occur here. Nevertheless, it is easy to recognize that, for example, the often used expression, the "1s orbit of the electron in the hydrogen atom," from our point of view has no sense. In order to measure this 1s "path" we have to illuminate the atom with light whose wavelength is considerably shorter than 10^{-8} cm. However, a single photon of such light is enough to eject the electron completely from its "path" (so that only a single point of such a path can be defined). Therefore here the word "path" has no definable meaning. This conclusion can already be deduced, without knowledge of the recent theories, simply from the experimental possibilities.

In contrast, the contemplated measurement of position can be carried out on many atoms in a 1s state. (In principle, atoms in a given "stationary" state can be selected, for example, by the Stern-Gerlach experiment.) There must therefore exist for a definite state-for example, the 1s state-of the atom a probability function for the location of the electron which corresponds to the mean value for the classical orbit, averaged over all phases, and which can be determined through
the measurement with an arbitrary precision. According to Born,* this function is given by $\psi_{1s}(q)\bar{\psi}_{1s}(q)$ where $\psi_{1s}(q)$ designates the Schrödinger wave function belonging to the 1s state. With a view to later generalizations I should like to saywith Dirac and Jordan-that the probability is given by $S(1s,q)\bar{S}(1s,q)$, where $S(1\text{ s},\text{q})$ designates that column of the matrix $S(E,q)$ of transformation from E to q that belongs to the energy $E = E_{1\text{ s}}$.

In the fact that in quantum theory only the probability distribution of the position of the electrons can be given for a definite state, such as 1 s , one can recognize, with Born and Jordan, a characteristically statistical feature of quantum theory as contrasted to classical theory However, one can say, if one will, with Dirac, that the statistics are brought in by our experiments. For plainly even in classical theory only the probability of a definite position for the electron can be given as long as we do not know the phase of [the motion of the election in] the atom. The distinction between classical and quantum mechanics consists rather in this: classically we can always think of the phase as determined through suitable experiments. In reality, however, this is impossible, because every experiment for the determination of phase perturbs or changes the atom. In a definite stationary "state" of the atom, the phases are in principle indeterminate, as one can see as a direct consequence of the familiar equations

$$\mathbf{Et} - \mathbf{tE} = -i\hbar \quad \text{or} \quad \mathbf{Jw} - \mathbf{wJ} = -i\hbar,$$

where $\bar{J}$ is the action variable and $\mathbf{w}$ is the angle variable.
The word "velocity" can easily be defined for an object by measurements when the motion is free of force. For example, one can illuminate the object with red light and by way of the Doppler effect in the scattered light determine the velocity of the particle. The determination of the velocity is the more exact the longer the wavelength of the light that is used, as then the change in velocity of the particle, per light quantum, by way of the Compton effect is so much less. The determination of position becomes correspondingly inexact, in agreement with equation (1). If one wants to measure the velocity of the electron in the atom at a definite instant, then, for example, one will let the nuclear charge and the forces arising

- The statistical interpretation of de Broglie waves was first formulated by A. Einstein (Sitzungsber. d. preussische Akad. d. Wiss., p. 3 [1925]). This statistical feature of

quantum mechanics then played an essential role in M. Born, W. Heisenberg, and P. Jordan, Quantenmechanik II (Zeits. f. Physik, 35, 557 [1926]), especially chapter 4, §3, and P. Jordan (Zeits. f. Physik, 37, 376 [1926]). It was analyzed mathematically in a seminal paper of M. Born (Zeits. f. Physik, 38, 803 [1926]) and used for the interpretation of collision phenomena. One finds how to base the probability picture on the theory of the transformation of matrices in the following papers. W. Heisenherg (7.pits *f* Physik, 40, 501 [1926]), P. Jordan (Zeits. f. Physik, 40, 661 [1926]), W. Pauli (remark in Zeits. f. Physik, 41, 81 [1927]), P. Dirac (Proc. Roy. Soc. A113, 621 [1926]), and P. Jordan (Zeits. f. Physik, 40, 809 [1926]). The statistical side of quantum mechanics is discussed more generally in P. Jordan (Naturwiss., 15, 105 [1927]) and M. Born (Naturwiss, 15, 238 [1927]).

from the other electrons suddenly be taken away, so that the motion from then on is force-free, and one will then carry out the measurement described above. As above, one can again easily convince oneself that a [momentum] function $p(t)$ cannot be defined for a given state-such as the 1 s-state-of an atom. On the contrary, there is again a probability function for p in this state which according to Dirac and Jordan has the value $S(1\text{ s},p)\bar{S}(1\text{ s},p)$. Here $S(1\text{ s},p)$ again designates that column of the matrix $S(E,p)$-that transforms from $\mathbf{E}$ to $\mathbf{p}$-which belongs to $E = E_{1\text{ s}}$.

Finally we come to experiments which allow one to measure the energy or the value of the action variable J. Such experiments are especially important hecause only with their help can we define what we mean when we speak of the discontinuous change of the energy and of J. The Franck-Hertz collision experiments allow one to hase the measurement of the energy of the atom on the measurement of the energy of electrons in rectilinear motion, because of the validity of the law of conservation of energy in quantum theory. This measurement in principle can be carricd out with arbitrary accuracy if only one forgoes the simultaneous determination of the position of the electron or its phase (see the determination of p, above), corresponding to the relation $\mathbf{Et} - \mathbf{tE} = -i\hbar$. The Stern-Gerlach experiment allows one to determine the magnetic or an average electric moment of the atom, and therefore to measure quantities which depend only on the action variable J. The phases remain undetermined in principle. It makes as little sense to speak of the frequency of the light wave at a definite instant as of the energy of an atom at a definite moment. Contespondingly, in the Stern-Geriach experiment the accuracy of the energy measurement decreases as we shorten the time during which the atom is under the influence of the deflecting field.* Specifically, an upper bound is given for the deviating force through the circumstance that the potential energy of that deflecting force can at most vary inside the beam by an amount which is considerably smaller than the differences in energy of the stationary states. Only then will a determination of the energy of the stationary states be at all possible. Let E_1 be an amount of energy which satisfies this condition (E_1 also fixes the precision of the energy measurement). Then E_1/d specifies the highest allowable value for the deflecting force, if d is the breadth of the beam (measurable through the spacing of the slits employed). The angular deviation of the atomic beam is then $E_1 t_1/dp$, where we designate by t_1 the time during which the atoms are under the influence of the deflecting field, and by p the momentum of the atoms in the direction of the beam. This deflection must be of at least the same order of magnitude as the natural broadening of the beam brought about by the diffraction by the slits, if any measurement is to be possible. The diffraction angle is roughly λ/d if λ denotes the de Broglie wavelength; thus,

- In this connection see W. Pauli. l.c.. p. 61.

$$\lambda/d \sim E_1 t_1/dp,$$

or, as $\lambda = h/p$,

$$E_1 t_1 \sim h. \tag{2}$$

This equation contesponds io equation (1) and shows how a precise determination of energy can only be obtained at the cost of a corresponding uncertainty in the time.

§2. The Dirac-Jordan Theory

We might summarize and generalize the results of the preceding section in this statement: All concepts which can be used in classical theory for the description of a mechanical system can also be defined exactly for atomic processes in analogy to the classical concepts. The experiments which provide such a definition themselves suffer an indeterminacy introduced purely by the observational procedures we use when we ask of them the simultaneous determination of two canonically conjugate quantities. The magnitude of this indeterminacy is given by relation (1) (generalized to any canonically conjugate quantities whatsoever). It is natural in this respect to compare quantum theory with special relativity. According to relativity, the word "simultaneous" cannot be defined except through experiments in which the velocity of light enters in an essential way. If there existed a "sharper" definition of simultaneity, as, for example, signals which propagate infinitely fast, then relativity theory would be impossible. However, because there are no such signals, or, rather, because already in the definition of simultaneity the velocity of light appears, there is room left for the postulate of the constancy of the speed of light so that this postulate does not contradict any meaningful use of the words "position, velocity, time." We find a similar situation with the definition of the concepts of "position of an electron" and "velocity" in quantum theory. All experiments which we can use for the definition of these terms necessarily contain the uncertainty implied by equation (1), even though they permit one to define exactly the concepts p and q taken in isolation. If there existed experiments which allowed simultaneously a "sharper" determination of p and q than equation (1) permits, then quantum mechanics would be impossible. Thus only the uncertainty which is specified by equation (1) creates room for the validity of the relations which find their most pregnant expression in the quantum-mechanical commutation relations,

$$\mathbf{pq} - \mathbf{qp} = -i\hbar$$

That uncertainty makes possible this equation without requiring that the physical meaning of the quantities p and q be changed.

For those physical phenomena whose quantum-mechanical formulation is still unknown (for example, electrodynamics), equation (1) makes a demand which may be useful for the discovery of the new laws. For quantum mechanics equation (1) can be derived from the Dirac-Jordan formulation by a slight generalization. If, for any definite state variable η we determine the position q of the electron as q' with an uncertainty q_1, then we can express this fact by a probability amplitude $S(\eta, q)$ which differs appreciably from zero only in a region of spread q_1 near q'. For example, one can write

$$S(\eta, q) \text{ proportional to } \exp\left[-(q-q')^2/2q_1^2 - (ip'/\hbar)(q-q')\right] \tag{3a}$$

with therefore

$$S\bar{S}' \text{ proportional to } \exp\left[-(q-q')^2/q_1^2\right]. \tag{3b}$$

Then for the probability amplitude for any given value of p we have

$$S(\eta, p) = \int S(\eta, q) S(q, p) dq \tag{4}$$

For $S(q, p)$, according to Jordan, we can write

$$S(q, p) = \exp(ipq/\hbar) \tag{5}$$

Then, according to (4), $S(\eta, p)$ differs appreciably from zero only for values of p for which $(p - p')\, q_1/\hbar$ is not significantly greater than 1 . Specifically, employing (3), we find $S(\eta, p)$ is proportional to

$$\int \exp\left[i\,(p - p')\, q/\hbar - (q - q')^2\, /2q_i^2\right] dq$$

that is, proportional to

$$\exp\left[-\,(p - p')^2\, /2p_1^2 + iq'\,(p - p')\, /\hbar\right]$$

and thus

$$S\bar{S} \text{ is proportional to } \exp\left[-\,(p - p')^2\, /p_1^2\right]$$

where

$$p_1 q_1 = \hbar \tag{(6}$$

The assumption (3) for $S(\eta, q)$ corresponds therefore to the experimental fact tha the value p' is measured for p and the value q' for q [with the limit (6) on the precision].

From the purely mathematical point of view it is characteristic of the Dirac

Jordan formulation of quantum mechanics that the relations between $\mathbf{p}, \mathbf{q}, \mathbf{E}$, etc. can be described as equations connecting very general matrices in such a way that any predetermined quantum-theoretic quantity appears as a diagonal matrix. The possibility of writing things in such a way is evident when one pictures the matrices as tensors (for example, moment-of-inertia tensors) in a multidimensional space between which there are mathematical connections. One can always pick the axis of the coordinate system in which one expresses these relations along the principal axes of one of these tensors. Finally, one also can always characterize the mathematical relation between two tensors A and B through the transformation equations which take a coordinate system oriented along the principal axes of A over into another oriented along the principal axes of B. This latter formulation corresponds to the Schrödinger theory. In contrast, one will view Dirac's q-number formulation as the formulation of quantum mechanics that is really "invariant" and independent of all coordinate systems. When we want to derive physical results from that mathematical framework, then we have to associate numbers with the quantum-theoretical magnitudes-that is, with the matrices (or "tensors" in multidimensional space). This task is to be understood in these terms: In that multicimensional space a definite direction is arbitrarily prescribed (by the nature of the experimental setup); and it is asked what is the "value" of the matrix (for example, in that picture, what is the value of the moment of incria) in this given direction. This question only has a well-defined meaning when the given direction coincides with the direction of one of the principal axes of that matrix. In this case there is an exact answer for the question. But also when the prescribed direction differs only little from one of the principal axes of the matrix one can still speak of the "value" of the matrix in the prescribed direction up to a definite uncertainty determined by the angle between the two directions. One can therefore say that associated with every quantum-theoretical quantity or matrix is a number which gives its "value" within a certain definite statistical error. The

statistical error depends on the coordinate system. For every quantum-theoretical quantity there exists a coordinate system in which the statistical error for this quantity is zero. Therefore a definite experiment can never give exact information on all quantumtheoretical quantities. Rather, it divides physical quantities into "known" and "unknown" (or more and less accurately known quantities) in a way characteristic of the experiment in question. The results of two experiments can be derived exactly one from the other only then when the two experiments divide the physical quantities in the same way into "known" and "unknown" (that is, when the tensors in that multidimensional space frequently invoked-for ease of visualization-are "looked at" in both experiments from the same direction). When two experiments use different divisions into "known" and "unknown," then their results can be related only statistically.

For a more detailed discussion of this statistical connection let a gedankenexperiment be considered. Let a Stern-Gerlach atomic beam be sent first through
a field F_1 which is so strongly inhomogeneous in the direction of the beam that it induces many transitions by sudden reversal in the force on the spin. Then let the atomic beam run free up to a definite distance from F_1. But there let a second field F_2 begin, as inhomogeneous as F_1. Between F_1 and F_2 let it be possible to measure the number of atoms in the different stationary states through an optionally applied magnetic field. Let all radiation by the atoms be neglected. If we know that an atom was in a state of energy E_n before it passed F_1, then we can express this fact by ascribing to the atom a wave function-for example, in p space - with the definite energy E_n and the undetermined phase β_n,

$$S(E_n, p) = \psi(E_n, p) \exp[-i(E_n/h)(\alpha + \beta_n)].$$

After passage through the field F_1, this function is changed into*

$$S(E_n, p) \xrightarrow{F_1} \sum_m c_{nm} \psi(E_m, p) \exp[-i(E_m/h)(\alpha + \beta_m)] \tag{7}$$

Here we can make some arbitrary determination of the β_m so that the c_{nm} are uniquely determined by F_1. The matrix c_{nm} transforms the energy values before the transition through F_1 to the values after the transition. If after F_1 we carry out a determination of the stationary state, say, by use of an inhomogeneous magnetic field, then we will find that the atom has jumped from the nth state to the m th state with a probability $c_{nm}\bar{c}_{nm}$. When we find experimentally that an atom has indeed jumped to the m th state, then we have to ascribe to it in all calculations thereafter, not the function $\sum_m c_{nm} S_m$, but simply the function S_m with an undetermined phase. Through the experimental determination, " m th state," we select out of the multitude of different possibilities (c_{nm}) a definite one, m. However, ai the same time we disturb everything that was still contained in the phase relations between the quantities c_{nm}, as detailed below. In the transition of the atomic beam through F_2, what happened at F_1 repeats itself. Let d_{nm} be the coefficients of the transformation matrix which transform the energies before F_2 to the energies after F_2. If no determination of the state is carried out between F_1 and F_2, then the eigenfunction is transformed according to the following scheme,

$$S(E_n, p) \xrightarrow{F_1} \sum_m c_{nm} S(E_m, p) \xrightarrow{F_2} \sum_n \sum_l c_{nm} d_{ml} S(E_l, p) \tag{8}$$

Let $\sum_m c_{nm} d_{ml}$ be called e_{nl}. If the stationary state of the atom is determined beyond F_2, then one will find the state l with the probability $c_{nl}\bar{e}_{nl}$. In contrast, if between F_1 and F_2 one determines the state - and finds for it the value E_m-then

- See P. Dirac (Proc. Roy. Soc. A112. 661 [1926]) and M. Born (Leits. f. Phyik, 40. 167 [1926]).
  the probability for "l" beyond F_2 is given by $d_{ml}\bar{d}_{ml}$. In many repetitions of the entire

experiment (in which each time the state is determined between F_1 and F_2) one will therefore observe the state l, beyond F_2, with the relative frequency $Z_{nl} = \sum_m c_{nm}\bar{c}_{nm}d_{ml}\bar{d}_{ml}$. This expression does not agree at all with $e_{nl}\bar{e}_{nl}$. For this reason Jordan (l.c.) has spoken of an "interference of probabilities." I cannot agree. The two kinds of experiments which lead respectively to $e_{nl}\bar{e}_{nl}$ and Z_{nl} are physically distinct. In one case the atom experiences no disturbance between F_1 and F_2. In the other case it is perturbed by the apparatus which determines its stationary state. This apparatus has as a consequence that the "phase" of the atom changes by an amount that is in principle uncheckable, as the momentum of an electron likewise changes with a determination of its position (see §1). The magnetic field for the determination of the state between F_1 and F_2 will separate the eigenvalues E. In the observation of the path of the atomic beam the atoms are slowed down by statisticaily different and uncheckable amounts (I think here, say, of Wilson cloudchamber pictures). This has as a consequence that the final transformation matrix (from the energy value before entry into F_1 to the energy after exit from F_2) is no longer given by $\sum c_{nm}d_{ml}$, but every term in this sum has additionally an unknown phase factor. No expectation is therefore open to us, except that the mean value of $e_{nl}\bar{e}_{nl}$ averaged over aii these expected phase alterations is equal to Z_{nl}. A simple calculation confirms that this is the case. We can therefore deduce from one experiment the possible results of another by definite statistical rules. The other experiment itself selects out of the plenitude of all possibilities a quite definite one, and thereby limits the possibilities for all later experiments. Such an interpretation of the equation for the transformation matrix S or the Schrödinger wave equation is only possible because the sum of solutions is again a solution. In this circumstance we see the deep significance of the linearity of Schrödinger wave equations. On that account they can be understood only as equations for waves in phase space; and on that account we may regard as hopeless every attempt to replace these equations by nonlinear equations, for example in the relativistic case (for more than one electron).

§3. The Transition from Micro- to Macromechanics

It seems to me that the concepts of kinematics and mechanics in quantum theory are sufficiently clarified by the analysis of the words "position of an electron," "velocity," "energy," etc., in the preceding sections that physical understanding of macroscopic processes from the standpoint of quantum mechanics must also be possible. The transition from micro- to macromechanics has already been treated by Schrödinger,* but I do not believe that Schrödinger's considerations

- E. Schrödinger, Naturwiss., 14, 664 (1926).
get to the heart of the problem, and this is why: According to Schrödinger, in a high state of excitation a sum of eigenfunctions ought to be able to give a wave packet of limited extent which-through periodic changes in its form-will carry out the periodic motions of the classical "electron." There is an argument against this outlook: If the wave packet had such properties as ascribed to it by this view, then the radiation sent out by the atom would be representable as a Fourier series in which the frequencies of the higher vibrations were integer multiples of the basic frequency. The frequencies of the spectral lines sent out by the atom are, however, according to quantum mechanics, never integer multiples of the basic frequency-except in the special case of the harmonic oscillator. Thus Schrödinger's reasoning is only viable for the case of the harmonic oscillator treated by him; in all other cases a wave packet spreads out in the course of time over the whole immediate neighborhood of the atom. The higher the state of excitation of the atom, the slower is that spreading of the wave packet. However, if one waits long enough it happens.

The reasoning developed above about the radiation sent out by the atom might at first sight be used against all experiments which look for a direct transition from quantum to classical mechanics at high quantum numbers. For that reason the attempt was made earlier to circumvent such reasoning by referring to the natural radiation broadening of stationary states - certainly wrongly, first of all because this way out is blocked already in the case of the hydrogen atom on account of the weakness of the radiation for high states, and secondly, because the transition from quantum to classical mechanics ought to be understandable without caliing on electrodynamics. Bohr* has aiready refeired many times to these well-known difficulties which stand in the way of a direct connection between quantum and classical theory. We have spelled them out again here so explicitly only because in recent times they seem to be forgotten.

I believe that one can fruitfully formulate the origin of the classical "orbit" in this way: the "orbit" comes into being only when we observe it. For example, let an atom be given in a state of excitation $n = 1000$. The dimensions of the orbit in this case are already relatively large so that, in accordance with §1, it is enough to use light of relatively low wavelength to determine the position of the electron. If the position determination is not to be too fuzzy then the Compton recoil will put the atom in some state of excitation between, say, 950 and 1050. Simultaneously, the momentum of the electron can be determined from the Doppler effect with a precision given by (1). One can characterize the experimental finding by a wavepacket, or, better, a probability-amplitude packet, in q-space of a spread given by the wavelength of the light used, and built up primarily out of eigenfunctions between the 950 th and 1050th eigenfunction-and by a corresponding packet in p-space. Let a new determination of position be made after some time with the same precision. Its result, according to §2, can be predicted only statistically. All
positions count as likely (with calculable probability) which lie within the bounds of the now broadened wavepacket. The situation would be no different in classical theory, for there too the result of the second position measurement would be predictable only statistically because of the uncertainty in the first measurement. Also, the orbits of classical theory would spread out like the wavepacket. However, statistical laws themselves are different in quantum mechanics and in classical theory. The second determination of the position selects a definite " q " from the totality of possibilities and limits the options for all subsequent measurements. After the second position determination the results of later measurements can only be calculated when one again ascribes to the electron a "smaller" wavepacket of extension λ (wavelength of the light used in the observation). Thus every position determination reduces the wavepacket back to its original extension λ. The "values" of the quantities $\mathbf{p}, \mathbf{q}$ are known throughout all the experiments with a certain precision. The values of $\mathbf{p}$ and $\mathbf{q}$ stay within the precision limits fixed by the classical equations of motion. This can be seen directly from the quantum-mechanical equations,

$$\dot{\mathbf{p}} = -\hat{\imath}\mathbf{H}/\hat{\imath}\mathbf{q}; \quad \dot{\mathbf{q}} = \hat{\imath}\mathbf{H}/\hat{\imath}\mathbf{p}. \tag{9}$$

However, the orbit, as noted earlier, can be calculated only statistically from the initial conditions, a circumstance that one can consider as a consequence of the fundamental indeterminism of the initial conditions. The statistical laws are different for quantum mechanics and classical theory. This distinction, under appropriate circumstances, can give rise to gross macroscopic differences between classical and quantum theory. Before I discuss an example, I should like to indicate how the transition, discussed above, to classical theory is formulated mathematically for a simple mechanical system, the force-free motion of a particle. In one dimension the equations of motion run

$$\mathbf{H} = \mathbf{p}^2/2m; \quad \dot{\mathbf{q}} = \mathbf{p}/m; \quad \dot{\mathbf{p}} = 0 \tag{10}$$

As time can be treated as a parameter (or "c-number") when there are no timedependent external forces, the solution of this equation is

$$\mathbf{q} = \mathbf{p}_0 t/m + \mathbf{q}_0; \quad \mathbf{p} = \mathbf{p}_0 \tag{11}$$

where $\mathbf{p}_0$ and $\boldsymbol{q}_0$ are the momentum and the position at the time $t = 0$. At $t = 0$ the value $q_0 = q'$ is measured with accuracy q_1, and $p_0 = p'$ with accuracy p_1 [see equations (3) to (6)]. In order to draw conclusions from the "values" of $\mathbf{p}_o$ and $\mathbf{q}_0$ about the "values" of $\mathbf{q}$ at the time t, one must find-according to Dirac and Jordan-that transformation function which transforms all matrices in the
representation* in which $\mathbf{q}_0$ is diagonal to that representation in which $\mathbf{q}$ is diagonal. In the matrix scheme in which $\mathbf{q}_0$ is diagonal, $\mathbf{p}_0$ can be replaced by the operator - $i\hbar\hat{r}/\hat{c}q_0$. According to Dirac [l.c. equation (11)] the desired transformation amplitude $S(q_0, q)$ satisfies the differential equation,

$$\{-i(ht/m)\hat{\imath}/\hat{\imath}q_0 + q_0\} S(q_0, q) = qS(q_0, q) \tag{12}$$

or

$$-i(\hbar t/m)\hat{\imath}S/\hat{c}q_0 = (q_0 - q) S(q_0, q)$$

[with the solution]

$$S(q_0, q) = \text{ const } \exp\left[(im/ht)\int (q - q_0)\, dq_0\right] \tag{13}$$

$S\bar{S}$ is therefore independent of q_0. In other words, if at the time $t = 0$ we know $\tilde{q}_0$ exactiy, then at any time $t > \hat{0}$ all values of q are equally probable; that is, the probability that q lies in any finite region is quite nil. Physically this is already clear without further investigation. Thus the exact determination of q_0 leads to an intinitely large Compton recoil. The same would naturally apply for an arbitrary mechanical system. If, however, q_0 is known at the time $t = 0$ only within the range q_1, and p_0 in the range p_1 [see equation (3)], then

$$S(\eta, q_0) = \text{ const } \exp\left[-(q_0 - q')^2/2q_1^2 + (i/h)p'(q_0 - q')\right]$$

and the probability [amplitude] function for q is to be calculated according to the formula,

$$S(\eta, q) = \int S(\eta, q_0) S(q_0, q)\, dq_0$$

The result is
$S(\eta, q) = \text{const} \int \exp\left\{(im/\hbar t)\left[q_0(q - tp'/m) - q_0^2/2\right] - (q' - q_0)^2/2q_1^2; dq_0\right.$.
With the abbreviation

$$\beta = th/mq_1^2 \tag{15}$$

the exponent in (14) becomes

- The word "representation," not employed by Heisenberg himself, is introduced here for clarity. He uses the phrase "matrix scheme." (Translators' note.)

$$-\left\{q_0^2(1 + i/\beta) - 2q_0\left[q' + i(q - tp'/m)/\beta\right] + q'^2; /2q_1^2\right.$$

The term with q'^2 can be taken into the constant (q-independent factor) and the integration gives

$$S(\eta,\eta) = \text{ const } \exp\left\{\left[q' + i\left(\bar{q} - t\bar{p}'/m\right)/\beta\right]^2 / \left[2(1+i/\beta)q_1^2\right]\right\}$$
$$= \text{ const } \exp - \left\{\left[\left(q - tp'/m - i\beta q'\right)^2 (1 - i/\beta)\right] / \left[2q_1^2\left(1+\beta^2\right)\right]\right\}. \qquad (16)$$

It follows that

$$S(\eta,q)\bar{S}(\eta,q) = \text{ const } \exp - \left\{\left[q - tp'/m - q'\right]^2 / q_1^2\left(1+\beta^2\right)\right\} \qquad (17)$$

Thus the electron is located at the time t at the position $tp'/m + q'$ with a spread $q_1\left(1 \quad | \quad \beta^2\right)^{1/2}$. The "wavepacket" or, better, "probability packet" has expanded by the factor $\left(1+\beta^2\right)^{1/2}$. According to (15), β is proportional to the time t, inversely proportional to the mass, as is entirely plausible, and inversely proportional to q_1^2. Too much precision in q_0 produces great uncertainty in p_0 and thus leads to a large uncertainty in q. The parameter η which we have brought in above for formal reasons might be left out here in all formulas, as it does not enter the calculation. To illustrate that the difference between the classical and the quantum statistical laws leads to gross macroscopic differences between the results of the two theorics, let the reflection of a beam of electrons at a grating be discussed briefly. When the spacing of the rulings is of the order of the de Broglie wavelength of the electrons, then refiection occurs in definite, discrete directions like the refiection of light at a grating. What classical theory gives is grossly and macroscopically different. Nevertheless, from the orbit of an individual electron we can in no way find a contradiction with a classical theory. We might if we could, direct the electron, say, to a definite point on a grating ruling, and then verify that the reflection there violates classical theory. However, when we want to determine the position of the electron so precisely that we can say at what point on a grating ruling it hits, then the electron acquires through this position determination a large velocity, and the de Broglie wavelength of the electron becomes so much shorter that now the reflection really can and will take place approximately as predicted classically, without violating the laws of the quantum theory.

§4. Discussion of a Few Special Idealized Experiments

According to the physical interpretation of quantum theory aimed at here, the time of transitions or "quantum jumps" must be as concrete and determinable by measurement as, say, energies in stationary states. The spread within which such an instant is specifiable is given according to equation (2) by $h/\Delta E$, if ΔE designates
the change of energy in a quantum jump.* We consider, for example, the following experiment. An atom, at time $t = 0$ in state $n = 2$ may transit, via radiation, to the ground state, $n = 1$. Then, in analogy to equation (7), we can ascribe to the atom the eigenfunction

$$S(t,p) = e^{-2t}\psi\left(E_2,p\right)e^{-iE_2t'h} + \left(1 - e^{-2at}\right)^{1/2}\psi\left(E_1,p\right)e^{-iE_1t/h} \qquad (18)$$

if we assume that the radiation damping is expressed in a factor of the form e^{-a1} in the eigenfunction (the real dependence is perhaps not so simple). This atom is sent through an inhomogeneous magnetic field for the determination of its energy, level, as is usual in the Stern-Gerlach experiment; yet we also have the inhomqgeneous field follow the atomic beam over a long stretch of its path. The consequent acceleration we will measure, say, in this way: we divide the entire stretch that the atomic beam pursues in the magnetic field into short sections, at the end of each of which we determine the deviation of the beam. Depending on the velocity of the atomic beam, the division into intervals of space corresponds for the atom tc division into small time intervals Δt. According to §1, equation (2), there corresponds to a time interval Δt

a spread in energy of $h/\Delta t$. The probability of measuring the definite energy E can be directly deduced from $S(p,E)$ and is therefore calcuiated for the interval from $n\Delta t$ to ($n+1$) Δt as,

$$\underset{n\Delta t-(n+1)\Delta t}{S(p,E)} = \int_{n\Delta t}^{(n+1)\Delta t} S(p,t)e^{iEt_th}dt$$

If the determination "state $n=2$ " is made at the time $(n+1)\Delta t$, then for everything later one must ascribe to the atom not the eigenfunction (18) but one which results from (18) when t is replaced by $t-(n+1)\Delta t$. If, on the contrary, one finds "state $n=1$," then from that point on one has to attribute to the atom the eigenfunction

$$\psi\left(E_1,p\right)e^{-iE_{1i},n}.$$

Thus one will first find for a series of intervals Δt "state $n=2$," then steadily "state $n=1$." In order that a distinction between the two states will still be possible, Δt cannot be shrunk below $h/\Delta E$. Thus the instant of the transition is determinable within this spread. We imply an experiment of the kind just sketchec quite in the spirit of the old formulation of quantum theory founded by Planck Einstein, and Bohr when we speak of the discontinuous change of the energy. A: such an experiment can in principle be carried out, an agreement about its outcomf must be possible.

In Bohr's basic postulates of quantum theory, the energy of an atom has the

advantage-just as do the values of the action variables J-over other determinants of the motion (position of the electron, etc.) in that its numerical value can always be given. This preferred position which the energy has over other quantum-mechanical quantities it owes only to the circumstance that it represents an integral of the equations of motion for closed systems (the energy matrix $\mathbf{E}$ is a constant). For open systems, in contrast, the cncrgy is not singled out over any other quantum-mechanical quantity. In particular, one will be able to devise experiments in which the phases, w, of the atom are precisely measurable, but in which then the energy remains in principle undetermined, corresponding to the relation $\mathfrak{J}w - w\ \mathrm{J} = -i\hbar$ or $J_iw_i \sim h$. Resonance floorescence is such an experiment. If one irradiates an atom with an eigenfrequency, say $v_{12} = \left(E_2 - E_1\right)/h$, then the atom vibrates in phase with the external radiation. Then, even in principle, it makes no sense to ask in which state, $\boldsymbol{E}_1$ on $\boldsymbol{E}_2$, the atom is thus vibrating. The phase relation between atom and external radiation may be determined, for example, by the phase relations of large numbers of atoms with one another ([R. W.] Wood's experiments). If one prefers to avoid experiments with radiation then one can also measure the phase relation by carrying out exact position determinations on the electron in the sense of §1 at different times relative to the phase of the light impinging (on many atoms). A "wave function," say, of the form,

$$S(q,t) = c_2\psi_2\left(E_2,q\right)e^{-i(E_2t+\beta)/\hbar} + \left(1-c_2^2\right)^{1/2}\psi_1\left(E_1,q\right)e^{-iE_1t/\hbar} \tag{19}$$

can be ascribed to the individual atom. Here c_2 depends on the strength and β on the phase of the incident light. The probability of a definite position q is thus

$$\begin{aligned} S(q,t)\bar{S}(q,t) =& c_2^2\psi_2\bar{\psi}_2 + \left(1-c_2^2\right)\psi_1\bar{\psi}_1 \\ &+ c_2\left(1-c_2^2\right)^{1/2}\left\{\psi_2\bar{\psi}_1e^{-i[(E_2-E_1)t+\beta]/h} + \bar{\psi}_2\psi_1e^{+i[(E_2-E_1)t+\beta]/h}\right\} \end{aligned} \tag{20}$$

8

- Compare W. Pauli, l.c., p. 12.

The periodic term in (20) is experimentally distinguishable from the unperiodic ones, as the determinations of position can be carried out for different phases of the incident light.

In a well-known idealized experiment proposed by Bohr, the atoms of a SternGerlach atomic beam are first excited to a resonance fluorescence at a definite state by incident radiation. After a little way they go through an inhomogeneous magnetic field. The radiation emerging from the atoms can be observed during the whole path, before and after the magnetic field. Before the atoms enter the magnetic field, ordinary resonance radiation takes place; that is, as in dispersion theory, it must be assumed that all atoms send out spherical waves in phase with the incident light. The latter view at first sight contradicts the result that a crude application of the quantum theory of light or the basic rules of quantum theory would give. Thus from this view one would conclude that only a few atoms are raised to the
"upper state" through absorption of the light quantum, and that therefore the entire resonance radiation arises from a few intensively radiating centers. It therefore seemed natural in earlier times to say that the concept of light quanta ought to be brought in here only to account for the balance of energy and momentum, and that "in reality" all atoms in the ground state radiate weak and coherent spherical waves. After the atoms have passed the magnetic fieid, however, there can hardly be any doubt that the atomic beam has divided into two beams of which one corresponds to atoms in the upper state, the other in the lower. If now the atoms in the lower state were to radiate, then we would have a gross violation of the law of conservation of energy. For all the energy of excitation resides in the beam with atoms in the upper state. Still less can there be any doubt that past the magnetic field only the "upper state" beam sends out light, and indeed incoherent light, from the few intensively radiating atoms in the upper state. As Bohr has shown, this idealized experiment makes it especially clear that care is often needed in applying the concept of "stationary state." The formulation of quantum theory deveioped here alows a discussion of the Bohr experiment to be carried through without any difficulty. In the external radiation field the phases of the atoms ate determined. Therefore it is meaningless to speak of the "energy of the atom." Also, after the atom has left the radiation field one is not entitled to say that it is in a definite stationary state, insofai as one enquires about the coherence properties of the radiation. However, one can set up an experiment to find out in what state the atom is. The result of this experiment can be stated only statistically. Such an experiment is really performed by the inhomogeneous magnetic field. Beyond the magnetic field the energies of the atoms are well determined and therefore the phases are indeterminate. The resulting radiation is incoherent and comes only from atoms in the upper state. The magnetic field determines the energies and therefore destruys the plase relation. Bohr's idealized experiment is a very beautiful illustration of the fact that the energy of the atom "in reality" is not a number but a matrix. The conservation law holds for the energy matrix and therefore also for the value of the energy as precisely as it can be measured. In mathematical terms the lifting of the phase relation can be traced out as follows, for example. Let Q be the coordinates of the center of gravity of the atom, so that one ascribes to the atom, instead of (19), the eigenfunction

$$S(Q,t)S(q,t) = S(Q,q,t) \tag{21}$$

Here $S(Q,t)$ is a function that, like $S(\eta,q)$ in (16), differs from zero only in a small neighborhood of a point in Q-space and propagates with the velocity of the atoms in the direction of the beam. The probability of a relative amplitude q regardless of Q is given by the integral of
$S(Q,q,t)\bar{S}(Q,q,t)$
over Q-that is, through (20). However, the eigenfunction (21) will change by a calculable amount in a magnetic field and, on account of the different deviation of atoms in the upper and lower state, will have changed beyond the magnetic field into
$S(Q,q,t) - c_2 S_2(Q,t)\psi_2(E_2,q)\,e^{-i(E_2 t+\beta)/\hbar} + (1-c_2^2)^{1/2}\,S_1(Q,t)\psi_1(E_1,q)\,e^{-iE_1 t/\hbar}$.(22)

Here $S_1(Q,t)$ and $S_2(Q,t)$ will be functions in Q-space which differ from zero only in the small neighborhood of a point; but this point is different for S_1 and S_2. The product $S_1 S_2$ is therefore zero everywhere. The probability of a relative amplitude q and a definite value Q is therefore

$$S(Q,q,t)\bar{S}(Q,q,t) = c_2^2 S_2 \bar{S}_2 \psi_2 \bar{\psi}_2 + \left(1 - c_2^2\right) S_1 \bar{S}_1 \psi_1 \bar{\psi}_1 \tag{23}$$

The periodic term of (20) has disappeared and with it the possibility of measuring a phase relation. The statistical result of position determinations will always be the same, whatever the phase of the incident radiation. We may assume that experiments with radiation, the theory of which has not yet been developed, will give the same results about phase relations between atoms and incident radiation.

Finally let us examine the connection* of equation (2), $E_1 t_1 \sim h$, with a complex of problems which Ehrenfest and other investigators have discussed on the basis of Bohr's correspondence principle in two important papers. † Ehrenfest and Toiman speak of "weak quantization" when the quantized periodic motion is interrupted through quantum jumps or rather perturbations in intervals of time which can be regarded as not very long compared to the periods of the system. These cases should reveal not only the exact quantum energy values but also energy values which do not differ too much from the quantum values, and these with a smaller and qualitatively predictable a priori probability. In quantum mechanics this behavior is to be interpreted in these terms. As the energy is really changed by external perturbations or quantum jumps, every energy measurement, insofar as it is to he unique, must be done in the time between two perturbations. In this way an upper bound is specified for t_1 in the sense of §1. Therefore we measure the energy value E_0 of a quantized state also only within a spread $E_1 \sim h/t_1$. Here the question is meaningless even in principle whether the system "really" takes on with the correspondingly lower statistical weight such energy values E as deviate from E_0, or whether their experimental realization is to be attributed only to the inaccuracy of the measurement. If t_1 is smaller than the period of the system then it is no longer meaningful to speak of discrete stationary states or discrete energy values.

*** W. Pauli drew my attention to this connection.**

* P. Ehrentest and G. Breit (Zeits. /. Physik, 9. 20/ [1922]) and P. Ehrenjest and K. C. Toiman (Phys. Rev., 24. 287 [1924]). See also the discussion in N. Bohr, Grundpostulate der Quantentheorie, l.c.

Ehrenfest and Breit in a similar connection draw attention to the following paradox. A rotator, which we will visualize as a gear-wheel, is provided with an attachment which after f revolutions of the wheel exactly reverses the direction of its rotation. For example, let the gear-wheel mesh with a toothed sliding member which moves on a straight line between two stops. The slider hits a stop after a definite number of rotations and in that way reverses the rotation of the gearwheel. The true period T of the system is long in comparison with the rotation period t of the wheel. The discrete energy levels are densely packed-and the denser the packing, the greater the value of T. From the standpoint of consistent quantum theory all stationary states have the same statistical weight. Therefore, for sufficiently great T, practically all energy values occur with equal frequency, in opposition to what would be expected for the rotator. We may sharpen this paradox a little before we treat it from our standpoint. Thus, in order to determine whether the system takes on the discrete energy values helonging to the pure rotator exclusively or particularly often, or whether it assumes with equal probability all possible values (that is, values which correspond to the small energy interval h/T), a time t_1 suffices which is small relative to T (but $2 > t$). In other words, although the long period plays no part at all in such measurements, it appears to express itself in the fact that all possible energy values can occur. We are of the view that, in reality also, such experiments

for the determination of the total energy of the system would give all possible energy values with equal probability. The factor responsible for this outcome is not the big period T, but the sliding member. Even if the system sometimes happens to have an energy identical with the quantized energy value of the simple rotator, it can be modificd casily by external forces acting on the stop-to states which do not correspond to the quantization of the simple rotator.* The coupled system, rotator-plus-slider, indeed shows a periodicity entirely different from that of the rotator. The solution of the paradox lies rather in a different circumstance. When we want to measure the energy of the rotator alone, we must first break the coupling between the rotator and the slider. In classical theory, when the mass of the slider is sufficiently small, the coupling can be broken without a change in energy; and there, consequently, the energy of the entire system can be equated to that of the rotator (for small slider mass). In quantum mechanics the energy of interaction between slider and rotator is at least of the same order of magnitude as the level spacing of the rotator (even for small slider mass there is a high zero point energy associated with the elastic interaction between rotator and slider). On decoupling, the slider and the rotator individually take their characteristic quantum energies. Consequently, insofar as we are able to measure the energy values of the rotator alone we always find the quantum energy values with experimental accuracy. Even for

*According to Ehrenfest and Breit this cannot happen, or can happen only rarely, through forces which act on the gear-wheel.

vanishing mass of the slider, however, the energy of the coupled system is different from the energy of the rotator. The energy of the coupled system can take on all possible values (consistent with the T-quantization) with equal probability.

Quantum kinematics and mechanics show far-reaching differences from the ordinary theory. The applicability of classical kinematics and mechanical concepts, however, can be justified neither from our laws of thought nor from experiment. The basis for this conclusion is relation (1), $p_1 q_1 \sim h$. As momentum, position, energy, etc. are precisely defined concepts, one does not need to complain that the basic equation (1) contains only qualitative predictions. Moreover, as we can think through qualitatively the experimental consequences of the theory in all simple cases, we will no longer have to lovk at quantum mechanics as unphysical and abstract.* Of course we would also like to be able to derive, if possible, the quantitative laws of quantum mechanics directly from the physical foundations-that is, essentially, from relation (1). On this account Jordan has sought to interpret the equation,

$$S(q, q'') = \int S(q, q')\, S(q', q'')\, dq'$$

as a probability relation. However, we cannot accept this interpretation (§2). We believe, rather, that for the time being the quantitative laws can be derived out of the physical foundations only by use of the principle of maximum simplicity. If, for example, the X-coordinate of the electron is no longer a "number" as can be concluded experimentally, according to equation (1), then the simplest assumption conceivable [that does not contradict (1)] is that this X-coordinate is a diagonal term of a matrix whose nondiagonal terms express themselves in an uncertainty or-by transformation-in other ways (see for example §4). The prediction that, say, the velocity in the X-direction is "in reality" not a number but the diagonal term of the matrix, is perhaps no more abstract and no more unvisualizable than the statement that the electric field strengths are "in reality" the time part of an antisymmetric tensor located in space-time. The phrase "in reality" here is as much and as little justified as it is in any mathematical description of natural processes. As soon as one accepts that all quantum-theoretical quantities are "in reality" matrices, the quantitative laws follow without difficulty.

If one assumes that the interpretation of quantum mechanics is already correct

- Schrödinger describes quantum mechanics as a formal theory of frightening, indeed repul-

sive, abstracturss and lack of visualizability. Certainiy one cannot overestimate the vaiue of the mathematical (and to that extent physical) mastery of the quantum-mechanical laws that Schrödinger's theory has made possible. However, as regards questions of physical interpretation and principle, the popular view of wave mechanics, as I see it, has actually deflected us from exactly those roads which were pointed out by the papers of Einstein and de Broglie on the one hand and by the papers of Bohr and by quantum mechanics on the other hand.

in its essential points, it may be permissible to outline briefly its consequences of principle. We have not assumed that quantum theory-in opposition to classical theory-is an essentially statistical theory in the sense that only statistical conclusions can be drawn from precise initial data. The well-known experiments of Geiger and Bothe, for example, speak directly against such an assumption. Rather, in all cases in which relations exist in classical theory between quantities which are really all exactly measurable, the corresponding exact relations also hold in quantum theory (laws of conservation of momentum and energy). But what is wrong in the sharp formulation of the law of causality, "When we know the present precisely, we can predict the future," is not the conclusion but the assumption. Even in principle we cannot know the present in all detail. For that reason everything observed is a selection from a plenitude of possibilities and a limitation on what is possible in the future. As the statistical character of quantum theory is so closely linked to the inexactness of all perceptions, one might be led to the presumption that behind the perceived statistical world there still hides a "real" world in which causality holds. But such speculations seem to us, to say it explicitiy, fruitless and senseless. Physics ought to describe only the correlation of observations. One can express the true state of affairs better in this way: Because all experiments are subject to the laws of quantum mechanics, and therefore to equation (1), it follows that quantum mechanics establishes the final failure of causality.

Addition in Proof

After the conclusion of the foregoing paper, more recent investigations of Bohr have led to a point of view which permits an essential deqpening and sharpening of the analysis of quantum-mechanical correlations attempted in this work. In this connection Bohr has brought to my attention that I have overlooked essential points in the course of several discussions in this paper. Above all, the uncertainty in our observation does not arise exclusively from the occurrence of discontinuities, but is tied directly to the demand that we ascribe equal validity to the quite different experiments which show up in the corpuscular theory on one hand, and in the wave theory on the other hand. In the use of an idealized gamma-ray microscope, for example, the necessary divergence of the bundle of rays must be taken into account. This has as one consequence that in the observation of the position of the electron the direction of the Compton recoil is only known with a spread which then leads to relation (1). Furthermore, it is not sufficiently stressed that the simple theory of the Compton effect, strictly speaking, only applies to free electrons. The consequent care needed in employing the uncertainty relation is, as Professor Bohr has explained, essential, among other things, for a comprehensive discussion of the transition from micro- to macromechanics. Finally, the discussion of resonance fluorescence is not entirely correct because the connection between
the phase of the light and that of the electronic motion is not so simple as was assumed. I owe great thanks to Professor Bohr for sharing with me at an early stage the results of these more recent investigations of his-to appear soon in a paper on the conceptual structure of quantum theory-and for discussing them with me.

Copenhagen, Institute for Theoretical Physics of the University.

24.7 I. 4 Complementarity

Commentary of Rosenfeld (1963)

Complementarity is no system, no doctrine with ready-made precepts. There is no via regia to it; no formal definition of it can even be found in Bohr's writings, and this worries many people. The French are shocked by this breach of the Cartesian rules; they blame Bohr for indulging in "clairobscur" and shrouding himself in "les brumes du Nord." The Germans in their thoroughness have been at work distinguishing several forms of complementarity and studying, in hundreds of pages, their relations to Kant. Pragmatic Americans have dissected complementarity with the scalpel of symbolic logic and undertaken to define this gentle art of the correct use of words without using any words at all. Bohr was content to teach by example. He often evoked the thinkers of the past who had intuitively recognized dialectical aspects of existence and endeavored to give them poetical or philosophical expression; our only advantage over these great men, he would observe, is that in physics we have been presented with such a simple and clear case of complementarity that we are able to study it in detail and thus arrive at a precise formulation of a logical relationship of universal scope. The nature of this relation he regarded as sufficiently illustrated by his analyses of the limits of validity of classical physical concepts.

Commentary of Rosenfeld (1971a; CONTINUED FROM §I. 3 above)

As to Rohr's "forthcoming" publication more than a year elapsed before il appeared in print: it was a much furbished version of a lecture he delivered. shortly after the events just retraced, at a physicists' conference in Como. He had the greatest misgivings about presenting his conception of complementarity to the community of physicists in a state which he judged immature; but he yicIded to the advice of his more practically-minded brother Harald. Upon the latter's urging, he even consented to write up a brief account, that could be promptly published in Nature, as a letter to the editor: but this letter never reached its destination. With the help of Klein, he actually managed to complete it just on the night of his reluctant departure for Como. However, when Klein came up to the Institute the next morning, and enquired whether the letter had been sent off, he learned that there had been a double hitch, of a kind to delight Freudians. Bohr had missed the night train, because he could not find his passport (which lay on his desk); he had departed by the next train, taking with him the famous letter.

Commentary of Heisenberg (1967; CONTINUED FROM §I. 3 above)

How closely the idea of complementarity was in accord with Bohr's older philosophical ideas became apparent through an episode, which, if I remember correctly, took place on a sailing trip from Copenhagen to Svendborg on the island Fyn. At that time Bohr and a colleague and friend uwned a sailing boat, the captain of which was the brilliant and extremely charming chemist Bjerrum. The distinguished surgeon Chievitz kept spirits high even in stormy weather, and the other friends contributed each in his way to this happy and untroubied existence. Bohr was full of the new interpretation of
quantum theory, and as the boat took us full sail southwards in sunshine, there was plenty of time to tell of this scientific event and to reflect philosophically on the nature of atomic theory. Bohr began by talking of the difficulties of language, of the limitations of all our means of expressing ourselves, which one had to take into account from the very beginning if one wants to practice science, and he explained how satisfying it was that this limitation had already been expressed in the foundation of atomic theory in a mathematically lucid way. Finally, one of the

friends remarked drily, "Bt, Nicls, this is not really new, you said exactly the same ten years ago."

24.8 I. 4 the Quantum Postulate and the Recent Development of Atomic Theory

Although it is with great pleasure that I follow the kind invitation of the presidency of the congress to give an account of the present state of the quantum theory in order to open a general discussion on this subject, which takes so central a position in modern physical science, it is with a certain hesitation that I enter on this task. Not only is the venerated originator of the theory present himself, but among the audience there will be several who, due to their participation in the remarkable recent development, will surely be more conversant with details of the highly developed formalism than I am. Still I shall try, by making use only of simple considerations and without going into any details of technical mathematical character, to describe to you a certain general point of view which I believe is suited to give an impression of the general trend of the development of the theory from its very beginning and which I hope will be helpful in order to harmonize the apparently conflicting views taken by different scientists. No subject indeed may be better suited than the quantum theory to mark the development of physics in the century passed since the death of the great genius, whom we are here assembled to commemorate. At the same time, just in a field like this where we are wandering on new paths and have to rely

Originally published in Nature, 121, 580 – 90 (1928). Reprinted in Niels Bohr (1934), Atomic Theory and the Description of Nature, Cambridge University Press, pp. 52-91, from which book this paper is reproduced here.

upon our own judgment in order to escape from the pitfalls surrounding us on all sides, we have perhaps morc occasion than ever at every step to be remindful of the work of the old masters who have prepared the ground and furnished us with our tools.

I. QUANTUM POSTULATE AND CAUSALITY

The quantum theory is characterized by the acknowledgment of a fundamental limitation in the classical physical ideas when applied to atomic phenomena. The situation thus created is of a peculiar nature, since our interpretation of the experimental material rests essentially upon the classical concepts. Notwithstanding the difficulties which, hence, are involved in the formulation of the quantum theory, it seems, as we shall see, that its essence may be expressed in the so-called quantum postulate, which attributes to any atomic process an essential discontinuity, or rather individuality, completely foreign to the classical theories and symbolized by Planck's quantum of action.

This postulate implies a renunciation as regards the causal spacc-time co-ordination of atomic processes. Indeed, our usual description of physical phenomena is based entirely on the idea that the phenomena concerned may be observed without disturbing them appreciably. This appears, for example, clearly in the theory of relativity, which has been so fruitful for the elucidation of the classical theories. As emphasized by Einstein, every observation or measurement ultimately rests on the coincidence of two independent events at the same spacetime point. Just these coincidences will not be affected by any differences which the space-time co-ordination

of different observers otherwise may exhibit. Now, the quantum postulate implies that any observation of atomic phenomena will involve an interaction with the agency of observation not to be neglected. Accordingly, an independent reality in the ordinary physical sense can neither be ascribed to the phenomena nor to the agencies of observation. After all, the concept of observation is in so far arbitrary as it depends upon which objects are included in the

system to he ohserved. Ultimately, every observation can, of course, be reduced to our sense perceptions. The circumstance, however, that in interpreting observations use has always to be made of theoretical notions entails that for every particular case it is a question of convenience at which point the concept of observation involving the quantum postulate with its inherent "irrationality" is brought in.

This situation has far-reaching consequences. On one hand, the definition of the state of a physical system, as ordinarily understood, claims the elimination of all external disturbances. But in that case, according to the quantum postulate, any observation will be impossible, and, above all, the concepts of space and time lose their immediate sense. On the other hand, if in order to make observation possible we permit certain interactions with suitable agencies of measurement, not belonging to the system, an unambiguous definition of the state of the system is naturally no longer possible, and there can be no question of causality in the ordinary sense of the word. The very nature of the quantum theory thus forces us to regard the space-time co-ordination and the claim of causality, the union of which characterizes the classical theories, as complementary but exclusive features of the
description, symbolizing the idealization of observation and definition respectively. Just as the relativity theory has taught us that the convenience of distinguishing sharply between space and time rests solely on the smallness of the velocities ordinarily met with compared to the velocity of light, we learn from the quantum theory that the appropriateness of our usual causal space-time description depends entirely upon the small value of the quantum of action as compared to the actions involved in ordinary sense perceptions. Indeed, in the description of atomic phenomena, the quantum postulate presents us with the task of developing a " complementarity" theory the consistency of which can be judged only by weighing the possibilities of definition and observation.

This view is already clearly brought out by the muchdiscussed question of the nature of light and the ultimate constituents of matter. As regards light, its propagation in space and time is adequately expressed by the electromagnetic theory. Especially the interference phenomena in vacuo and the optical properties of material media are completely governed by the wave theory superposition principle. Nevertheless, the conservation of energy and momentum during the interaction between radiation and matter, as evident in the photo-electric and Compton effect, finds its adequate expression just in the light quantum idea put forward by Einstein. As is well known, the doubts regarding the validity of the superposition principle, on one hand, and of the conservation laws, on the other, which were suggested by this apparent contradiction, have been definitely disproved through direct experiments. This situation would seem clearly to indicate the impossibility of a causal space-time descrip-
tion of the light phenomena. On one hand, in attempting to trace the laws of the time-spatial propagation of light according to the quantum postulate, we are confined to statistical considerations. On the other hand, the fulfilment of the claim of causality for the individual light processes, characterized by the quantum of action, entails a renunciation as regards the space-time description. Of course, there can be no question of a quite independent application of the ideas of space and time and of causality. The two views of the nature of light are rather to be considered as different attempts at an interpretation of experimental evidence in which the limitation of the classical concepts is expressed in complementary ways.

The problem of the nature of the constituents of matter presents us with an analogous situation. The individuality of the elementary electrical corpuscles is forced upon us by general evidence. Nevertheless, recent experience, above all the discovery of the selective reflection of electrons from metal crystals, requires the use of the wave theory superposition principle in accordance with the original ideas of L . de Broglie. Just as in the case of light, we have consequently in the question of the nature of matter, so far as we adhere to classical concepts, to face an inevitable dilemma which has to be regarded as the very expression of experimental

evidence. In fact, here again we are not dealing with contradictory but with complementary pictures of the phenomena, which only together offer a natural generalization of the classical mode of description. In the discussion of these questions, it must be kept in mind that, according to the view taken above, radiation in free space as well as isolated material particles are abstractions, their properties on the quantum theory being definable and observable only through their interaction with other systems. Nevertheless, these abstractions are, as we shall see, indispensable for a description of experience in connection with our ordinary space-time view.

The difficulties with which a causal space-time description is confronted in the quantum theory, and which have been the subject of repeated discussions, are now placed into the foreground by the recent development of the symbolic methods. An important contribution to the problem of a consistent application of these methods has been made lately by Heisenberg. In particular, he has stressed the peculiar reciprocal uncertainty which affects all measurements of atomic quantities. Before we enter upon his results, it will be advantageous to show how the complementary nature of the description appearing in this uncertainty is unavoidable already in an analysis of the most elementary concepts employed in interpreting experience.

2. QUANTUM OF ACTION AND KINEMATICS

The fundamental contrast between the quantum of action and the classical concepts is immediately apparent from the simple formulae which form the common foundation of the theory of light quanta and of the wave theory of material particles. If Planck's constant be denoted by h, as is well known,

$$E\tau = I\lambda = h, \tag{I}$$

where E and I are energy and momentum respectively, τ and λ the corresponding period of vibration and wavelength. In these formulae the two notions of light and also of matter enter in sharp contrast. While energy and momentum are associated with the concept of particles, and, hence, may be characterized according to the classical point of view by definite space-time co-ordinates, the period of vibration and wave-length refer to a plane harmonic wave train of unlimited extent in space and time. Only with the aid of the superposition principle does it become possible to attain a connection with the ordinary mode of description. Indeed, a limitation of the extent of the wave-fields in space and time can always be regarded as resulting from the interference of a group of elementary harmonic waves. As shown by de Broglie, the translational velocity of the individuals associated with the waves can be represented by just the so-called group-velocity. Let us denoie a plane elementary wave by

$$A\cos 2\pi\left(\nu t - x\sigma_x - y\sigma_y - z\sigma_z + \delta\right),$$

where A and δ are constants determining respectively the amplitude and the phase. The quantity $\nu = I/\tau$ is the frequency, $\sigma_x, \sigma_y, \sigma_z$ the wave numbers in the direction of the co-ordinate axes, which may be regarded as vector components of the wave number $\sigma = 1/\lambda$ in the directions of propagation. While the wave or phase velocity is given by ν/σ, the group-velocity is defined by $d\nu/d\sigma$. Now according to the relativity theory we have for a particle with the velocity v :

$$I = \frac{v}{c^2}E \text{ and } vdI = dE$$

where c denotes the velocity of light. Hence by equation (I) the phase velocity is c^2/v and the group-velocity v. The circumstance that the former is in general greater

than the velocity of light emphasizes the symbolic character of these considerations. At the same time, the possibility of identifying the velocity of the particle with the group-velocity indicates the field of application of space-time pictures in the quantum theory. Here the complementary character of the description appears, since the use of wave-groups is necessarily accompanied by a lack of sharpness in the definition of period and wave-length, and hence also in the definition of the corresponding energy and momentum as given by relation (1).

Rigorously speaking, a limited wave-field can only be obtained by the superposition of a manifold of elementary waves corresponding to all values of v and σ_x, σ_y, σ_z. But the order of magnitude of the mean difference between these values for two elementary waves in the group is given in the most favourable case by the condition

$$\underline{\Delta}t\underline{\Delta}v - \underline{\Delta}x\Delta\sigma_x = \Delta y\underline{\Delta}\sigma_y = \Delta z\underline{\Delta}\sigma_z = \mathrm{I}$$

where $\Delta t, \Delta x, \Delta y, \Delta z$ denote the extension of the wavefield in time and in the directions of space corresponding to the co-ordinate axes. These relations-well known from the theory of optical instruments, especialiy from Rayleigh's investigation of the resolving power of spectral apparatus-express the condition that the wave-trains extinguish each other by interference at the space-time boundary of the wave-field. They may be regarded also as signifying that the group as a whole has no phase in the same sense as the elementary waves. From equation (1) we find thus:

$$\Delta t\Delta E = \Delta x\Delta I_x = \Delta y\Delta I_y = \Delta z\Delta I_z = h \tag{2}$$

as determining the highest possible accuracy in the
definition of the energy and momentum of the individuals associated with the wave-field. In general, the conditions for attributing an energy and a momentum value to a wave-field by means of formula (1) are much less favourable. Even if the composition of the wavegroup corresponds in the beginning to the relations (2), it will in the course of time be subject to such changes that it becomes less and less suitable for representing an individual. It is this very circumstance which gives rise to the paradoxical character of the problem of the nature of light and of material particles. The limitation in the classical concepts expressed through relation (2), is, besides, closely connected with the limited validity of classical mechanics, which in the wave theory of matter corresponds to the geometrical optics in which the propagation of waves is depicted through "rays". Only in this limit can energy and momentum be unambiguously defined on the basis of space-time pictures. For a general definition of these concepts we are confined to the conservation laws, the rational formulation of which has been a fundamental problem for the symbolical methods to be mentioned below.

In the language of the relativity theory, the content of the relations (2) may be summarized in the statement that according to the quantum theory a general reciprocal relation exists between the maximum sharpness of definition of the space-time and energy-momentum vectors associated with the individuals. This circumstance may be regarded as a simple symbolical expression for the complementary nature of the space-time description and the claims of causality. At the same time, however, the general character of this relation makes it
possible to a certain extent to reconcile the conservation laws with the space-time co-ordination of observations, the idea of a coincidence of well-defined events in a space-time point being replaced by that of unsharply defined individuals within finite space-time regions.

This circumstance permits us to avoid the well-known paradoxes which are encountered in attempting to describe the scattering of radiation by free electrical particles as well as the collision of two such particles. According to the classical concepts, the description of the scattering requires a finite extent of the radiation in space and time, while in the change of the motion of the electron demanded by the quantum postulate one seemingly is dealing with an

instantaneous effect taking place at a definite point in space. Just as in the case of radiation, however, it is impossible to define momentum and energy for an electron without considering a finite spacetime region. Furthermore, an application of the conservation laws to the process implies that the accuracy of definition of the energy-momentum vector is the same for the radiation and the electron. In consequence, according to relation (2), the associated space-time regions can be given the same size for both individuals in interaction.

A similar remark applies to the collision between two material particles, although the significance of the quantum postulate for this phenomenon was disregarded before the necessity of the wave concept was realized. Here, this postulate does, indeed, represent the idea of the individuality of the particles which, transcending the space-time description, meets the claim of causality. While the physical content of the light-quantum idea is
wholly connected with the conservation theorems for energy and momentum, in the case of the electrical particles the electric charge has to be taken into account in this connection. It is scarcely necessary to mention that for a more detailed description of the interaction between individuals we cannot restrict ourselves to the facts expressed by formulae (1) and (2), but must resort to a procedure which allows us to take into account the coupling of the individuals, characterizing the interaction in question, where just the importance of the electric charge appears. As we shall see, such a procedure necessitates a further departure from visualization in the usual sense.

3. MEASUREMENTS IN The QUANTUM THEORY

In his investigations already mentioned on the consistency of the quantum-theoretical methods, Heisenberg has given the relation (2) as an expression for the maximum precision with which the space-time coordinates and momentum-energy components of a particle can be measured simultaneously. His view was based on the following consideration: On one hand, the co-ordinates of a particle can be measured with any desired degree of accuracy by using, for example, an optical instrument, provided radiation of sufficiently short wavelength is used for illumination. According to the quantum theory, however, the scattering of radiation from the object is always connected with a finite change in momentum, which is the larger the smaller the wave-length of the radiation used. The momentum of a particle, on the other hand, can be determined with any desired degree of accuracy by measuring, for example, the Doppler effect of the scattered radiation, provided the wave-length
of the radiation is so large that the effect of recoil can be neglected, but then the determination of the space coordinates of the particle becomes correspondingly less accurate.

The essence of this consideration is the inevitability of the quantum postulate in the estimation of the possibilities of measurement. A closer investigation of the possibilities of definition would still seem necessary in order to bring out the general complementary character of the description. Indeed, a discontinous change of energy and momentum during observation could not prevent us from ascribing accurate values to the spacetime co-ordinates, as well as to the momentum-energy components before and after the process. The reciprocal uncertainty which always affects the values of these quantities is, as will be clear from the preceding analysis, essentially an outcome of the limited accuracy with which changes in energy and momentum can be defined, when the wave-fields used for the determination of the spacetime co-ordinates of the particle are sufficiently small.

In using an optical instrument for determinations of position, it is necessary to remember that the formation of the image always requires a convergent beam of light. Denoting by λ the wave-length of the radiation used, and by ϵ the so-called numerical aperture, that is, the sine of half the angle of convergence, the resolving power of a microscope is given by the well-known expression $\lambda/2\epsilon$. Even if the object is illuminated by parallel light, so that the momentum h/λ of the incident light quantum is known both as regards magnitude and direction, the finite

value of the aperture will prevent an exact knowledge of the recoil accompanying the scattering. Also,
even if the momentum of the particle were accurately known before the scattering process, our knowledge of the component of momentum parallel to the focal plane after the observation would be affected by an uncertainty amounting to $2\epsilon h/\lambda$. The product of the least inaccuracies with which the positional co-ordinate and the component of momentum in a definite direction can be ascertained is therefore just given by formula (2). One might perhaps expect that in estimating the accuracy of determining the position, not only the convergence but also the length of the wave-train has to be taken into account, because the particle could change its place during the finite time of illumination. Due to the fact, however, that the exact knowledge of the wave-length is immaterial for the above estimate, it will be realized that for any value of the aperture the wave-train can always be taken so short that a change of position of the particle during the time of observation may be neglected in comparison to the lack of sharpness inherent in the determination of position due to the finite resolving power of the microscope.

In measuring momentum with the aid of the Doppler effect-with due regard to the Compton effect-one will employ a parallel wave-train. For the accuracy, however, with which the change in wave-length of the scattered radiation can be measured the extent of the wave-train in the direction of propagation is essential. If we assume that the directions of the incident and scattered radiation are parallel and opposite, respectively, to the direction of the position co-ordinate and momentum component to be measured, then $c\lambda/2l$ can be taken as a measure of the accuracy in the determination of the velocity, where l
denotes the length of the wave-train. For simplicity, we here have regarded the velocity of light as large compared to the velocity of the particle. If m represents the mass of the particle, then the uncertainty attached to the value of the momentum after observation is $cm\lambda/2l$. In this case the magnitude of the recoil, $2\bar{h}/\lambda$, is sufficiently well defined in order not to give rise to an appreciable uncertainty in the value of the momentum of the particle after observation. Indeed, the general theory of the Compton effect allows us to compute the momentum components in the direction of the radiation before and after the recoil from the wave-lengths of the incident and scattered radiation. Even if the positional co-ordinates of the particle were accurately known in the beginning, our knowledge of the position after observation nevertheless will be affected by an uncertainty. Indeed, on account of the impossibility of attributing a definite instant to the recoil, we know the mean velocity in the direction of observation during the scattering process only with an accuracy $2h/m\lambda$. The uncertainty in the position after observation hence is $2hl/mc\lambda$. Herc, too, the product of the inaccuracies in the measurement of position and momentum is thus given by the general formula (2).

Just as in the casc of the determination of position, the time of the process of observation for the determination of momentum may be made as short as is desired, if only the wave-length of the radiation used is sufficiently small. The fact that the recoil then gets larger does not, as we have seen, affect the accuracy of measurement. It should further be mentioned, that in referring to the velocity of a particle as we have here done repeatedly, the purpose
has only been to obtain a connection with the ordinary space-time description convenient in this case. As it appears already from the considerations of de Broglie mentioned above, the concept of velocity must always in the quantum theory be handled with caution. It will also be seen that an unambiguous definition of this concept is excluded by the quantum postulate. This is particularly to be remembered when comparing the results of successive observations. Indeed, the position of an individual at two given moments can be measured with any desired degree of accuracy; but if, from such measurements, we would calculate the velocity of the individual in the ordinary way, it must be clearly realized that we are dealing with an abstraction, from which no unambiguous information concerning the previous or future behaviour of the individual can be obtained.

According to the above considerations regarding the possibilities of definition of the properties of individuals, it will obviously make no difference in the discussion of the accuracy of measurements of position and momentum of a particle if collisions with other material particles are considered instead of scattering of radiation. In both cases, we see that the uncertainty in question equally affects the description of the agency of measurement and of the object. In fact, this uncertainty cannot be avoided in a description of the behaviour of individuals with respect to a co-ordinate system fixed in the ordinary way by means of solid bodies and unperturbable clocks. The experimental devices-opening and closing of apertures, etc.-are seen to permit only conclusions regarding the space-time extension of the associated wave-fields.

In tracing observations back to our sensations, once more regard has to be taken to the quantum postulate in connection with the perception of the agency of observation, be it through its direct action upon the eye or by means of suitable auxiliaries such as photographic plates, Wilson clouds, etc. It is easily seen, however, that the resulting additional statistical element will not influence the uncertainty in the description of the object. It might even be conjectured that the arbitrariness in what is regarded as object and what as agency of observation would open up a possibility of avoiding this uncertainty altogether. In connection with the measurement of the position of a particle, one might, for example, ask whether the momentum transmitted by the scattering could not be determined by means of the conservation theorem from a measurement of the change of momentum of the microscope-including light source and photographic plate-during the process of observation. A closer investigation shows, however, that such a measurement is impossible, if at the same time one wants to know the position of the microscope with sufficient accuracy. In fact, it follows from the experiences which have found expression in the wave theory of matter that the position of the centre of gravity of a body and its total momentum can only be defined within the limits of reciprocal accuracy given by relation (2).

Strictly speaking, the idea of observation belongs to the causal space-time way of description. Due to the general character of relation (2), however, this idea can be consistently utilized also in the quantum theory, if only the uncertainty expressed through this relation is taken into account. As remarked by Heisenberg, one
may even obtain an instructive illustration of the quantum-theoretical description of atomic (microscopic) phenomena by comparing this uncertainty with the uncertainty, due to imperfect measurements, inherently contained in any observation as considered in the ordinary description of natural phenomena. He remarks on that occasion that even in the case of macroscopic phenomena we may say, in a certain sense, that they are created by repeated observations. It must not be forgotten, however, that in the classical theories any succeeding observation permits a prediction of future events with cver-increasing accuracy, because ii improves our knowledge of the initial state of the system. According to the quantum theory, just the impossibility of neglecting the interaction with the agency of measurement means that every observation introduces a new uncontrollable element. Indeed, it follows from the above considerations that the measurement of the positional co-ordinates of a particle is accompanied not only by a finite change in the dynamical variables, but also the fixation of its position means a complete rupture in the causal description of its dynamical behaviour, while the determination of its momentum always implies a gap in the knowledge of its spatial propagation. Just this situation brings out most strikingly the complementary character of the description of atomic phenomena which appears as an inevitable consequence of the contrast between the quantum postulate and the distinction between object and agency of measurement, inherent in our very idea of observation.

4. CORRESPONDENCE PRINCIPLE AND MATRIX THEORY

Hitherto we have only regarded certain general features of the quantum problem. The situation

implies, however, that the main stress has to be laid on the formulation of the laws governing the interaction between the objects which we symbolize by the abstractions of isolated particles and radiation. Points of attack for this formulation are presented in the first place by the problem of atomic constitution. As is well known, it has been possible here, by means of an elementary use of classical concepts and in harmony with the quantum postulate, to throw light on essential aspects of experience. For example, the experiments regarding the excitation of spectra by electronic impacts and by radiation are adequately accounted for on the assumption of discrete stationary states and individual transition processes. This is primarily due to the circumstance that in these questions no closer description of the space-time behaviour of the processes is required.

Here the contrast with the ordinary way of description appears strikingly in the circumstance that spectral lines, which on the classical view would be ascribed to the same state of the atom, will, according to the quantum postulate, correspond to separate transition processes, between which the excited atom has a choice. Notwithstanding this contrast, however, a formal connection with the classical ideas could be obtained in the limit where the relative difference in the properties of neighbouring stationary states vanishes asymptotically and where in statistical applications the discontinuities may
be disregarded. Through this connection it was possible to a large extent to interpret the regularities of spectra on the basis of our ideas about the structure of the atom.

The aim of regarding the quantum theory as a rational generalization of the classical theories led to the formulation of the so-called correspondence principle. The utilization of this principle for the interpretation of spectroscopic results was based on a symbolical application of classical electrodynamics, in which the individual transition processes were each associated with a harmonic in the motion of the atomic particles to be expected according to ordinary mechanics. Except in the limit mentioned, where the relative difference between adjacent stationary states may be neglected, such a fragmentary application of the classical theorics could only in certain cases lead to a strictly quantitative description of the phenomena. Especially the connection developed by Ladenburg and Kramers between the classical treatment of dispersion and the statistical laws governing the radiative transition processes formulated by Einstein should be mentioned here. Although it was just Kramers' treatment of dispersion that gave important hints for the rational development of correspondence considerations, it is only through the quantum-theoretical methods created in the last few years that the general aims laid down in the principle mentioned have obtained an adequate formulation.

As is known, the new development was commenced in a fundamental paper by Heisenberg, where he succeeded in emancipating himself completely from the classical concept of motion by replacing from the very start the
ordinary kinematical and mechanical quantities by symbols which refer directly to the individual processes demanded by the quantum postulate. This was accomplished by substituting for the Fourier development of a classical mechanical quantity a matrix scheme, the elements of which symbolize purely harmonic vibrations and are associated with the possible transitions between stationary states. By requiring that the frequencies ascribed to the elements must always obey the combination principle for spectral lines, Heisenberg could introduce simple rules of calculation for the symbols which permit a direct quantum theoretical transcription of the fundamental equations of classical mechanics. This ingenious attack on the dynamical problem of atomic theory proved itself from the beginning to be an excecdingly powerful and fertile method for interpreting quantitatively the experimental results. Through the work of Born and Jordan, as well as of Dirac, the theory was given a formulation which can compete with classical mechanics as regards generality and consistency. Especially, the element characteristic of the quantum theory, Planck's constant, appears explicitly only in the algorithms to which the symbols, the so-called matrices, are subjected. In fact, matrices, which represent canonically

conjugated variables in the sense of the Hamiltonian equations, do not obey the commutative law of multiplication, but two such quantities, q and p, have to fulfil the exchange rule

$$pq - qp = \sqrt{-1}\frac{h}{2\pi}. \tag{3}$$

Indeed, this exchange relation expresses strikingly the symbolical character of the matrix formulation of the
quantum theory. The matrix theory has often been called a calculus with directly observable quantities. It must be remembered, however, that the procedure described is limited just to those problems, in which in applying the quantum postulate the space-time description may largely be disregarded, and the question of observation in the proper sense therefore placed in the background.

In pursuing further the correspondence of the quantum laws with classical mechanics, the stress placed on the statistical character of the quantum-theoretical description, which is brought in by the quantum postulate, has been of fundamental importance. Here the generalization of the symbolical method made by Dirac and Jordan represented a great progress by making possible the operation with matrices, which are not arranged according to the stationary states, but where the possible values of any set of variables may appcar as indices of the matrix elements. In analogy to the interpretation considered in the original form of the theory of the "diagonal elements" connected only with a single stationaty state, as time averages of the quantity to be represented, the general transformation theory of matrices permits the representation of such averages of a mechanical quantity, in the calculation of which any set of variables characterizing the "state" of the system has given values, while the canonically conjugated variables are allowed to take all possible values. On the basis of the procedure developed by these authors and in close connection with ideas of Born and Pauli, Heisenberg has in the paper already cited above attempted a closer analysis of the physical content of the quantum
theory, especially in view of the apparently paradoxical character of the exchange relation (3). In this connection he has formulated the relation

$$\Delta q \Delta p \sim h \tag{4}$$

as the general expression for the maximum accuracy with which two canonically conjugated variables can simultaneously be observed. In this way Heisenberg has been able to elucidate many paradoxes appearing in the application of the quantum postulate, and to a large extent to demonstrate the consistency of the symbolic method. In connection with the complementary nature of the quantum-theoretical description, we must, as already mentioned, constantly keep the possibilities of definition as well as of observation before the mind. For the discussion of just this question the method of wave mechanics developed by Schrödinger has, as we shall see, proved of great help. It permits a general application of the principle of superposition also in the problem of interaction, thus offering an immediate connection with the above considerations concerning radiation and free particles. Below we shall return to the relation of wave mechanics to the general formulation of the quantum laws by means of the transformation theory of matrices.

5. WAVE MECHANICS AND The QUANTUM POSTULATE

Already in his first considerations concerning the wave theory of material particles, de Broglie pointed out that the stationary states of an atom may be visualized as an interference effect of the phase wave associated with a bound electron. It is true that this point of view at first did not, as regards quantitative results, lead beyond the

earlier methods of quantum theory, to the development of which Sommerfeld has contributed so essentially. Schrödinger, however, succeeded in developing a wavetheoretical method which has opened up new aspects, and has proved to be of decisive importance for the great progress in atomic physics during the last years. Indeed, the proper vibrations of the Schrödinger wave equation have been found to furnish a representation of the stationary states of an atom meeting all requirements. The energy of each state is connected with the corresponding period of vibration according to the general quantum relation (i). Furthermore, the number of nodes in the various characteristic vibrations gives a simple interpretation to the concept of quantum number which was already known from the older methods, but at first did not seem to appear in the matrix formulation. In addition, Schrödinger could associate with the solutions of the wave equation a continuous distribution of charge and current which, if applied to a characteristic vibration, represents the electrostatic and magnetic properties of an atom in the corresponding stationary state. Similarly, the superposition of two characteristic solutions corresponds to a continuous vibrating distribution of electrical charge, which on classical electrodynamics would give rise to an emission of radiation, illustrating instructively the consequences of the quantum postulate and the correspondence requirement regarding the transition process between two stationary states formulated in matrix mechanics. Another application of the method of Schrödinger, important for the further development, has been made by Born in his investigation of the problem of collisions between atoms and free electric particles. In this
connection he succeeded in obtaining a statistical interpretation of the wave functions, allowing a calculation of the probability of the individual transition processes required by the quantum postulate. This includes a wavemechanical formulation of the adiabatic principle of Ehrenfest, the fertility of which appears strikingly in the promising investigations of Hund on the problem of the formation of molecules.

In view of these results, Schrödinger has expressed the hope that the development of the wave theory will eventually remove the irrational element expressed by the quantum postulate and open the way for a complete description of atomic phenomena along the line of the classical theories. In support of this view, Schrödinger, in a recent paper, emphasizes the fact that the discontinuous exchange of energy between atoms required by the quantum postulate, from the point of view of the wave theory, is replaced by a simple resonance phenomenon. In particular, the idea of individual stationary states would be an illusion and its applicability only an iiliustration of the resonance mentioned. It must be kept in mind, however, that just in the resonance problem mentioned we are concerned with a closed system which, according to the view presented here, is not accessible to observation. In fact, wave mechanics, just as the matrix theory, on this view represents a symbolic transcription of the problem of motion of classical mechanics adapted to the requirements of quantum theory and only to be interpreted by an explicit use of the quantum postulate. Indeed, the two formulations of the interaction problem might be said to be complementary in the same sense as the wave and particle idea in the description of the free
individuals. The apparent contrast in the utilization of the energy concept in the two theories is just connected with this difference in the starting-point.

The fundamental difficulties opposing a space-time description of a system of particles in interaction appear at once from the inevitability of the superposition principle in the description of the behaviour of individual particles. Already for a free particle the knowledge of energy and momentum excludes, as we have seen, the exact knowledge of its space-time co-ordinates. This implies that an immediate utilization of the concept of energy in connection with the classical idea of the potential energy of the system is excluded. In the Schrödinger wave equation these difficulties are avoided by replacing the classical expression of the Hamiltonian by a differential operator by means of the relation

$$p = \sqrt{-1}\frac{h}{2\pi}\frac{\delta}{\delta q}, \tag{5}$$

where p denotes a generalized component of momentum and q the canonically conjugated variable. Here the negative value of the energy is regarded as conjugated to the time. So far, in the wave equation, time and space as well as energy and momentum are utilized in a purely formal way.

The symbolical character of Schrödinger's method appears not only from the circumstance that its simplicity, similarly to that of the matrix theory, depends essentially upon the use of imaginary arithmetic quantities. But above all there can be no question of an immediate connection with our ordinary conceptions because the "geometrical" problem represented by the wave equation is associated with the so-called co-ordinate space, the number of dimensions of which is equal to the number of degrees of freedom of the system, and, hence, in general greater than the number of dimensions of ordinary space. Further, Schrödinger's formulation of the interaction problem, just as the formulation offered by matrix theory, involves a neglect of the finite velocity of propagation of the forces claimed by relativity theory.

On the whole, it would scarcely seem justifiable, in the case of the interaction problem, to demand a visualization by means of ordinary space-time pictures. In fact, all our knowledge concerning the internal properties of atoms is derived from experiments on their radiation or collision reactions, such that the interpretation of experimental facts ultimately depends on the abstractions of radiation in free space, and free material particles. Hence, our whole space-time view of physical phenomena, as well as the definition of energy and momentum, depends ultimately upon these abstractions. In judging the applications of these auxiliary ideas, we should only demand inner consistency, in which connection special regard has to be paid to the possibilities of definition and observation.

In the characteristic vibrations of Schrödinger's wave equation we have, as mentioned, an adequate representation of the stationary states of an atom allowing an unambiguous definition of the energy of the system by means of the general quantum relation (1). This entails, however, that in the interpretation of observations a fundamental renunciation regarding the space-time description is unavoidable. In fact, the consistent application of the concept of stationary states excludes, as we shall see, any specification regarding the behaviour of the separate particles in the atom. In problems where a description of this behaviour is essential, we are bound to use the general solution of the wave equation which is obtained by superposition of characteristic solutions. We meet here with a complementarity of the possibilities of definition quite analogous to that which we have considered earlier in connection with the properties of light and free material particles. Thus, while the definition of energy and momentum of individuals is attached to the idea of a harmonic elementary wave, every space-time feature of the description of phenomena is, as we have seen, based on a consideration of the interferences taking place inside a group of such elementary waves. Also in the present case the agreement between the possibilities of observation and those of definition can be directly shown.

According to the quantum postulate any observation regarding the behaviour of the electron in the atom will be accompanied by a change in the state of the atom. As stressed by Heisenberg, this change will, in the case of atoms in stationary states of low quantum number, consist in general in the ejection of the electron from the atom. A description of the "orbit" of the electron in the atom with the aid of subsequent observations is, hence, impossible in such a case. This is connected with the circumstance that from characteristic vibrations with only a few nodes no wave packages can be built up which would even approximately represent the "motion" of a particle. The complementary nature of the description, however, appears particularly in that the use of observations concerning the behaviour of particles in the atom rests on the possibility

of neglecting, during the process
of observation, the interaction between the particles, thus regarding them as free. This requires, however, that the duration of the process is short compared with the natural periods of the atom, which again means that the uncertainty in the knowledge of the energy transferred in the process is large compared to the energy differences between neighbouring stationary states.

In judging the possibilities of observation it must, on the whole, be kept in mind that the wave-mechanical solutions can be visualized only in so far as they can be described with the aid of the concept of free particles. Here the difference between classical mechanics and the quantum-theoretical treatment of the problem of interaction appears most strikingly. In the former such a restriction is unnecessary because the "particles" are here endowed with an immediate "reality", independently of their being free or bound. This situation is particularly important in connection with the consistent utilization of Schrödinger's electric density as a measure of the probability for electrons being present within given space regions of the atom. Remembering the restriction mentioned, this interpretation is seen to be a simple consequence of the assumption that the probability of the presence of a free electron is expressed by the electric density associated with the wave-field in a similar way to that by which the probability of the presence of a light quantum is given by the energy density of the radiation.

As already mentioned, the means for a general consistent utilization of the classical concepts in the quantum theory have been created through the transformation theory of Dirac and Jordan, by the aid of which Heisen-
berg has formulated his general uncertainty relation (4). In this theory also the Schrödinger wave equation has obtained an instructive application. In fact, the characteristic solutions of this equation appear as auxiliary functions which define a transformation from matrices with indices representing the energy values of the system to other matrices, the indices of which are the possible values of the space co-ordinates. It is also of interest in this connection to mention that Jordan and Klein have recently arrived at the formulation of the problem of interaction expressed by the Schrödinger wave equation, taking as starting-point the wave representation of individual particles and applying a symbolic method closely related to the deep-going treatment of the radiation probiem developed by Dirac from the point of view of the matrix theory, to which we shall return below.

6. REALITY OF STATIONARY STATES

In the conception of stationary states we are, as mentioned, concerned with a characteristic application of the quantum postulate. By its very nature this conception means a complete renunciation as regards a time description. From the point of view taken here, just this renunciation forms the necessary condition for an unambiguous definition of the energy of the atom. Moreover, the conception of a stationary state involves, strictly speaking, the exclusion of all interactions with individuals not belonging to the system. The fact that such a closed system is associated with a particular energy value may be considered as an immediate expression for the claim of causality contained in the theorem of conservation of energy. This circumstance justifies the assumption of
the supra-mechanical stability of the stationary states, according to which the atom, before as well as after an external influence, always will be found in a well-defined state, and which forms the basis for the use of the quantum postulate in problems concerning atomic structure.

In a judgment of the well-known paradoxes which this assumption entails for the description of collision and radiation reactions, it is essential to consider the limitations of the possibilities of definition of the reacting free individuals, which is expressed by relation (2). In fact, if the definition of the energy of the reacting individuals is to be accurate to such a degree as to entitle us to speak of conservation of energy during the reaction, it is necessary, according to this relation, to co-ordinate to the reaction a time interval long compared to the vibration

period associated with the transition process, and connected with the energy difference between the stationary states according to relation (1). This is particularly to be remembered when considering the passage of swiftly moving particles through an atom. According to the ordinary kinematics, the effective duration of such a passage would be very small as compared with the natural periods of the atom, and it seemed impossible to reconcile the principle of conservation of energy with the assumption of the stability of stationary states. In the wave representation, however, the time of reaction is immediately connected with the accuracy of the knowledge of the energy of the colliding particle, and hence there can never be the possibility of a contradiction with the law of conservation. In connection with the discussion of paradoxes of the kind mentioned, Campbell suggested
the view that the conception of time itself may be essentially statistical in nature. From the view advanced here, according to which the foundation of space-time description is offered by the abstraction of free individuals, a fundamental distinction between time and space, however, would seem to be excluded by the relativity requirement. The singular position of the time in problems concerned with stationary states is, as we have seen, due to the special nature of such problems.

The application of the conception of stationary states demands that in any observation, say by means of collision or radiation reactions, permitting a distinction between different stationary states, we are entitled to disregard the previous history of the atom. The fact that the symbolical quantum theory methods ascribe a particular phase to each stationary state the value of which depends upon the previous history of the atom, would for the first moment seem to contradict the very idea of stationary states. As soon as we are really concerned with a time problem, however, the consideration of a strictly closed system is excluded. The use of simply harmonic proper vibrations in the interpretation of observations means, therefore, only a suitable idealization which in a more rigorous discussion must always be replaced by a group of harmonic vibrations, distributed over a finite frequency interval. Now, as already mentioncd, it is a general consequence of the superposition principle that it has no sense to co-ordinate a phase value to the group as a whole, in the same manner as may be done for each elementary wave constituting the group.

This inobservability of the phase, well known from the theory of optical instruments, is brought out in a
particularly simple manner in a discussion of the SternGerlach experiment, so important for the investigation of the properties of single atoms. As pointed out by Heisenberg, atoms with different orientation in the field may only be separated if the deviation of the beam is larger than the diffraction at the slit of the de Brogie waves representing the translational motion of the atoms. This condition means, as a simple calculation shows, that the product of the time of passage of the atom through the field, and the uncertainty due to the finite width of the beam of its energy in the field, is at least equal to the quantum of action. This result was considered by Heisenberg as a support of relation (2) as regards the reciprocal uncertainties of energy and time values. It would seem, however, that here we are not simply dealing with a measurement of the energy of the atom at a given time. But since the period of the proper vibrations of the atom in the field is connected with the total energy by relation (1), we realize that the condition for separability mentioned just means the loss of the phase. This circumstance removes also the apparent contradictions, arising in certain problems concerning the coherence of resonance radiation, which have been discussed frequently, and were also considered by Heisenberg.

To consider an atom as a closed system, as we have done above, means to neglect the spontaneous emission of radiation which even in the absence of external influences puts an upper limit to the lifetime of the stationary states. The fact that this neglect is justified in many applications is connected with the circumstance that the coupling between the atom and the radiation field, which is to be expected on classical electro-

dynamics, is in general very small compared to the coupling between the particles in the atom. It is, in fact, possible in a description of the state of an atom to a considerable extent to neglect the reaction of radiation, thus disregarding the unsharpness in the energy values connected with the lifetime of the stationary states according to relation (2). This is the reason why it is possible to draw conclusions concerning the properties of radiation by using classical electrodynamics.

The treatment of the radiation problem by the new quantum-theoretical methods meant, to begin with, just a quantitative formulation of this correspondence consideration. This was the very starting-point of the original considerations of Heisenberg. It may also be mentioned that an instructive analysis of Schrödinger's treatment of the radiation phenomena from the point of view of the correspondence principle has been recently given by Klein. In the more rigorous form of the theory developed by Dirac, the radiation field itself is included in the closed system under consideration. Thus it became possible in a rational way to take account of the individual character of radiation demanded by the quantum theory and to build up a dispersion theory, in which the finite width of the spectral lines is taken into consideration. The renunciation regarding space-time pictures characterizing this treatment would seem to offer a striking indication of the complementary character of the quantum theory. This is particularly to be borne in mind in judging the radical departure from the causal description of Nature met with in radiation phenomena, to which we have referred above in connection with the excitation of spectra.

In view of the asymptotic connection of atomic properties with classical electrodynamics, demanded by the correspondence principle, the reciprocal exclusion of the conception of stationary states and the description of the behaviour of individual particles in the atom might be regarded as a difficulty. In fact, the connection in question means that in the limit of large quantum numbers where the relative difference between adjacent stationary states vanishes asymptotically, mechanical pictures of electronic motion may be rationally utilized. It must be emphasized, however, that this connection cannot be regarded as a gradual transition towards classical theory in the sense that the quantum postulate would lose its significance for high quantum numbers. On the contrary, the conclusions obtained from the correspondence principle with the aid of classical pictures depend just upon the assumptions that the conception of stationary states and of individual transition processes are maintained even in this limit.

This question offers a particularly instructive example for the application of the new methods. As shown by Schrödinger, it is possible, in the limit mentioned, by superposition of proper vibrations to construct wavegroups small in comparison to the "size" of the atom, the propagation of which indefinitely approaches the classical picture of moving material particles, if the quantum numbers are chosen sufficiently large. In the special case of a simple harmonic vibrator, he was able to show that such wave-groups will keep together even for any length of time, and will oscillate to and fro in a manner corresponding to the classical picture of the motion. This circumstance Schrödinger has regarded as
a support of his hope of constructing a pure wave theory without referring to the quantum postulate. As emphasized by Heisenberg, the simplicity of the case of the oscillator, however, is exceptional and intimately connected with the harmonic nature of the corresponding classical motion. Nor is there in this example any possibility for an asymptotical approach towards the problem of free particles. In general, the wave-group will gradually spread over the whole region of the atom, and the "motion" of a bound electron can only be followed during a number of periods, which is of the order of magnitude of the quantum numbers associated with the proper vibrations. This question has been more closely investigated in a recent paper by Darwin which contains a number of instructive examples of the behaviour of wave groups. From the viewpoint of the matrix theory a treatment of analogous problems has been carried out by Kennard.

Here again we meet with the contrast between the wave-theory superposition principle and the assumption of the individuality of particles with which we have been concerned already in

the case of free particles. At the same time the asymptotical connection with the classical theory, to which a distinction between free and bound particles is unknown, offers the possibility of a particularly simple illustration of the above considerations regarding the consistent utilization of the concept of stationary states. As we have seen, the identification of a stationary state by means of collision or radiation reactions implies a gap in the time description, which is at least of the order of magnitude of the periods associated with transitions between stationary states. Now, in the
limit of high quantum numbers these periods may be interpreted as periods of revolution. Thus we see at once that no causal connection can be obtained between observations leading to the fixation of a stationary state and earlier observations on the behaviour of the separate particles in the atom.

Summarizing, it might be said that the concepts of stationary states and individual transition processes within their proper field of application possess just as much or as little "reality" as the very idea of individual particles. In both cases we are concerned with a demand of causality complementary to the space-time description, the adequate application of which is limited only by the restricted possibilities of definition and of observation.

7. The PROBLEM OF The ELEMENTARY PARTICLES

When due regard is taken of the complementary feature required by the quantum postulate, it seems, in fact, possible with the aid of the symbolic methods to build up a consistent theory of atomic phenomena, which may be considered as a rational generalization of the causal space-time description of classical physics. This view does not mean, however, that classical electron theory may be regarded simply as the limiting case of a vanishing quantum of action. Indeed, the connection of the latter theory with experience is based on assumptions which can scarcely be separated from the group of problems of the quantum theory. A hint in this direction was already given by the well-known difficulties met with in the attempts to account for the individuality of
ultimate electrical particles on general mechanical and electrodynamical principles. In this respect also, the general relativity theory of gravitation has not fulfilled expectations. A satisfactory solution of the problems touched upon would seem to be possible only by means of a rational quantum-theoretical transcription of the general field theory, in which the ultimate quantum of electricity has found its natural position as an expression of the feature of individuality characterizing the quantum theory. Recently Klein has directed attention to the possibility of connecting this problem with the five-dimensional unified representation of electromagnetism and gravitation proposed by Kaluza. In fact, the conservation of electricity appears in this theory as an analogue to the conservation theorems for energy and momentum. Just as these concepts are complementary to the spacetime description, the appropriateness of the ordinary four-dimensional description as well as its symbolical utilization in the quantum theory would, as Klein emphasizes, seem to depend essentially on the circumstance that in this description electricity always appears in welldefined units, the conjugated fifth dimension being as a consequence not open to observation.

Quite apart from these unsolved deep-going problems, the classical electron theory up to the present time has been the guide for a further development of the correspondence description in connection with the idea first advanced by Compton that the ultimate electrical particles, besides their mass and charge, are endowed with a magnetic moment due to an angular momentum determined by the quantum of action. This assumption, introduced with striking success by Goudsmit and

Uhlenbeck into the discussion of the origin of the anomalous Zeeman effect, has proved most fruitful in connection with the new methods, as shown especially by Heisenberg and Jordan. One might say, indeed, that the hypothesis of the magnetic electron, together with the reso-

nance problem elucidated by Heisenberg, which occurs in the quantum-theoretical description of the behaviour of atoms with several electrons, have brought the correspondence interpretation of the spectral laws and the periodic system to a certain degree of completion. The principles underlying this attack have even made it possible to draw conclusions regarding the properties of atomic nuclei. Thus Dennison, in connection with ideas of Heisenberg and Hund, has succeeded recently in a very interesting way in showing how the explanation of the specific heat of hydrogen, hitherto beset with difficulties, can be harmonized with the assumption that the proton is endowed with a moment of momentum of the same magnitude as that of the electron. Due to its larger mass, however, a magnetic moment much smaller than that of the electron must be associated with the proton.

The insufficiency of the methods hitherto developed as concerns the problem of the elementary particles appears in the questions just mentioned from the fact that they do not allow of an unambiguous explanation of the difference in the behaviour of the electric elementary particles and the "individuals" symbolized through the conception of light quanta expressed in the so-called exclusion principle formulated by Pauli. In fact, we meet in this principle, so important for the problem of atomic structure as well as for the recent development of
statistical theories, with one among several possibilities, each of which fulfils the correspondence requirement. Moreover, the difficulty of satisfying the rclativity requirement in quantum theory appears in a particularly striking light in connection with the problem of the magnetic electron. Indeed, it seemed not possible to bring the promising attempts made by Darwin and Pauli in generalizing the new methods to cover this problem naturally, in connection with the relativity kinematical consideration of Thomas so fundamental for the interpretation of experimental results. Quite recently, however, Dirac has been able successfully to attack the problem of the magnetic electron through a new ingenious extension of the symbolical method and so to satisfy the relativity requirement without abandoning the agreement with spectral evidence. In this attack not only the imaginary complex quantities appearing in the earlier procedures are involved, but his fundamental equations themselves contain quantities of a still higher degree of complexity that are represented by matrices.

Already the formulation of the relativity argument implies essentially the union of the space-time co-ordination and the demand of causality characterizing the classical theories. In the adaptation of the relativity requirement to the quantum postulate, we must therefore be prepared to meet with a renunciation as to visualization in the ordinary sense going still further than in the formulation of the quantum laws considered here. Indeed, we find ourselves here on the very path taken by Einstein of adapting our modes of perception borrowed from the sensations to the gradually deepening knowledge of the laws of Nature. The hindrances met with on this path
originate above all in the fact that, so to say, every word in the language refers to our ordinary perception. In the quantum theory we meet this difficulty at once in the question of the inevitability of the feature of irrationality characterizing the quantum postulate. I hope, however, that the idea of complementarity is suited to characterize the situation, which bears a deep-going analogy to the general difficulty in the formation of human ideas, inherent in the distinction between subject and object.

The uncertainty principle is one of the most characteristic and important consequences of the new quantum mechanics. This principle, as formulated by Heisenberg for two conjugate quantum-mechanical variables, states that the accuracy with which two such variables can be measured simultaneously is subject to the restriction that the product of the uncertainties in the two measurements is at least of order h (Planck's constant). Condon* has remarked that an uncertainty relation of this type can nut hodid the general case where the two variables under consideration are not conjugate, and has stressed the desirability of obtaining a general formulation of the principle. It is the purpose of the present letter to give such gurpe of to and

to apply it in particular ton, ase of angular momentum.
We define the "mean value" A_0 of an (Hermitean) operator A in a system whose state is described by the (normal) function ψ as

$$A_0 = \int_{\bar{\psi}}^{-} A\psi d\tau$$

where the integral is extended over the entire coordinate space. The Hermitean character of A (i.e.

$$\int_{\bar{\phi}}^{-} A\psi d\tau = \int_{\bar{\psi}} A\phi d\tau$$

for arbitrary ϕ, ψ) insures the reality of A_0. The "uncertainty" ΔA in the value of A is then defined, in accordance with statistical usage, as the root mean square of the deviation of A from this mean, i.e.

$$(\Delta A)^2 = \int \bar{\psi} \left(A - A_0\right)^2 \psi d\tau$$

The uncertainty principle for two such variables A, B, whose commutator $AB - BA = hC/2\pi i$, is expressed by

$$\Delta A \cdot \Delta B \geqq h \left|C_0\right| /4\pi$$

i.e. the product of the uncertainties in A, B is not less than half the absolute value of the mean of ineir cummuiaior.

- E. U. Condon "Remarks on Uncertainty Principles" Science LXIX, p. 573 (May 31, 1929), and in conversations with the writer on this topic.

24.9 I. 5 the Uncertainty Principle

We here confine ourselves to sketching the proof of this principle for a one-particle system and for quantum mechanical variables $A(q,p), B(q,p)$ which are linear in the momenta (p_x, p_y, p_z) .[1] (The proof for the general case in which the operators can be expanded in powers of the momenta can be made along exactly the same lines.) Writing

$$A = a + a_x p_x + a_y p_y + a_z p_z$$

where $p_x = (h/2\pi i)\partial/\partial x$, etc. and the a 's are functions of position, the Hermitean character of A requires that these functions be real and that div $(a_x, a_y, a_*) = 0$. The expression for $(\Delta A)^2$ may be written, on integrating once by parts, using the fact that div $(\bar{u}) = 0$ and discarding the resulting surface integral, in the form

$$(\Delta A)^2 = \int \left|\left(A - A_0\right)\psi\right|^2 dr$$

We are now in a position to apply the Schwarzian inequality [2]
$\left[\int \left(f_1 \bar{f}_1 + f_2 \bar{f}_9\right) d\tau\right] \left[\int \left(g_1 \bar{g}_1 + g_2 \bar{g}_2\right) d\tau\right]$

$$\geqq \left|\int \left(f_1 g_1 + f_2 g_2\right) d\tau\right|^2$$

Taking

$$\bar{f}_1 = (A - A_0)\,\psi = f_i, g_1 = (B - B_0)\,\psi = -\bar{g}_i$$

and reducing the integral on the right hand side by integration by parts we find

$$\Delta A \cdot \Delta B \geqq \frac{1}{2}\left|\int \bar{\psi}(AB - BA)\psi d\tau\right|$$

the required result.

We obviously obtain Heisenberg's result if the two variables are conjugate, for then C, and consequently C_0, are ± 1. As a further illustration of the principle, we apply it to the case of angular momentum. Here we have

$M_x = yp_z - zp_y, M_xM_y - M_yM_x = -hM_2/2\pi i$ so the product of the uncertainties in two of the components of angular momentum is not less than $h/4\pi$ times the mean value of the third component in the state under consideration.

[1] Cf. proof of special case $A = p, B = q$ in H. Weyl "Gruppentheorie und Quantenmechanik" pp. 66, 272.

[2] Weyl, 1. c. n. 272.

Consider in particular the state, treated by Now from the uncertainty principle for M_x, Condon, defined by M_ν we find

$$\psi = f(r)e^{im\phi}P_l^m(\cos\theta)$$

where the pole of the spherical coordinates lies on the z-axis. Then $M_z, M^2\,(= {M_x}^2 + {M_y}^2 + {M_z}^2)$ have the definite values

$M_z - M_{z0} - mil/2_n, M^2 = l(l+1)(h/2\pi)^2$

the mean values of M_x, M_y are zero and the uncertainties are given by

$(\Delta M_x)^2 = (\Delta M_y)^2 = \frac{1}{2}\left[l(l+1) - m^2\right](h/2\pi)^2$, $\Delta M_z = 0$.

$$l(l+1) \geqq m(m+1)$$

which is in fact the case. This example shows that for $m = l$ the equality holds; the inequality is consequently the most restrictive one that can be deduced for angular momenta, for we have here a case in which the ultimate limit has (in principle) been reached.

H. P. Robertson

Palmer Physical Laboratory,
Princeton, N. J.,
Princeton, N. J.,
June 18, 1929.

24.10 I. 6 the Wave Mechanics of α-ray Tracks

The present note is suggested by a recent paper by Prof. Darwin,* and is intended to show how one of the most typically particle-like properties of matter can be derived from the wave mechanics. In the theory of radioactive disintegration, as presented by Gamow, the α-particle is represented by a spherical wave which slowly leaks out of the nucleus. On the other hand, the α-particle, once emerged, has particle-like properties, the most striking being the ray tracks that it forms in a Wilson cloud chamber. It is a little difficult to picture how it is that an outgoing spherical wave can produce a straight track; we think intuitively that it should ionise atoms at random throughout space. We could consider that Gamow's outguing spherical wave should give the probability of disintegration, but that, when the particle is outside the nucleus, it should be represented by a wave packet moving in a definite direction, so as to produce a straight track. But it ought not to be necessary to do this. The wave mechanics unaided

ought to be able to predict the possible results of any observation that wo could make on a system, without invoking, until the moment at which the observation is made, the classical particle-like properties of the electrons or $\alpha-$ particles forming that system. If we consider the α-ray alone as the system under consideration, then the gas of the Wilson chamber must be considered as the means by which we observe the particle; so in this case we must consider the α-ray as a particle as soon as it is outside the nucleus, because that is the moment at which the observation is made. If, however, we consider the α-particle and the gas together as one system, then it is ionised atoms that we observe; interpreting the wave function should give us simply the probability that such and such an atom is ionised. Until this final interpretation is made, no mention should be made of the α-ray being a particle at all.

The difficulty that we have in picturing how it is that a spherical wave can produce a straight track arises from our tendency to picture the wave as existing in ordinary three dimensional space, whereas we are really dealing with wave functions in the multispace formed by the co-ordinates both of the α-particle and of every atom in the Wilson chamber.

• ' Roy. Soc. Proc.,' A, voil. 124, p. 375 (1929).

Originally published in Proceedings of the Royal Society, London, A126, 79-84 (1929).

For our purpose it will be sufficient to consider only two atoms; for simplicity we shall suppose that they are hydrogen atoms. The position of the nuclei of the atoms we shall treat as parameters; this is legitimate, since the nuclei are many times heavier than the electrons, and move very much more slowly than the α-particles; therefore, during the whole time of formation of a track, they may be considered effectively at rest.* We shall then show that the atoms cannot both be ionised unless they lie in a straight line with the radioactive nucleus.

Let $\psi_S(\mathbf{r})$ be the wave function of an excited hydrogen atom, referred to axes that pass through its nucleus. We shall denote by $\psi_0(\mathbf{r})$ the wave function corresponding to the normal state. We shall take axes such that the nucleus of the radioactive atom lies at the urigin, and the two hydrogen atoms at the points $\mathbf{a}_1, \mathbf{a}_2$. Then the wave functions of the two hydrogen atoms are, in these co-ordinates

$$\Psi^{\overline{\mathrm{I}}}(\mathbf{r}) = \psi(\mathbf{r} - \mathbf{a}_1)$$
$$\Psi^{\mathrm{II}}(\mathbf{r}) = \psi(\mathbf{r} - \mathbf{a}_2).$$

Let $\mathbf{R}$ be the co-ordinate of the α-particle and $\mathbf{r}_1, \mathbf{r}_2$ the co-ordinates of the two electrons. Let $\mathbf{F}(\mathbf{R}, \mathbf{r}_1, \mathbf{r}_2)\, e^{i\mathbf{E}t/\hbar}$ be a periodic wave function of the α-particle and of the two atomic electrons. We can expand F in a series of wave functions of the two atoms, of the form

$$\mathbf{F}(\mathbf{R}, \mathbf{r}_1, \mathbf{r}_2) = \sum_{\mathrm{J}_1\ \mathrm{J}_2} f_{\mathrm{J}_2\ \mathrm{J}_2}(\mathbf{R})\, \mathrm{Ir}_{\mathrm{J}_1}{}^{\mathrm{I}}(\tilde{\mathbf{r}}_1)\, \Psi_{\mathrm{J}_2}{}^{\mathrm{II}}(\mathbf{r}_2). \tag{1}$$

We can now see what form the wave function must have, in order that we shall obtain straight tracks. Interpret– ia nucieus ing our wave function, we see that $|\, f_{\mathrm{J_J J}}, \mathbf{R})\,|^2\, d\,\mathrm{V}$ is the probability that we shall find the α-particle in the volume element $d\,\mathrm{V}$, and at the same time the first atom in the excited (or ionised) state J_1 and the second in the state J_2. To obtain a consistent theory of the straight tracks, we must have $f_{00}(\mathbf{R})$ representing an outgoing spherical wave, at any rate for $|\mathbf{R}|$ less than either $|\mathbf{a}_1|$ or $|\mathbf{a}_2|$. $f_{\mathrm{J}_1 0}(\mathbf{R})$ will represent the probable positions of an α-particle that has excited the first atom, but not the second. It should therefore be independent of $\mathbf{a}_2$, and should represent a * We do not consider the possibility of a collision between the α-particle and the nucleus.
wave diverging from the point $\mathbf{a_1}$, whose amplitude vanishes except inside a small cone, pointing away from the origin. Finally, $f_{\mathrm{J}_1\ \mathrm{J}_2}(\mathbf{R})$ will give the probability that the α-particle excites both atoms.

$f_{\mathrm{J}_1\ \mathrm{J}_2}(\mathbf{R})$ should vanish, therefore, unless the line joining $\mathbf{a}_1$ and $\mathbf{a}_2$ passes near the origin. We shall obtain a solution with these properties.

The wave equation is

$$\left\{\frac{h^2}{2\mathrm{M}}\nabla_{\mathrm{R}}^2+\frac{h^2}{2m}\left(\nabla_1^2+\nabla_2^2\right)+\mathrm{E}+\frac{\varepsilon^2}{|\mathbf{r}_1-\mathbf{a}_1|}+\frac{\varepsilon^2}{|\mathbf{r}_2-\mathbf{a}_2|}+\frac{2\varepsilon^2}{|\mathbf{R}-\mathbf{r}_1|}+\frac{2\varepsilon^2}{|\mathbf{R}-\mathbf{r}_2|}\right\}\mathbf{F}=0 \tag{2}$$

where ${\nabla_{\mathrm{R}}}^2$ refers to the co-ordinates of the α-particle, and ${\nabla_1}^2, {\nabla_2}^2$ to the co-ordinates of the electrons. We have left out the terms giving the interaction between the α-particle and the nuclei of the atoms, which would in fact produce doviations from the straight track, and are irrelevant to our purpose. We treat the interaction of the atoms and the α-particle as a perturbation, and solve by a method of successive approximations, similar to that used by Born* in his work on collisions. We set
with

$$\begin{gathered}\mathrm{F}=\mathrm{F}^{(0)}+\mathrm{F}^{(\bar{1})}+\mathrm{F}^{(2)}+\ldots\\ \mathrm{F}^{(0)}=e^{ik|\mathbf{R}|}/|\mathbf{R}|\cdot\Psi_0^{\mathbf{I}}(\mathbf{r}_1)\,{\Psi_0}^{\mathrm{II}}(\mathbf{r}_2),\\ k=\sqrt{2\mathrm{M}\,(\mathrm{E}-2\mathrm{E}_0)}/h,\end{gathered}$$

where
representing an outgoing wave for the α-particle, and the normal states of both atoms. Then $\mathbf{F}$ is a solution of (2) if

$$\left\{\frac{h^2}{2\mathrm{M}}\nabla_{\mathrm{R}}^2+\frac{h^2}{2m}\left(\nabla_1^2+\nabla_2^2\right)+\mathrm{E}+\frac{\varepsilon^2}{|\mathbf{r}_1-\mathbf{a}_1|}+\frac{\varepsilon^2}{|\mathbf{r}_2-\mathbf{a}_2|}\right\}\mathrm{F}^{(n)}=\left\{\frac{-2\varepsilon^2}{|\mathbf{R}-\mathbf{r}_1|}+\frac{-2\varepsilon^2}{|\mathbf{R}-\mathbf{r}_2|}\right\}\mathrm{F}^{(n-1)} \tag{3}$$

Let us solve first for $F^{(1)}$. We expand $F^{(1)}$ as a series of the form (1), namely

$$F^{(1)}(\mathbf{R},\mathbf{r}_1,\mathbf{r}_2)=\sum_{J_1J_2}f^{(1)}_{J_1J_2}(\mathbf{R})\Psi^{\mathrm{I}}_{J_,}(\mathbf{r}_1)\,\Psi^{\mathrm{II}}_{J_4}(\mathbf{r}_2) \tag{4}$$

If we insert (4) in (3), multiply by ${\Psi_{J_1}}^{\mathbf{I}}(\mathbf{r}_1)\,{\Psi_{J_2}}^{\mathbf{II}}(\mathbf{r}_2)$ and integrate over all $\mathbf{r}_1\mathbf{r}_2$, we obtain a differential equation satisfied by $f^{(1)}_{\mathrm{J,J,}}(\mathbf{R})$, namely

$$\left\{\frac{h^2}{2\mathrm{M}}\nabla^2+\mathbf{E}-\mathrm{E}_{\mathrm{J}_1}-\mathrm{E}_{\mathrm{J}_2}\right\}f^{(1)}_{\mathrm{J}_1\ \mathrm{J}_2}(\mathbf{R})=\mathbf{K}(\mathbf{R}),$$

where

$$\begin{aligned}\mathbf{K}(\mathbf{R})&=\mathrm{V}_{0\ \mathrm{J}}(\mathbf{R}-\mathbf{a}_1)\,e^{ik|\mathbf{R}|}/|\mathbf{R}| && \text{if } \mathrm{J}_1=\mathrm{J},\ \mathrm{J}_2=0\\ &=\mathrm{V}_{0\ \mathrm{J}}(\mathbf{R}-\mathbf{a}_2)\,e^{ik|\mathbf{R}|}/|\mathbf{R}| && \text{if } \mathrm{J}_2=\mathrm{J},\ \mathrm{J}_1=0\\ &=0. && \text{otherwise.}\end{aligned}$$

In these formul

$$V_{0J}(R)=\int 2\varepsilon^2/|R-r|\cdot\psi_0(r)\psi_J(r)dr$$

Now, the most general solution of (5) is*

$$f^{(1)}_{\mathrm{J}_2\ \mathrm{J}_2}(\mathbf{R}) = \frac{1}{4\pi}\int \frac{2\mathrm{M}}{h^2}\mathbf{K}\left(\mathbf{R}'\right)\cdot\frac{e^{\pm ik'|\mathbf{R}-\mathbf{R}'|}}{|\mathbf{R}-\mathbf{R^1}|}d\mathbf{R}' + \mathbf{G}(\mathbf{R}), \tag{6}$$

where

$$\sqrt{\overline{2\mathrm{M}}\left(\overline{\mathrm{E}} - \overline{\mathrm{E}}_{\mathrm{J}_1} - \overleftarrow{\mathrm{E}}_{\mathrm{J}_1}\right)} = \ddot{k}\check{h}$$

and $G(\mathbf{R})$ is the most general solution of

$$\left(\nabla^2 + k'^2\right)\mathrm{G} = 0.$$

Now, it is clear that our starting conditions, namely that both atoms are in the normal state before collision, require that

$$G(\mathbf{R}) = 0;$$

for $\mathrm{G}(\mathbf{R})$ represents streams of particles fired at already excited atoms. We see, therefore, that if neither J_1 nor J_2 define the normal state of an atom, $f^{(1)}_{\mathrm{J}_1\ \mathrm{J}_2}(\mathbf{R})$ vanishes, and therefore, to this approximation, there is no probability that both atoms will be excited. This is to be expected; we have treated the probability that one atom will be excited as a small quantity of the first order ; the probability of both being excited will therefore be a small quantity of the second order.

If, say, J_1 represents the normal state, then $K(R)$ vanishes except in the neighbourhood of $\mathbf{a}_2$. Except in the neighbourhood of $\mathbf{a}_2$, therefore, $f^{(1)}_{0J_2}(\mathbf{R})$ is given by the asymptotic formula

$$f^{(1)}_{0J_2}(\mathbf{R}) \sim \frac{e^{ik'|\mathbf{R}-\mathbf{a}_2|}}{|\mathbf{R}-\mathbf{a}_2|}\mathfrak{J}(1)$$

where

$$\mathbf{l} = \left(\mathbf{R}-\mathbf{a}_2\right)/\left|\mathbf{R}-\mathbf{a}_2\right|$$

and

$$\mathfrak{J}(\mathbf{1}) = \frac{1}{4\pi}\int \frac{2m}{h^2}\ \mathrm{V}_{0J_\mathbf{2}}\left(\mathbf{R}'\right)e^{-ik'(|\mathbf{R}')+ik|\mathbf{R}'+\mathbf{a_2}|}d\mathbf{R}'. \tag{7}$$

• Uf. Courant-Hbert, "Methoden der Mathematischen Physik," chap. 5, § .

We have taken the positive value of ik' in (6), so that $f^{(1)}_{0J_2}$ shall represent a wave diverging from $\mathbf{a}_2$; $\mathrm{Im}\left(\mathbf{R}-\mathbf{a}_2/\left|\mathbf{R}-\mathbf{a}_2\right|\right)$ gives the amplitude of the wave in any direction.

We can easily see that $\mathfrak{J}(\mathbf{1})$ is very small except in the neighbourhood of

$$l = a_2/\left|a_2\right| \tag{8}$$

that is to say, except in a small cone with its vertex at $\mathbf{a}_2$, pointing away from the radioactive nucleus.

For we can see from (5) that $V_{0J}(\mathbf{R})$ must become very small except in the neighbourhood of $\mathbf{R}-0$. The exponentials oscillate very rapidly in the region where $\mathbf{R}$ does not vanish. $\mathfrak{J}(1)$, therefore, will have a strong maximum when the two exponential terms are in phase at the origin. Since $k-k'$ is negligible compared to k, this will be the case when (8) is satisfied.

It is interesting to work out the function Im (i) for a particular case. Born* has calculated the function V_{0J} for certain simple cases, and also the functions Im (1) using a plane wave instead

of our spherical wave. His results are applicable to our case, however, since the integrand in (7) vanishes except in a small region, in which the spherical wave may be considered plane. We have then †

$$\Sigma|\operatorname{Im}(1)|^2 = 0.9866. \quad a_{\mathrm{H}}^2 \frac{\mathrm{M}^2}{m^2}\frac{k'}{k}\frac{1}{z^2\left(1+z^2\right)^5}$$

where a_{H} is the radius of the normal orbit of the hydrogen atom, and

$$z = \frac{2}{3} a_{\mathrm{H}} \left|k\mathbf{1} - k^{\mathbf{1}}\mathbf{a_2}/\left|\mathbf{a_2}\right|\right|$$

and the summation is over all the three states with principal quantum number two. It is clear that this function is only appreciable in the neighbourhood (8), since ka_{H} is a very large number.

In order to find the probability that both atoms should be excited, we shall now consider $\mathrm{F}^{(2)}$. If we expand in a series of the form (4), as before, and insert in (3), then we obtain, analogously to (3), the following differential equation satisfied by $f^{(2)}_{\mathrm{J}_1\ \mathrm{J}_2}(\mathbf{R})$

$$\begin{aligned}\left\{\frac{h^2}{2\mathrm{M}}\ \nabla^2 + \mathrm{E} - \mathrm{E}_{\mathrm{J}_1} - \mathrm{E}_{\mathrm{J}_3}\right\} f^{(2)}_{\mathrm{J}_1\ \mathrm{J}_2}(\mathbf{R}) \\ = \iint \mathrm{F}^{(1)}\left(\mathbf{R}\mathbf{r}_1\mathrm{r}_2\right)\Psi^{\mathrm{I}}_{\mathrm{J}_1}\left(\mathrm{r}_1\right)\Psi^{\mathrm{II}}_{\mathrm{J}_2}\left(\mathrm{r}_2\right)d\mathrm{r}_1 d\mathrm{r}_2 \\ = f^{(1)}_{\mathrm{J}_1 0}(\mathbf{R})\mathrm{V}_{0\ \mathrm{J}_2}\left(\mathbf{R}-\mathrm{a}_2\right). \qquad (9)\end{aligned}$$

∗ Gott. Nachr., p. 146(1926),

\+ Ioc. git., equation (32).

Now, if the point $\mathbf{a}_2$ does not lie very near the straight line joining the origin to $\mathbf{a}_1$, then the right-hand side of (9) will vanish for all $\mathbf{R}$; for $f^{(1)}_{\mathrm{J}_1 0}(\mathbf{R})$ vanishes except in the neighbourhood of this line, as we have shown, and $\mathbf{V}_{0J_2}\left(\mathbf{R}-\mathbf{a}_2\right)$ vanishes except in the neighbourhood of $\mathbf{a}_2$. Therefore in this case, it follows, as before, that the only solution of (9) satisfying our initial conditions is

$$f^{(2)}_{\mathrm{J}_2\ \mathrm{J}_{\mathbf{2}}}(\mathbf{R}) = 0$$

and there is therefore no probability of both atoms being excited. If, on the other hand, the line joining $\mathbf{a}_1, \mathbf{a}_2$ does pass through the origin, then we can obtain as before a solution representing a wave diverging from the point $\mathbf{a}_2$. The amplitude of this wave gives the probability that both atoms are excited, and that the particle is moving in a given direction after exciting both.

In conclusion, the author would like to express his thanks to Prof. Darwin, who has contributed a great deal to the course of the development of this paper.

It is well known that the principles of quantum mechanics limit the possibilities of exact prediction as to the future path of a particle. It has sometimes been supposed, nevertheless, that the quantum mechanics would permit an exact description of the past path of a particle.

The purpose of the present note is to discuss a simple ideal experiment which shows that the possibility of describing the past path of one particle would lead to predictions as to the future behaviour of a second particle of a kind not allowed in the quantum mechanics. It will hence be concluded that the principles of quantum mechanics actually involve aii uncertainty in the description of past events which is analogous to the uncertainty in the prediction of future events. And it will be shown for the case in hand, that this uncertainty in the description of

the past arises from a limitation of the knowledge that can be obtained by measurement of momentum.

Consider a small box B, as shown in the figure, containing a number of identical paiticles in thermal agitation, and provided with two small openings which are closed by the shutter S. The shutter is arranged to open automatically for a short time and then close again, and the number of particles in the box is so chosen that cases arise in which one particle leaves the box and travels over the direct path SO to an observer at O, and a second particle travels over the longer path SRO through elastic reflection at the ellipsoidal reflector R.

The box is accurately weighed before and after the shutter has opened in order to determine the total energy of the particles which have left, and the observer at O is provided with means for observing the arrival of particles, a clock for measuring their time of arrival, and some apparatus for measuring

24.11 I. 7 Knowledge of Past and Future in Quantum Mechanics

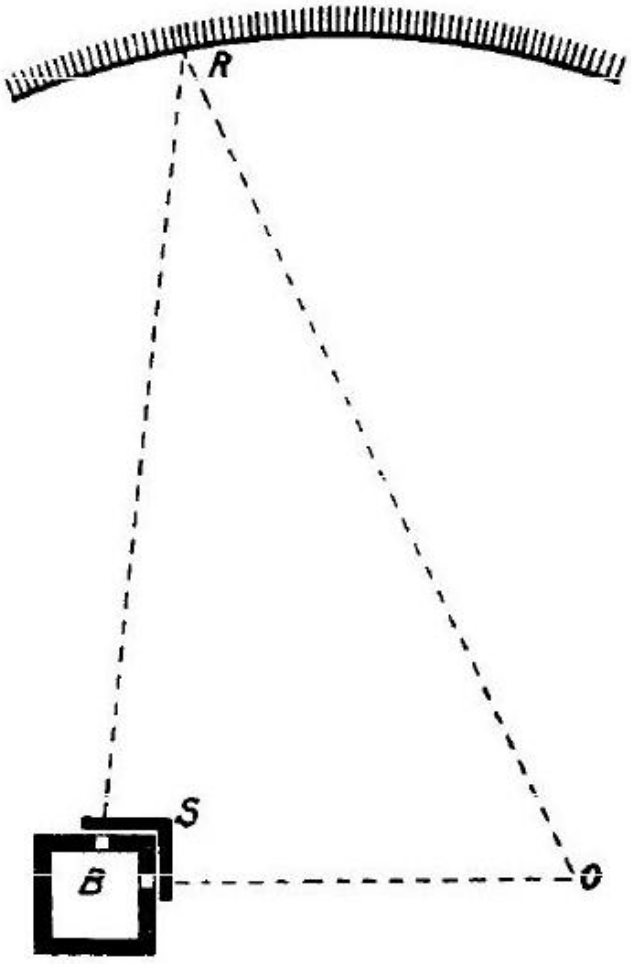


Fig. 1.

momentum. Furthermore the distances SC and SRO are accurately measured beforehand – the distance SO being sufficient so that the rate of the clock at O is not disturbed by the gravitational effects involved in weighing the box, and the distance SRO being very long ir order to permit an accurate reweighing of the box before the arrival of the second particle

Let us now suppose that the observer at C measures the momentum of the first particle as it approaches along the path SO and ther measures its of course the latter observation, made for

example with the help of the gamma-ray illumination, will change ertheless, knowing the ticle in the par locity and past, and hence also its past ve calculate the time when the shutter must have een open from the known time of arrival of the first particle, and to calculate the energy and velocity of the second particle from the known loss in the energy content of the box hen the shutter opened. It would then seem ossible to predict beforehand both the energy nd the time of arrival of the second particie, a paradoxical result since energy and time are quantities which do not commute in quantum echanics.
The explanation of the apparent paradox ust lie in the circumstance that the past motion of the first particle cannot be accurately determined as was assumed. Indeed, we are corced to conclude that there can be no methdd for measuring the momentum of a particie it value. For example an without changing its value. For example, an analysis of the method of observing the Doppler effect in the reflected infrared ight from an approaching particle shows that, although it permits a determination of the momentum of the particle both before and after collision with the light quantum used, it leaves an uncertainty as to the time at which the collision with the quantum takes place. Thus in our example, although the velocity of the first particle could be determined both before and after interaction with the infrared light. it
would not be possible to determine the exact position along the path SO at which the change in velocity occurred as would be necessary to obtain the exact time at which the shutter was open.

It is hence to be concluded that the principles of the quantum mechanics must involve an uncertainty in the description of past events which is analogous to the uncertainty in the prediction of future events. It is also to be noted that although it is possible to measure the momentum of a particle and follow this with a measurement of position this will not give sufficient information for a complete reconstruction of its past path, since it has been shown that there can be no method for measuring the momentum of a particie without changing its value. Finally, it is of scial special interest to emphasize the remarkable conclusion that the principles of quantum mechanics would actually impose limitations on the localization in time of a macroscopic phenomenon such as the opening and closing of a shutter.

Albert Einstein Richard C. Tolman Boris Podolsky California Institute of Technology, February 26, 1931.
[Einstein] attended [Bohr's 1933 Solvay] lecture and followed the argument with the closest attention; he made no direct comment on it, but put at once the discussion on the general theme of the meaning of quantum theory. He had no longer any doubt about the logic of Bohr's argumentation; but he still felt the same uneasiness as before ("Unbehagen" was his word) when confronted with the strange consequences of the theory. "What would you say of the following situation?" he asked mc. "Suppose two particles are set in motion towards each other with the same, very large, momentum, and that they interact with each other for a very short time when they pass at known positions. Consider now an observer who gets hold of one of the particles, far away from the region of interaction, and measures its momentum; then, from the conditions of the experiment, he will obviously be able to deduce the momentum of the other particle. If, however, he chooses to measure the position of the first particle, he will be able to tell where the other particle is. This is a perfectly correct and straightforward deduction from the principles of quantum mechanics; but is it not very paradoxical? How can the final state of the second particle be influenced by a measurement performed on the first, after all physical interaction has ceased between them?"

I had not the impression that Einstein
at that time saw in this case, cleverly presented with all the appearances of a paradox, anything else than an illustration of the unfamiliar features of quantum phenomena. Two years later, however, he gave it a much more prominent role in a paper written jointly with Podolsky and Rosen; combined with a "criterion of reality," it was now used with the intention to expose

an essential imperfection of quantum theory. Any attribute of a physical system that can be accurately determined without disturbing the system, thus went the argument, is an "element of physical reality," and a description of the system can only be regarded as complete if it embodies all the elements of reality which can be attached to it. Now, the example of the two particles shows that the position and the momentum of a given particle can be obtained by appropriate measurements performed on another particle without disturbing the first, and are therefore elements of reality in the sense indicated. Since quantum theory does not allow both to enter into the description of the state of the particle, such a description is incomplete. The paradox which this incomplete description presents, by suggesting an unaccountable influence of the measurement on the state of the particle, would of course not appear in a complete theory.

This onslaught came down upon us as a bolt from the blue.

24.12 I. 8 the Einstein-podolsky-rosen Paper

Commentary of Rosenfeld (1967)

In a complete theory there is an element corresponding to each element of reality. A sufficient condition for the reality of a physical quantity is the possibility of predicting it with certainty, without disturbing the system. In quantum mechanics in the case of two physical quantities described by non-commuting operators, the knowledge of one precludes the knowledge of the other. Then either (1) the description of reality given by the wave function in

1.

ANY serious consideration of a physical theory must take into account the distinction between the objective reality, which is independent of any theory, and the physical concepts with which the theory operates. These concepts are intended to correspond with the objective reality, and by means of these concepts we picture this reality to ourselves.

In attempting to judge the success of a physical theory, we may ask ourselves two questions: (1) "Is the theory correct?" and (2) "Is the description given by the theory complete?" It is only in the case in which positive answers may be given to both of these questions, that the concepts of the theory may be said to be satisfactory. The correctness of the theory is judged by the degree of agreement between the conclusions of the theory and human experience. This experience, which alone enables us to make inferences about reality, in physics takes the form of experiment and measurement. It is the second question that we wish to consider here, as applied to quantum mechanics.

quantum mechanics is not complete or (2) these two quantities cannot have simultaneous reality. Consideration of the problem of making predictions concerning a system on the basis of measurements made on another system that had previously interacted with it leads to the result that if (1) is false then (2) is also false. One is thus led to conclude that the description of reality as given by a wave function is not complete.

Whatever the meaning assigned to the term complete, the following requirement for a complete theory seems to be a necessary one: every element of the physical reality must have a counterpart in the physical theory. We shall call this the condition of completeness. The second question is thus easily answered, as soon as we are able to decide what are the elements of the physical reality.

The elements of the physical reality cannot be determined by a priori philosophical considerations, but must be found by an appeal to results of experiments and measurements. A comprehensive definition of reality is, however, unnecessary for our purpose. We shall be satisfied with the following criterion, which we regard as reasonable. If, without in any way

disturbing a system, we can predict with certainty (i.e., with probability equal to unity) the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity. It seems to us that this criterion, while far from exhausting all possible ways of recognizing a physical reality, at least provides us with one
such way, whenever the conditions set down in it occur.' Regarded not as a necessary, but merely as a sufficient, condition of reality, this criterion is in agreement with classical as well as quantum-mechanical ideas of reality.

To illustrate the ideas involved let us consider the quantum-mechanical description of the behavior of a particle having a single degree of freedom. The fundamental concept of the theory is the concept of state, which is supposed to be completely characterized by the wave function ψ, which is a function of the variables chosen to describe the particle's behavior. Corresponding to each physically observable quantity A there is an operator, which may be designated by the same letter.
If ψ is an eigenfunction of the operator A, that is, if

$$\psi' \equiv A\psi = a\psi \tag{1}$$

where a is a number, then the physical quantity A has with certainty the value a whenever the particle is in the state given by ψ. In accordance with our criterion of reality, for a particle in the state given by ψ for which Eq. (1) holds, there is an element of physical reality corresponding to the physical quantity A. Let, for example,

$$\psi = e^{(2\pi i/h)p_0 x}, \tag{2}$$

where h is Planck's constant, p_0 is some constant number, and x the independent variable. Since the operator corresponding to the momentum of the particle is

$$p = (h/2\pi i)\partial/\partial x, \tag{3}$$

we obtain

$$\psi' = p\psi = (h/2\pi i)\partial\psi/\partial x = p_0\psi. \tag{4}$$

Thus, in the state given by Eq. (2), the momentum has certainly the value p_0. It thus has meaning to say that the momentum of the particle in the state given by Eq. (2) is real.
On the other hand if Eq. (1) does not hold, we can no longer speak of the physical quantity A having a particular value. This is the case, for example, with the coordinate of the particle. The operator corresponding to it, say q, is the operator of multiplication by the independent variable. Thus,

$$q\psi = x\psi \neq a\psi. \tag{5}$$

In accordance with quantum mechanics we can only say that the relative probability that a measurement of the coordinate will give a result lying between a and b is

$$P(a,b) = \int_a^b \bar{\psi}\psi dx = \int_a^b dx = b - a \tag{6}$$

Since this probability is independent of a, but depends only upon the difference $b - a$, we see that all values of the coordinate are equally probable.

A definite value of the coordinate, for a particle in the state given by Eq. (2), is thus not predictable, but may be obtained only by a direct measurement. Such a measurement however disturbs the particle and thus alters its state. After the coordinate is determined, the particle will no longer be in the state given by Eq. (2). The usual conclusion from this in quantum

mechanics is that when the momentum of a particle is known, its coordinate has no physical reality.

More generally, it is shown in quantum mechanics that, if the operators corresponding to two physical quantities, say A and B, do not commute, that is, if $AB \neq BA$, then the precise knowledge of one of them precludes such a knowledge of the other. Furthermore, any attempt to determine the latter experimentally will alter the state of the system in such a way as to destroy the knowledge of the first.

From this follows that either (1) the quantummechanical description of reality given by the wave function is not complete or (2) when the operators corresponding to two physical quantities do not commute the two quantities cannot have simultaneous reality. For if both of them had simultaneous reality-and thus definite values these values would enter into the complete description, according to the condition of completeness. If then the wave function provided such a complete description of reality, it would contain these values; these would then be predictable. This not being the case, we are left with the alternatives stated.

In quantum mechanics it is usually assumed that the wave function does contain a complete description of the physical reality of the system in the state to which it corresponds. At first sight this assumption is entirely reasonable, for the information obtainable from a wave function seems to correspond exactly to what can be measured without altering the state of the system. We shall show, however, that this assumption, together with the criterion of reality given above, leads to a contradiction.

2.

For this purpose let us suppose that we have two systems, I and II, which we permit to interact from the time $t = 0$ to $t = T$, after which time we suppose that there is no longer any interaction between the two parts. We suppose further that the states of the two systems before $t = 0$ were known. We can then calculate with the help of Schrödinger's equation the state of the combined system I + II at any subsequent time; in particular, for any $t > T$. Let us designate the corresponding wave function by Ψ. We cannot, however, calculate the state in which either one of the two systems is left after the interaction. This, according to quantum mechanics, can be done only with the help of further measurements. by a process known as the reduction of the wave packet. Let us consider the essentials of this process.

Let $a_1, a_2, a_3, \cdots$ be the eigenvalues of some physical quantity A pertaining to system I and $u_1(x_1), u_2(x_1), u_3(x_1), \cdots$ the corresponding eigenfunctions, where x_1 stands for the variables used to describe the first system. Then Ψ, considcred as a function of x_1, can be expressed as

$$\Psi(x_1, x_2) = \sum_{n=1}^{\infty} \psi_n(x_2)\, u_n(x_1), \tag{7}$$

where x_2 stands for the variables used to describe the second system. Here $\psi_n(x_2)$ are to be regarded merely as the coefficients of the expansion of Ψ into a series of orthogonal functions $u_n(x_1)$. Suppose now that the quantity A is measured and it is found that it has the value a_k. It is then concluded that after the measurement the first system is left in the state given by the wave function $u_k(x_1)$, and that the second system is left in the state given by the wave function $\psi_k(x_2)$. This is the process of reduction of the wave packet; the wave packet given by the
infinite scrics (7) is reduced to a single term $\psi_k(x_2)\, u_k(x_1)$.

The set of functions $u_n(x_1)$ is determined by the choice of the physical quantity A. If, instead of this, we had chosen another quantity, say B, having the eigenvalues $b_1, b_2, b_3, \cdots$ and eigenfunctions $v_1(x_1), v_2(x_1), v_3(x_1), \cdots$ we should have obtained, instead of Eq. (7), the expansion

$$\Psi(x_1, x_2) = \sum_{s=1}^{\infty} \varphi_s(x_2)\, v_s(x_1) \tag{8}$$

where φ_s 's are the new coefficients. If now the quantity B is measured and is found to have the value b_r, we conclude that after the measurement the first system is left in the state given by $v_r(x_1)$ and the second system is left in the state given by $\varphi_r(x_2)$.

We see therefore that, as a consequence of two different measurements performed upon the first system, the second system may be left in states with two different wave functions. On the other hand, since at the time of measurement the two systems no longer interact, no real change can take place in the second system in consequence of anything that may be done to the first system. This is, of course, merely a statement of what is meant by the absence of an interaction between the two systems. Thus, it is possible to assign two different wave functions (in our example ψ_k and φ_r) to the same reality (the second system after the interaction with the first).

Now, it may happen that the two wave functions, ψ_k and φ_r, are eigenfunctions of two noncommuting operators corresponding to some physical quantities P and Q, respectively. That this may actually be the case can best be shown by an example. Let us suppose that the two systems are two particles, and that

$$\Psi(x_1, x_2) = \int_{-\infty}^{\infty} e^{(2\pi i/h)(x_1 - x_2 + x_0)p} dp \tag{9}$$

where x_0 is some constant. Let A be the momentum of the first particle; then, as we have seen in Eq. (4), its eigenfunctions will be

$$u_n(x_1) = e^{(2\pi i/h)px_1} \tag{10}$$

corresponding to the eigenvalue p. Since we have here the case of a continuous spectrum, Eq. (7) will now be written

$$\psi(x_1, x_2) = \int_{-\infty}^{\infty} \psi_p(x_2)\, u_p(x_1)\, dp \tag{11}$$

where

$$\psi_p(x_2) = e^{-(2\pi i/h)(x_2 - x_0)p}. \tag{12}$$

This ψ_p however is the eigenfunction of the operator

$$P = (h/2\pi i)\partial/\partial x_2, \tag{13}$$

corresponding to the eigenvalue $-p$ of the momentum of the second particle. On the other hand, if B is the coordinate of the first particle, it has for eigenfunctions

$$v_x(x_1) = \delta(x_1 - x), \tag{14}$$

corresponding to the eigenvalue x, where $\delta(x_1 - x)$ is the well-known Dirac delta-function. Eq. (8) in this case becomes

$$\Psi(x_1, x_2) = \int_{-\infty}^{\infty} \varphi_x(x_2)\, v_x(x_1)\, dx \tag{15}$$

where

$$\varphi_x(x_2) = \int_{-\infty}^{\infty} e^{(2\pi i/h)(x-x_2+x_0)p}\, dp = h\delta(x - x_2 + x_0) \tag{16}$$

This φ_x, however, is the eigenfunction of the operator

$$Q = x_2' \tag{17}$$

corresponding to the eigenvalue $x + x_0$ of the coordinate of the second particle. Since

$$PQ - QP = h/2\pi i, \tag{18}$$

we have shown that it is in general possible for ψ_k and φ_r to be eigenfunctions of iwo noncommuting operators, corresponding to physical quantities.

Returning now to the general case contemplated in Eqs. (7) and (8), we assume that ψ_k and φ_r are indeed eigenfunctions of some noncommuting operators P and Q, corresponding to the eigenvalues p_k and q_r, respectively. Thus, by measuring either A or B we are in a position to predict with certainty, and without in any way
disturbing the second system, either the value of the quantity P (that is p_k) or the value of the quantity Q (that is q_r). In accordance with our criterion of reality, in the first case we must consider the quantity P as being an element of reality, in the second case the quantity Q is an element of reality. But, as we have seen, both wave functions ψ_k and φ_r belong to the same reality.

Previously we proved that either (1) the quantum-mechanical description of reality given by the wave function is not complete or (2) when the operators corresponding to two physical quantities do not commute the two quantities cannot have simultaneous reality. Starting then with the assumption that the wave function does give a complete description of the physical reality, we arrived at the conclusion that two physical quantities, with noncommuting operators, can have simultaneous reality. Thus the negation of (1) leads to the negation of the only other alternative (2). We are thus forced to conclude that the quantum-mechanical description of physical reality given by wave functions is not complete.

One could object to this conclusion on the grounds that our criterion of reality is not sufficiently restrictive. Indeed, one would not arrive at our conclusion if one insisted that two or more physical quantities can be regarded as simultaneous elements of reality only when they can be simultaneously measured or predicted. On this point of view, since either one or the other, but not both simultaneously, of the quantities P and Q can be predicted, they are not simultaneously real. This makes the reality of P and Q depend upon the process of measurement carried out on the first system, which does not disturb the second system in any way. No reasonable definition of reality could be expected to permit this.

While we have thus shown that the wave function does not provide a complete description of the physical reality, we left open the question of whether or not such a description exists. We believe, however, that such a theory is possible.

24.13 I. 9 Bohr's Reply

This onslaught came down upon us as a bolt fiom the blue. Its effect on Bohr was remarkable. We were then in the midst of groping attempts at exploring the implications of the fluctuations of charge and current distributions, which presented us with riddles of a kind we had not met in electrodynamics. A new worry could not come at a less propitious time. Yet, as soon as Bohr had heard my report of Einstein's argument, everything else was abandoned: we had to clear up such a misundcrstanding at once. We should reply by taking up the same example and showing the right way to speak about it. n great excitement, Bohr immediately started

dictating to me the outline of such a reply. Very soon, however, he became hesitant: "No, this won't do, we must try all over again . . . we must make it quite clear...." So it went on for a while, with growing wonder at the unexpected subtlety of the argument. Now and then, he would turn to me: "What can they mean? Do you understand it?" There would follow some inconclusive exegesis. Clearly, we were farther from the mark than we first thought. Eventually, he broke off with the familiar remark that he "must sleep on it." The next morning he at once took up the dictation again, and I was struck by a change in the tone of the sentences: there was no trace in them of the previous day's sharp expressions of dissent. As I pointed out to him that he seemed to take a milder view of the case, he

Commentary of Rosenfeld (1967)

smiled: "That's a sign," he said, "that we are beginning to understand the problem." And indeed, the real work now began in earnest: day after day, week after week, the whole argument was patientily scrutinized with the help of simpler and more transparent examples. Einstein's problem was reshaped and its solution reformulated with such precision and clarity that the weakness in the critics' reasoning became evident. and their whole argumentation, for all its faise briliance, fell to pieces. "They do it 'smartly,'" Bohr commented, "but what counts is to do it right."

The refutation of Einstein's criticism does not add any new clement to the conception of complementarity, but it is of great importance in laying bare a very deep-iying opposition between Bohr's general philosophical attitude and the still widespread habits of thought belonging to a glorious but irrevocably bygone stage in the evolution of science. Physical concepts, Einstein used to say, are "free creations of the mind." In the case under debate, the "criterion of reality" he proposed has very much this character, and it turns out to yield a striking illustration of the pitfalls to which one may be exposed by such arbitrary constructions of concepts. In spite of its apparent clarity, the criterion in question contains in fact a very essential ambiguity, hidden in the seemingly harmless restriction "without disturbing the system." To disclose this ambiguity, how-
ever, it is necessary to renounce any of the quantal description of physical pretension to impose upon nature our phenomena was the last clash between own preconceived notion of what "clements of reality" ought to be, and humbly take guidance, as Bohr exhorts us to do, in what we can iearn from nature herself.

When one realizes the fundamental nature of the issue at stake, it becomes easier to understand the state of exaltation in which Bohr accompiished this work. The writing of his reply, its typing, polishing, retyping and sending off to print did not take more than six weeksan astonishing speed when one knows how slow his usual pace was. It was impressive to watch him thus at the height of his powers, in utmost concentration and unrelenting effort to attain clarity through painstaking scrutiny of every detail - true as ever to his favourite Schiller aphorism "Nur die Flle fhrt zur Klarheit." He was particularly well served on this occasion by his uncommon ability to go into the opponent's views, dissect his arguments and turn them to the advantage of the truth. In this, however, he always procceded with complete openmindedness, and only rejoiced in victory if in winning it he had also deepened his own insight into the problem.

The contest about the completeness
the two giants. The confrontation of their diverging conceptions of the nature of scientific knowledge had now reached the limits set by confining it to the problems of the physical world. That there was no hope of carrying it further was soon made clear by Einstein himself, who commented on Bohn's position that it was logically possible, but "so very contrary to my scientific instinct that i cannot forego the search for a more complete conception." Bohr was very unhappy about this deadlock, for he admired Einstein precisely for the way in which

he had laid stress on the epistemological aspects of classical physics and, at an early stage, of quantum theory also. In fact, Einstein's approach to these problems had been so closely similar to his own, and such a source of inspiration to him, that he found Einstein's later lack of understanding doubly disheartening. On the other hand, he had good reason to look back with satisfaction on a controversy which had put to such severe test his own conception of the complementarity of physical phenomena, and even, in this last dispute about an alleged "criterion of reality," the underlying general ideas he had formed of the most fundamental aspects of human knowledge and man's position in the universe.

24.14 1. 9 Quantum Mechanics and Physical Reality

Niels Bohr

In a recent article by A. Einstein, B. Podolsky and N. Rosen, which appeared in the Physical Review of May 15, and was reviewed in Nature of June 22, the question of the completeness of quantum mechanical description has been discussed on the basis of a "criterion of physical reality", which the authors formulate as follows: "If, without in any way disturbing a system, we can predict with certainty the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity".

Since, as the authors show, it is always possible in quantum theory, just as in classical theory, to predict the value of any variable involved in the description of a mechanical system from measurements performed on other systems, which have only temporarily been in interaction with the system under investigation; and since in contrast to elassical mechanics it is never possible in quantum mechanics to assign definite values to both of two conjugate variables, the authors conclude from their criterion that quantum mechanical description of physical reality is incomplete.

I should like to point out, however, that the named criterion contains an essential ambiguity when it is applied to problems of quantum mechanics. It is true that in the measurements under consideration any direct mechanical interaction of the system and the measuring agencies is excluded, but a closer examination reveals that the procedure of measurements has an essential influence on the conditions on which the very definition of the physical quantities in question rests. Since these conditions must be considered as an inherent element of any, phenomenon to which the term "physical reality" can be unambiguously applied, the conclusion of the abovementioned authors would not appear to be justified. A fuller development of this argument will be given in an article to be published shortly in the Physical Review.

N. Bohr.

Institute of Theoretical Physics, Copenhagen.

June 29.

Originally published in Nature, 136, 65 (1935).

24.15 I. 10 Can Quantum-mechanical Description of Physical Reality Be Considered Complete?

It is shown that a certain "criterion of physical reality" formulated in a recent article with the above titie by A. Einstein, B. Pulusky aud N. Rusen cuntains an essential ambiguity when it is applied to quantum phenomena. In this connection a viewpoint termed "complementarity" is explained from which quantum-mechanical description of physical phenomena would seem to fulfill, within its scope, all rational demands of completeness.

I [N]a recent article [1] under the above title A . Einstein, B. Podolsky and N. Rosen have presented arguments which lead them to answer the question at issue in the negative. The trend of their argumentation, however, does not seem to me adequately to meet the actual situation

with which we are faced in atomic physics. I shall therefore be glad to use this opportunity to explain in somewhat greater detail a general viewpoint, conveniently termed "complementarity," which I have indicated on various previous occasions, [2] and from which quantum mechanics within its scope would appear as a completely rational description of physical phenomena, such as we meet in atomic processes.

The extent to which an unambiguous meaning can be attibuted to such an expression as "physical reality" cannot of course be deduced from a priori philosophical conceptions, but-as the authors of the article cited themselves emphasize-must be founded on a direct appeal to experiments and measurements. For this purpose they propose a "criterion of reality" formulated as follows: "If, without in any way disturbing a system, we can predict with certainty the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity." By means of an interesting example, to which we shall return below, they next proceed to show that in quantum mechanics, just as in classical mechanics, it is possible under suitable conditions to predict the value of any given variable pertaining to the description of a nechanical system from measurements performed entirely on other systems which previously have been in

iA. Einsiein, B. Fudusky and N. Rösen, Phys. Rev. 17, 777 (1935).

2 Cf. N. Bohr, Atomic Theory and Description of Nature, I [2] Cf. N. Bohr, Atom).
(Cambridge, 1934).

interaction with the system under investigation. According to their criterion the authors therefore want to ascribe an element of reality to each of the quantities represented by such variabies. Since, moreover, it is a well-known feature of the present formalism of quantum mechanics that it is never possible, in the description of the state of a mechanical system, to attach definite values to both of two canonicaily conjugate variables, they consequently deem this formalism to be incomplete, and express the belief that a more satisfactory theory can be developed.

Such an argumentation, however, would hardly seem suited to affect the soundness of quantum-mechanical description, which is based on a coherent mathematical formalism covering automatically any procedure of measurement like that indicated.* The apparent contradiction in

- The deductions contained in the article cited may in this respect be considered as an immediate consequence of the transtormation theorems other feature of the formalism contribute to sccure its mathematical completeness and its rational correspondence with classical mechanics. In fact, it is a ways possible in the description of a mechanical system, consisting of two partial systems (1) and (2), interacting or not, to replace any two pairs of to systems (1) and (2), respectively, and satisfying the usual commutation rules

$$[q_1 p_1] = [q_2 p_2] = ih/2\pi$$
$$[q_1 q_2] = [p_1 p_2] = [q_1 p_2] = [q_2 p_1] = 0$$

by two pairs of new conjugate variables $(Q_1 P_1)\,, (Q_2 P_2)$ related to the first variables by a simple orthogonal transformation, corresponding to a rotation of angle θ in the planes $(q_1 q_2)\,, (p_1 p_2)$

$$q_1 = Q_1 \cos\theta - Q_2 \sin\theta \quad p_1 = P_1 \cos\theta - P_2 \sin\theta$$
$$q_2 = Q_1 \sin\theta + Q_2 \cos\theta \quad p_2 = P_1 \sin\theta + P_2 \cos\theta$$

Since these variables will satisfy analogous commutation rules, in particular

$$[Q_1 P_1] = ih/2\pi, \quad [Q_1 P_2] = 0$$

it follows that in the description of the state of the combined system definite numerical values may not be assigned to both $\hat{Q}_1$ and F_1, bui that we may clearly assign

fact discloses only an essential inadequacy of the customary viewpoint of natural philosophy for a rational account of physical phenomena of the type with which we are concerned in quantum mechanics. Indeed the finite interaction between object and measuring agencies conditioned by the very existence of the quantum of action entails -because of the impossibility of controlling the reaction of the object on the measuring instruments if these are to serve their purpose-the necessity of a final renunciation of the classical ideal of causality and a radical revision of our attitude towards the problem of physical reality. In fact, as we shall see, a criterion of reality like that proposed by the named authors con-tains-however cautious its formulation may appear-an essential ambiguity when it is applied to the actual problems with which we are here concerned. In order to make the argument to this end as clear as possible, I shall first consider in some detail a few simple examples of measuring arrangements.

Let us begin with the simple case of a particle passing through a slit in a diaphragm, which may form part of some more or less complicated experimental arrangement. Even if the momentum of this particle is completely known before it impinges on the diaphragm, the diffraction by the slit of the plane wave giving the symbolic representation of its state will imply an uncertainty in the momentum of the particle, after it has passed the diaphragm, which is the greater the narrower the slit. Now the width of the slit, at any rate if it is still large compared with the wave-length, may be taken as the uncertainty Δq of the position of the particle relative to the diaphragm, in a direction perpendicular to the slit. Moreover, it is simply seen from de Broglie's relation between momentum and wave-length that the uncertainty Δp of the momentum of the particle in this direction is correlated to Δq by means of Heisenberg's general principle

$$\Delta p \Delta q \sim h$$

which in the quantum-mechanical formalism is a direct consequence of the commutation relation for any pair of conjugate variables. Obviously the uncertainty Δp is inseparably connected with the possibility of an exchange of momentum between the particle and the diaphragm; and the question of principal interest for our discussion is now to what extent the momentum thus exchanged can be taken into account in the description of the phenomenon to be studied by the experimental arrangement concerned, of which the passing of the particle through the slit may be considered as the initial stage.

Let us first assume that, corresponding to usual experiments on the remarkable phenomena of electron diffraction, the diaphragm, like the other parts of the apparatus,-say a second diaphragm with several slits parallel to the first and a photographic plate,-is rigidly fixed to a support which defines the space frame of reference. Then the momentum exchanged between the particle and the diaphragm will, together with the reaction of the particle on the other bodies, pass into this common support, and we have thus voluntarily cut ourselves off from any. possibility of taking these reactions separately into account in predictions regarding the final result of the experiment,-say the position of the spot produced by the particle on the photographic plate. The impossibility of a closer analysis of the reactions between the particle and the measuring instrument is indeed no peculiarity of the experimental procedure described, but is rather an essential property of any arrangement suited to the study of the phenomena of the type concerned, where we have to do with a feature of individuality completely foreign to classical physics. In fact, any possibility of taking into account the momentum exchanged between the particle and the separate parts of the apparatus would at once permit us to draw conclusions regarding the "course" of such phenomena,-say through what particular slit of the

[8]such values to both Q_1 and P_2. In that case it further results from the expressions of these variables in terms of ($q_1 p_1$) and ($q_2 p_2$), namely
$Q_1 = q_1 \cos\theta + q_2 \sin\theta, \quad P_2 = -p_1 \sin\theta + p_2 \cos\theta,$
that a subsequent measurement of either q_2 or p_2 will allow us to predict the value of q_1 or p_1 respectively.

second diaphragm the particle passes on its way to the photographic plate-which would be quite incompatible with the fact that the probability of the particle reaching a given element of area on this plate is determined not by the presence of any particular slit, but by the positions of all the slits of the second diaphragm within reach
of the associated wave diffracted from the slit of the first diaphragm.

By another experimental arrangement, where the first diaphragm is not rigidly connected with the other parts of the apparatus, it would at least in principle* be possible to measure its momentum with any desired accuracy before and after the passage of the particle, and thus to predict the momentum of the latter after it has passed through the slit. In fact, such measurements of momentum require only an unambiguous application of the classical law of conservation of momentum, applied for instance to a collision process between the diaphragm and some test body, the momentum of which is suitably controlled before and after the collision. It is true that such a control will essentially depend on an examination of the space-time course of some process to which the ideas of classical mechanics can be applied; if, however, all spatial dimensions and time intervals are taken sufficiently large, this involves clearly no limitation as regards the accurate control of the momentum of the test bodies, but only a renunciation as regards the accuracy of the control of their space-time coordination. This last circumstance is in fact quite analogous to the renunciation of the control of the momentum of the fixed diaphragm in the experimental arrangement discussed above, and depends in the last resort on the claim of a purely classical account of the measuring apparatus, which implies the necessity of allowing a latitude corresponding to the quantum-mechanical uncertainty relations in our description of their behavior.

The principal difference between the two experimental arrangements under consideration is, however, that in the arrangement suited for the control of the momentum of the first diaphragm, this body can no longer be used as a measuring instrument for the same purpose as in the previous case, but must, as regards its position relative to the rest of the apparatus, be treated, like the particle traversing the slit, as an object of

investigation, in the sense that the quantummechanical uncertainty relations regarding its position and momentum must be taken explicitly into account. In fact, even if we knew the position of the diaphragm relative to the space frame before the first measurement of its momentum, and even though its position after the last measurement can be accurately fixed, we lose, on account of the uncontrollable displacement of the diaphragm during each collision process with the test bodies, the knowledge of its position when the particle passed through the slit. The whole arrangement is therefore obviously unsuited to study the same kind of phenomena as in the previous case. In particular it may be shown that, if the momentum of the diaphragm is measured with an accuracy sufficient for allowing definite conclusions regarding the passage of the particle through some selected slit of the second diaphragm, then even the minimum uncertainty of the position of the first diaphragm compatible with such a knowledge will imply the total wiping out of any interference effect-regarding the zones of permitted impact of the particle on the photographic plate-to which the presence of more than one slit in the second diaphragm would give rise in case the positions of all apparatus are fixed relative to each other.

In an arrangement suited for measurements of the momentum of the first diaphragm, it is further clear that even if we have medsured this momentum before the passage of the particle

8

- The obvious impossibility of actually carrying out, with the experimental technique at our disposal, such measuring procedures as are discussed here and in the following does clearly not affect the theoretical argument, since the procedures in question are essentially equivalent with atomic processes, like the Compton effect, where a corresponding application of the conservation theorem of momentum is well established.

through the slit, we are after this passage still left with a free choice whether we wish to know the momentum of the particle or its initial position relative to the rest of the apparatus. In the first eventuality we need only to make a second determination of the momentum of the diaphragm, leaving unknown forever its exact position when the particle passed. In the second eventuality we need only to determine its position relative to the space frame with the inevitable loss of the knowledge of the momentum exchanged between the diaphragm and the particle. If the diaphragm is sufficiently massive in compatison with the particle, we may even arrange the procedure of measurements in such a way that the diaphragm after the first determination of its momentum will remain at rest in some unknown position relative to the
instrument rigidly fixed to the support which defines the space frame of reference. Under the experimental conditions described such a measurement will therefore also provide us with the knowledge of the location, otherwise completely unknown, of the diaphragm with respect to this space frame when the particles passed through the slits. Indeed, only in this way we obtain a basis for conclusions about the initial position of the other particle relative to the rest of the apparatus. By allowing an essentially uncontrollable momentum to pass from the first particle into the mentioned support, however, we have by this procedure cut ourselves off from any future possibility of applying the law of conservation of momentum to the system consisting of the diaphragm and the two particles and therefore have lost our only basis for an unambiguous application of the idea of momentum in predictions regarding the behavior of the second particle. Conversely, if we choose to measure the momentum of one of the particles, we lose through the uncontrollable displacement inevitable in such a measurement any possibility of deducing from the behavior of this particle the position of the diaphragm relative to the rest of the apparatus, and have thus no basis whatever for predictions regarding the location of the other particle.

From our point of view we now see that the wording of the above-mentioned criterion of physical reality proposed by Einstein, Podolsky and Rosen contains an ambiguity as regards the meaning of the expression "without in any way disturbing a system." Of course there is in a case like that just considered no question of a mechanical disturbance of the system under investigation during the last critical stage of the measuring procedure. But even at this stage there is essentially the question of an influence on the very conditions which define the possible types of predictions regarding the future behavior of the system. Since these conditions constitute an inherent element of the description of any phenomenon to which the term "physical reality" can be properly attached, we see that the argumentation of the mentioned authors does not justify their conclusion that quantum-mechanical description is essentially incomplete. On the contrary this description, as appears from the pre-
ceding discussion, may be characterized as a rational utilization of all possibilities of unambiguous interpretation of measurements, compatible with the finite and uncontrollable interaction between the objects and the measuring instruments in the field of quantum theory. In fact, it is only the mutual exclusion of any two experi mental procedures, permitting the unambiguous definition of complementary physical quantities, which provides room for new physical laws, the coexistence of which might at first sight appear irreconcilable with the basic principles of science. It is just this entirely new situation as regards the description of physical phenomena, that the notion of complementarity aims at characterizing.

The experimental arrangements hitherto discussed present a special simplicity on account of the secondary role which the idea of time plays in the description of the phenomena in question. It is true that we have freely made use of such words as "before" and "after" implying timerelationships; but in each case allowance must be made for a certain inaccuracy, which is of no importance, however, so long as the time intervals concerned are sufficiently large compared with the proper periods entering in the closer analysis of the phenomenon under investigation. As soon as we attempt a more accurate time description of quantum phenomena, we meet

with well-known new paradoxes, for the elucidation of which further features of the interaction between the objects and the measuring instruments must be taken into account. In fact, in such phenomena we have no longer to do with experimental arrangements consisting of apparatus essentially at rest relative to one another, but with arrangements containing moving parts,-like shutters before the slits of the diaphragms,-controlled by mechanisms serving as clocks. Besides the transfer of momentum, discussed above, between the object and the bodies defining the space frame, we shall therefore, in such arrangements, have to consider an eventual exchange of energy between the object and these clock-like mechanisms.

The decisive point as regards time measurements in quantum theory is now completely analogous to the argument concerning measurements of positions outlined above. Just as the transfer of momentum to the separate parts of
other parts of the apparatus, and the subsequent fixation of this position may therefore simply consist in establishing a rigid connection between the diaphragm and the common support.
My main purpose in repeating these simple, and in substance well-known considerations, is to emphasize that in the phenomena concerned we are not dealing with an incomplete description characterized by the arbitrary picking out of different elements of physical reality at the cost of sacrifying other such elements, but with a rational discrimination between essentially different experimental arrangements and procedures which are suited either for an unambiguous use of the idea of space location, or for a legitimate application of the conservation theorem of momentum. Any remaining appearance of arbitrariness concerns merely our freedom of handling the measuring instruments, characteristic of the very idea of experiment. In fact, the renunciation in each experimental arrangement of the one or the other of two aspects of the description of physical phenomena, -the combination of which characterizes the method of classical physics, and which therefore in this sense may be considered as complementary to one another,–depends essentially on the impossibility, in the field of quantum theory, of accurately controlling the reaction of the object on the measuring instruments, i.e., the transfer of momentum in case of position measurements, and the displacement in case of momentum measurements. Just in this last respect any comparison between quantum mechanics and ordinary statistical mechanics,-however useful it may be for the formal presentation of the theory, -is essentially irrelevant. Indeed we have in each experimental arrangement suited for the study of proper quantum phenomena not merely to do with an ignorance of the value of certain physical quantities, but with the impossibility of defining these quantities in an unambiguous way.
The last remarks apply equally well to the special problem treated by Einstein, Podolsky and Rosen, which has been referred to above, and which does not actually involve any greater intricacies than the simple examples discussed above. The particular quantum-mechanical state of two free particles, for which they give an explicit mathematical expression, may be reproduced, at least in principle, by a simple experimental arrangement, comprising a rigid diaphragm with two parallel slits, which are very narrow compared with their separation, and through each of which one particle with given initial momentum passes independently of the other. If the momentum of this diaphragm is measured accurately before as well as after the passing of the particles, we shall in fact know the sum of the components perpendicular to the slits of the momenta of the two escaping particles, as well as the difference of their initial positional coordinates in the same direction; while of course the conjugate quantities, i.e., the difference of the components of their momenta, and the sum of their positional coordinates, are entirely unknown.* In this arrangement, it is therefore clear that a subsequent single measurement either of the position or of the momentum of one of the particles will automatically determine the position or momentum, respectively, of the other particle with any desired accuracy; at least if the wave-length corresponding to the free motion of each particle is sufficiently short compared with the width of the slits. As pointed out by the named authors, we are therefore faced at this stage with a completely free choice whether we want to determine the

one or the other of the latter quantities by a process which does not directly interfere with the particle concerned.

Like the above simple case of the choice between the experimental procedures suited for the prediction of the position or the momentum of a single particle which has passed through a slit in a diaphragm, we are, in the "freedom of choice" offered by the last arrangement, just concerned with a discrimination between different experimental procedures which allow of the unambiguous use of complementary classical concepts. In fact to measure the position of one of the particles can mean nothing else than to establish a correlation between its behavior and some

the apparatus,-the knowledge of the relative positions of which is required for the description of the phenomenon,–has been seen to be entirely uncontrollable, so the exchange of energy between the object and the various bodies, whose relative motion must be known for the intended use of the apparatus, will defy any closer analysis. Indeed, it is excluded in principle to control the energy which goes into the clocks without interfering essentially with their use as time indicators. This use in fact entirely relies on the assumed possibility of accounting for the functioning of each clock as well as for its eventual comparison with other clocks on the basis of the methods of classical physics. In this account we must therefore obviously allow for a latitude in the energy balance, corresponding to the quan-tum-mechanical uncertainty relation for the conjugate time and energy variables. Just as in the question discussed above of the mutually exclusive character of any unambiguous use in quantum theory of the concepts of position and momentum, it is in the last resort this circumstance which entails the complementary relationship between any detailed time account of atomic plenomena on the one hand and the unclassical features of intrinsic stability of atoms, disclosed by the study of energy transfers in atomic reactions on the other hand.

This necessity of discriminating in each experimental arrangement between those parts of the physical system considered which are to be treated as measuring instruments and those which constitute the objects under investigation may indeed be said to form a principal distinction between classical and quantum-mechanical description of physical phenomena. It is true that the place within each measuring procedure where this discrimination is made is in both cases largely a matter of convenience. While, however, in classical physics the distinction between object and measuring agencies does not entail any difference in the character of the description of the phenomena concerned, its fundamental importance in quantum theory, as we have seen, has its root in the indispensable use of classical concepts in the interpretation of all proper measurements, even though the classical theories do not suffice in accounting for the new types of regularities with which we are concerned in atomic physics.

In accordance with this situation there can be no question of any unambiguous interpretation of the symbols of quantum mechanics other than that embodied in the well-known rules which allow to predict the results to be obtained by a given experimental arrangement described in a totally classical way, and which have found their general expression through the transformation theorems, already referred to. By securing its proper correspondence with the classical theory, these theorems exclude in particular any imaginable inconsistency in the quantum-mechanical description, connected with a change of the place where the discrimination is made between object and measuring agencies. In fact it is an obvious consequence of the above argumentation

---

8

- As will be seen, this description, apart from a trivial normalizing factor, corresponds exactly to the transformation of variables described in the preceding footnote if $(q_1 p_1), (q_2 p_2)$ represent the positional coordinates and components of momenta of the two particles and if $\theta = -\pi/4$. It may also be remarked that the wave function given by formula (9) of the article cited corresponds to the special choice of $P_2 = 0$ and the limiting case of two infinitely narrow slits.

that in each experimental arrangement and measuring procedure we have only a free choice of this place within a region where the quantum-mechanical description of the process concerned is effectively equivalent with the classical description.

Before concluding I should still like to emphasize the bearing of the great lesson derived from general relativity theory upon the question of physical reality in the field of quantum theory. In fact, notwithstanding all characteristic differences, the situations we are concerned with in these generalizations of classical theory present striking analogies which have often been noted. Especially, the singular position of measuring instruments in the account of quantum phenomena, just discussed, appears closely analogous to the well-known necessity in relativity theory of upholding an ordinary description of all measuring processes, including a sharp distinction between space and time coordinates, although the very essence of this theory is the establishment of new physical laws, in the comprehension of which we must renounce the customary separation of space and time ideas.*

The dependence on the reference system, in relativity theory, of all readings of scales and clocks may even be compared with the essentially uncontrollable exchange of momentum or energy between the objects of measurements and all instruments defining the space-time system of

arrangements, which had to be left out of this article, where the main stress is laid on the dialectic aspect of the question at issue.

reference, which in quantum theory confronts us with the situation characterized by the notion of complementarity. In fact this new feature of natural philosophy means a radical revision of our attitude as regards physical reality, which may be paralleled with the fundamental modification of all ideas regarding the absolute character of physical phenomena, brought about by the general theory of relativity.

24.16 I. 11 Present Situation in Quantum Mechanics: a Translation of Schrdinger's "cat Paradox" Paper

24.16.1 Introduction

This is a translation of Schrödinger's three-part 1935 paper [1] in Die Vaturaissenschaften. Earlier that same year there had appeared the Einstein. Podolsky, Rosen paper" (also famous in "paradoxology) when, Schrodinger says, in a footnote, motivated his offering. Nong with this article in German. Schrodinger had two closely related English-language publications. But the Cierman, aside from its oneparagraph presentation of the famous cat, covers additional territory and gives many fascinating insights into Schroulinger's thought. The translator's goal has been to adhere to the logical and physical content of the original. while at the same time trying to convey something of its semi-conversational, at times slightiy sardonic flavor.

8

- Just this circumstance, together with the relativistic invariance of the uncertainty relations of quantum mechanics, ensures the compatibility between the argumentation outlined in the present article and all exigencies of relativity theory. This question will be treated in greater detail in a paper under preparation, where the writer will in particular discuss a very interesting paradox suggested by Einstein concerning the application of gravitation theory to energy measurements, and the solution of which offers an especially instructive illustration of the generality of the argument of complementarity. On the same occasion a more thorough discussion of space-time measurements in quantum theory will be given with all necessary mathematical developments and diagrams of experimental

24.16.2 1. The L'hysics of Models

In the second half of the previous century there arose, from the great progress in kinetic theory of gases and in the mechanical theory of heat, an ideal of the exact description of nature that stands out as the reward of centuries-long search and the fulfillment of millennia-long hope, and that is called classical. These are its features.

Of natural objects, whose observed behavior one might ireat, one setis up a representation-based on the experimental data in one's possession but without handcuffing the intuitive imagination-that is worked out in all details exactly, much more exactly than any experience, considering its limited extent. can ever authenticate. The representation in its absolute determinacy resembles a mathematical concept or a geometric figure which can be completely calculated from a number of determining parts: as, e.g., a triangle's one side and two adjoining angles, as determining parts, also determine the third angle, the

other two sides. the three altitudes. the radius of the inscribed circle. etc. Yet the epresentation differs intrinsically from a geometric figure in this important respect. that also in time as fourth dimension it is just as sharply determined as the ligure is in the three space rlimensime. Thus it is a question as is self-evident) always of a concept that changes with time, that can assume different states and if a state becomes known in the necessary number of determining parts, then not only are all other parts also given for this moment (as illusirated for the triangle above). hut likewist all parts, the complete state, for any given later time: just as the character of a triangle on its hase determines its character at the apex. It is part of the inner law of the concept that it should change in a given mammer, that is, if left to itself in a given initial state, that it should continuously run through a given sequence of states, each one of which it reaches at a fully determined time. That is its nature. that is the hypothesis, which, as I said above, one builds on a foundation of intuitive imagination.

Of course one must not think so literally, that in this way one learns how things go in the real world. To show that one does not think this, one calls the precise thinking aid that one has created, an image or a model. With its hindsight-free clarity, which cannot be attained without arbitrariness, one has merely insured that a fully determined hypothesis can be tested for its consequences, without admitting turther arbitrarmess during the tedious calculations required for deriving these consequences. Here one has explicit marching orders and actually works out only what a clever fellow could have told directly from the data! . It least one then knows where the arbitrariness lies and where improvement must be made in case of disagreement with experience: in the initial hypothesis or model. For this one must always be prepared. If in many various experiments the matural object hehaves like the model, one is happy and thinks that the mage fits the reality in essential features. If it fails to agree, under novel experiments or with refined measuring techniques it is not said that one should not be happy. For basically this is the means of gradually bringing our picture, i.e., our thinking, closer to the realities.

The classical method of the precise model has as principal goal keeping the unavoidable arbitrariness

neatly isolated in the assumptions, more or less as body cells isolate the nucleoplasm, for the historical process of adaptation to continuing experience. Perhaps the method is based on the belief that somehoa' the initial state roally determines uniquely the subsequent events. or that a complete model. agreeing with reality in complete exactness would permit predictive

8

- Box 79. Route 1. Millington, Md. 21651.

[1] E. Schrodinger, "Die gegenwartige Situation in der Quantenmechanik," Naturzcissenschaften 23 : pp. 807-812: 823828; 844-849 (1935).

[2] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. 47 : p. 777 (1935).

[3] E. Schrödinger, Proc. Cambridge Phil. Soc. 31 : p. 555 (1935) ; ibid., 32 : p. 446 (1936).

calculation of outcomes of all experiments with complete exactness. Perhaps on the other hand this behef is based on the method. But it is quite probable that the adaptation of thought to experience is an infinite process and that "complete model" is a contradiction in terms, somewhat like "largest integer."

A clear presentation of what is meant by classical model. its determining parts. its state, is the foundation for all that follows. Above all. a determinate model and a determinate state of the same must not be confused. Best consider an example. The Rutherford model of the hydrogen atom consists of two point masses. As determining parts one could for example use the two times three rectangular coordinates of the two points and the two times three components of their velocities along the coordinate axes-thus twelve in all. Instead of these one could also choose: the coordinates and velocity components of the conter of mass. plus the separation of the two points, two angles that establish the direction in space of the line joining them, and the speeds (= time derivatives) with which the separation and the iwo angles are changing at the particular moment; this again adds up of course to twelve. It is not part of the concept "R-model of the 11-atom" that the determining parts hould have particular numerical values. Such being assigned to them. one arrives at a determinate state of the model. The clear view over the totality of possible states-yet without relationship among them -constitutes "the model" or "the model in any state whatsocrer." But the concept of the model then amounts to more than merey: the two points in certain positions, endowed with certain velocities. It embodies also knowledge for every state how it will change with time in absence of outside interference. (Information on how one half of the determining parts will change with time is indeed given by the other half, but how this other half will change must be independently determined.) This knowledge is implicit in the assumptions: the points have the masses m.M and the charges $-$e. $+$ e and therefore attract each other with force $\mathrm{e}^2/\mathrm{r}^2$, if their separation is r.

These results, with definite numerical values for m, M, and e (but of course not for r). belong to the description of the model (not first and only to that of a definite state). m, M, and e are not determining parts. By contrast, separation r is one. It appears as the seventh in the second "set" of the example introduced above. And if one uses the first, r is not an independent thirteenth but can be calculated from the 6 rectangular coordinates:

$$r = \left|(x_1 - x_y)^2 + (y_1 - y_y)'' + (z_1 - z_y)^2\right|^2 .$$

The number of determining parts (which are often called a riables in contrast to constants of the model such as m, M, e) is mulimited. Twelve conveniently chosen ones determine all others or the state. No twelve have the privilege of being the determining parts. Examples of other especially important determining parts are: the energy, the three compoments of angular momentum relative to center of mass, the kinetic energy of center of mass motion. These just named have, however, a special character. They are indeed zariable i.e.. they have different values in different states. But in every sequence of states, that is actually passed through in the course of time, they retain the same value. So they are also called constants of the motion– differing from constants of the model.

2. Statistics of Vodel I'anables in Unantam . Hechanics

At the pivot point of contemporary quantum mechanics (Q.M.) stands a doctrine, that perhaps may yet modergo many shifts of meaning but that will not, I an convinced. cease to be the pivot point. It is this, that models with determining parts that uniquely determine each other, as do the classical ones. cannot do justice to nature.

One might think that for anyone believing this, the classical models have played out their roles. But this is not the case. Rather one uses precisely than, not only to express the negative of the new doctrine, but also to describe the diminished mutual determinacy renaining afterwards as though obtaining among the same variables of the same models as were used earlier, as

follows:
-4 The chasical concept of state becomes lust, in that at most a well-chosen half of a complete set of variables can be assigned definite numerical values; in the Rutherford example for instance the six recdangular coordinates or the velocity components (still other grompings are possible). The other half then remains completely indeterminate, while supernumerary parts can show highly varying degrees of indeterminacy. In general. of a complete set (for the R-nodel twelve parts) all will be known only uncentainly. One can best keep track of the degree of meertainty by following classical mechanics and choosing variables arranged in pairs of so-called canonically-conjugate ones. The simplest example is a space coordinate x of a point mass and the component p_1 along the same direction, its linear momentum (i.e.. mass times velocity). Two such constrain each other in the precision with which they
may be simultaneously known. in that the product of their tolerance- or variation-widths (customarily designated by putting a Δ ahead of the quantity) cannot fall below the magnitude of a certain universal constant, [4] thus

$$\Delta x \cdot \Delta p_{\mathrm{n}} \geqq h$$

(Heisenberg uncertainty relation.)
B. If even at any given moment not all variables are determined by some of them, then of course neither are they all determined for a later moment by data obtainable earlier. This may be called a break with causality. but in view of %. it is nothing essentially new. If a classical state does not exist at any moment, it can hardly change causally. What do change are the statistics or probabilitics. these moreover causally. Individual variables meanwhile may become more. or less. mucertain. Overall it may be said that the total precision of the description does not change with time, because the principle of limitations described under . I. remains the same at every moment. —

Now what is the meaning of the terms "uncertain," "statistics." "probability"? Here Q.M. gives the following account. It takes over unquestioningly from the classical model the entire infaite roll call of imaginable variables or determining parts and proclaims each part to be directly measurable, indeerl measurable to arbitrary precision. so far as it alone is concerned. If through a well-chosen, constrained set of measurements one has gained that maximal knowledge of an object which is just possible according to A., then the mathematical apparatus of the new theory provicles means of assigning, for the same or for any later instant of time, a fully determined statistical distribution to equry variable, that is, an indication of the fraction of cases it will be found at this or that value, or within this or that small interval (which is also called probability.) The doctrine is that this is in fact the probability of encountering the relevant variable, if one measures it at the relevant time, at this or that value. By a single trial the correctness of this probability prodiction can be given at most an approximate test, namely in the case that it is comparatively sharp, i.e.. declares possible only a small range of values. To test it thoroughly one must repeat the entire trial *ab* ozo (i.e., including the orientational or preparatory measurements) very often and may use only those cases in which the preparatory measurements gave exactly the same results. For these cases. then, the statistics of a particular

variable, reckoned forward from the preparatory measurements, is to be confirmed by measurementthis is the doctrine.

One must guard against criticizing this doctrine because it is so difficult to express; this is a matter of language. But a different criticism surfaces. Scarcely a single physicist of the classical era would have dared to believe, in thinking about a model, that its determining parts are measurable on the natural object. Only much remoter consequences of the picture were actually

[84] h $= 1.041 \cdot 10^{-2 \cdot}$ergsec. Usually in the literature the 2π fold of this $\left(6.542 \cdot 10^{-27}\text{ergsec}\right)$ is designated as h and for our h an h with a cross-bar is written. [Transl. Note: In conformity with the now universal usage, $\hbar$ is used in the translation in piace of h.j]

open to experimental test. And all experience pointed toward one conclusion: long before the advancing experimental arts had bridged the broad chasm, the model would have substantially changed through gradual adaptation to new facts.-Now while the new theory calls the classical model incapable of specifying all details of the mutual interrclationship of the determining parts (for which its creators intended it), it nevertheless considers the model suitable for guiding us as to just which measurements can in principle be made on the relevant natural object. This would have seemed to those who thought up the picture a scandalous extension of their thought-pattern and an unscrupulous proscription against future development. Would it not be pre-established harmony of a peculiar sort if the classical-epoch researchers, those who, as we hear today, had no idea of what measuring truly is, had unwittingly gone on to give us as legacy a guidance scheme revealing just what is fundamentally measurable for instance about a hydrogen atom!?

I hope later to make clear that the reigning doctrine is born of distress. Meanwhile 1 continue to expound it.

24.16.3 3. Examples of Probability Predictions

All of the foregoing pertains to determining parts of a classical model, to positions and velocities of point masses, to energies, angular monemia. etc. The only unclassical feature is that only probabilities are predicted. l.et us have a closer look. The orthodox treatment is always that, by way of certain measurements performed now and by way of their resulting prediction of results to be expected of other measurements following thereafter either immediately or at some given time, one gains the best possible probability estimates permitted by nature. Now how does the matter really stand? In important and typical cases as follows.

If one measures the energy of a Planck oscillator, the probability of finding for it a value between E and E' cannot possibly be other than zero unless between E and E′ there lies at least one value from the series $3\pi h\nu, 5\pi h\nu, 7\pi h\nu, 9\pi h\nu, \ldots$. For any interval containing none of these values the probability is zero. In plain English: other measurement results are ex-

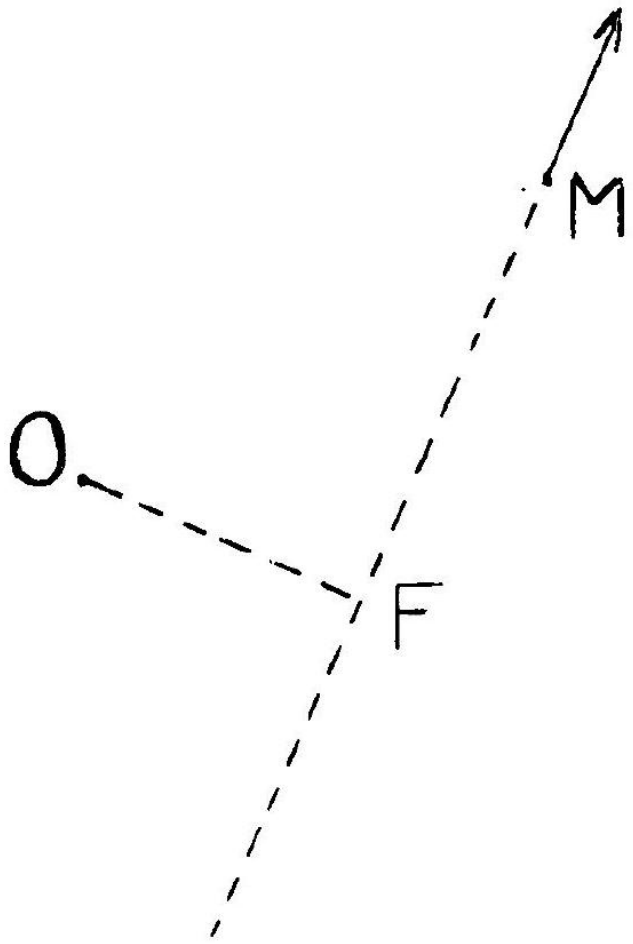


Fig. 1. Angular momentum. M is a material point, O a geometric reference point. The vector arrow represents the momentum (= mass times velocity) of M . Then the angular momontan is the product of the length of the arrow by the length OF.

cluded. The values are odd multiples of the constant of the model mhy

(Planck constant) 2π

$\nu =$ frequency of the oscillator.

Two points stand out. First. no account is taken of preceding measurements-these are quite unnecessary. Second, the statement certainly doesn't suffer an excessive lack of precision-quite to the contrary it is sharper than any actual measurement could ever be.

Another typical example is magnitude of angular momentum. In Fig. 1 let M be a moving point mass, with the vector representing, in magnitude and direction, its momentum (mass times velocity). O is any arbitrary fixed point in space, say the origin of coordinates; thus not a physically significant point, but rather a geometric reference point. As magnitude of the angular momentum of M about () classical mechanics designates the product of the length of the momentum vector by the length of the normal OF. In Q.M. the magnitude of angular momentum is governed much as the energy of the oscillator. Again the probability is zero for any interval not containing some value(s) from the following series
h $(2)^{\frac{1}{2}}, h(2\times 3)^{\frac{1}{2}}, h(3\times 4)^{\frac{1}{2}}, h(4\times 5)^{\frac{1}{2}}, \ldots;$
that is, only one of these values is allowed. Again
this is true without reference to preceding measurements. And one readily conceives how

important is this precise statement, much more important than knowing which of these values, or what probability for each of them, would actually pertain to a given case. Moreover it is also noteworthy here that there is no mention of the reference point: however it is chosen one will get a value from the series. This assertion seems unreasonable for the model, because the normal OF changes continuously as the point O is displaced. if the monentum vector remains unchanged. In this example we see how Q.M1. does indeed use the model to read off those quantities which one can measure and for which it makes sense to predict results, but finds the classical model inadequate for explicating relationships among these quantities. Now in both examples does one not get the feeling that the essential content of what is being said can only with some (lifficulty be forced into the Spanish boot of a prediction of probability of finding this or that measurement result for a variable of the classical model? Does one not get the impression that here one deals with funclamental properties of new classes of characteristics, that keep only the name in common with classical ones? Ind by no means do we speak here of exceptional cases, rather it is precisely the truly valuable statements of the new theory that have this character. There are indeed problems more nearly of the type for which the mode of expression is suitable. But they are by no means equally inportant. Moreover of no importance whatever are those that are naively set up as class exercises. "Given the position of the electron in the hydrogen atom at time $t = 0$, find the statistics of its position a a later time." No one cares about that.
The big iclea seems to be that all statements pertain to the intutive model. But the useful statements are scarcely intuitive to it, and its intuitive aspects are of little worth.

24.16.4 4. (an One Basc the Theory on Ideal Enswhles.'

The classcal model plays a Protean role in 0.M. Each of its determining parts can under certain circumstances become an object of meterest and achieve a certain reality. But never all of them together-now it is these, now those, and indeed always at most half of the complete set of variables allowed by a full picture of the momentary state. Neantime. how about the others? How they then no reality, perhaps (pardon the expression) a blurred reality: or are all of them always real and is it merely, according to Theorem A. of Sect. 2., that simultaneous knowledge of them is ruled out?

The second interpretation is especially appealing to those acquainted with the statistical vicwpoint that came up in the second half of the preceding century;
the more so. Considering that on the eve of the new century quantum theory was born from it, from a central problem in the statistical theory of heat (Max Planck's Theory of Hoat Radiation. December, 1899). The essence of this line of thought is precisely this. that one practically never knows all the determining parts of the system. but rather much fewer. To describe an actual body at a given moment one relies therefore not on one state of the model but on a socalled cibbs cnscmble. By this is meant an ideal. that is, merely imagined ensemble of states, that accurately reflects our limited knowledge of the actual body. The body is then considered to behave as though in a single state arbitrarily chosen from this casemble. This interpretation had the most extensive results. Its lighest triumphs were in those cases for which not all states appearing in the ensemble led to the same observable behavior. Thus the body's conduct is now this way, now that, just as foreseen (thermodynamic fluctuations). . It first thought one might well attempt likewise to refer back the always uncertain statements of ().MI. to an ideal ensemble of states, of which a quite specific one applies in any concrete instance–but one does not know which one.

That this won't work is shown by the one example of angular momentum, as one of many. Imagine in Fig. 1 the point M to be situated at various positions relative to () and fitted with various momentum vectors, and all these possibilities to be combined into an ideal ensemble.

Then one can indeed so choose these positions and vectors that in every case the product of vector length by length of normal OF yields one or the other of the acceptable valuesrelative to the particular point (). But for an arbitrary different point O', of course, unacceptable values occur. Thus appeal to the ensemble is no help at all. –Another example is the oscillator energy. Take the case that it has a sharply determined value, e.g., the lowest, 3π w. The separation of the two point masses (that constitute the ocillator) then appeas very unsharp. To be able to refer this statement to a statistical collective of states would require the distribution of separations to be sharply limited, at least toward large values. by that separation for which the potenfial chergy alone would equal or exceed the value $3\pi h$. But that's not the way it is-arbitrarily large separations occur. even though with markedly reduced probability. And this is no mere secondary calculation result. that might in some fashion be circumvented, without striking at the heart of the theory: along with many others, the quantum mechanical treatment of raclioactivity (Gamow) rests on this state of affairs.–One could go on indefinitely with more examples. One should note that there was no question of any time-dependent changes. It would be of no help to permit the model to vary quite "unclassicaliy," periaps to "jump." Already for the
single instant things go wrong. At no moment does there exist an ensemble of classical states of the model that squares with the totality of quantum mechanical statements of this moment. The same can also be said as follows: if I wish to ascribe to the model at each moment a definite (merely not exactly known to me) state. or (which is the same) to all determining parts definite (merely not exactly known to me) numerical values. then there is no supposition as to these numerical values to be imagined that would not conflict with some portion of quantum theoretical assertions.

That is not quite what one expects, on hearing that the pronomicements of the new theory are always uncertain compared to the classical ones.

24.16.5 5. Are the L'aridbles Really Blarra!'

The other alternative consisted of granting reality only to the momentarily sharp determining partsor in more general terms to each variable a sort of realization just corresponding to the quantum mechancal statistics of this variable at the relevant moment.

That it is in fact not impossible to express the degree and kind of blurring of all variables in one perfectly clear concept follows at once from the fact that ().Ml. as a matter of fact has and uses such an instrument, the so-called wave function or ψ-function, aliso calied system vector. Milch more is to be said about it further on. That it is an abstract, mintuitive mathematical construct is a scruple that almost always surfaces against new aids to thought and that carries no great message. At all events it is an imagined entity that inages the blurring of all variables at every moment junt as clearly and faithfully as the classical model does its sharp numerical values. Its equation of motion too, the law of its time variation, so long as the system is left undisturbed, lags not one iota, in clasity and tetermanacy, behimel the equations of motion of the classical model. So the latter could be straight-forwardly replaced by the ψ-function, so long as the blurring is confined to atomic scale, not open to direct control. In fact the function has provided quite intuitive and convenient ideas, for instance the "cloud of negative electricity" around the nucleus, etc. But serious misgivings arise if one notices that the uncertainty affects macroscopically tangible and visible things, for which the term "blurring" secons simply wrong. The state of a radioactive nucleus is presumably blurred in such degree and fashion that neither the instant of decay nor the direction. In which the emitted α-particle leaves the nucleus, is well-established. Inside the nucleus, blurring doesn't bother us. The emerging particle is described, if one wants to explain intuitively, as a spherical wave that continuously emanates in ail di-

rections from the nucleus and that impinges continuously on a surrounding luminescent screen over its full expanse. The screen however does not show a more or less constant uniform surface glow, but rather lights up at one instant at one spot-or, to honor the truth, it lights up now here, now there, for it is impossible to do the experiment with only a single radioactive atom. If in place of the luminescent screen one uses a spatially extended detector, perhaps a gas that is ionised by the α-particles, one finds the ion pairs arranged along rectilinear columns, [5] that project backwards on to the bit of radioactive matter from which the α-radiation comes (C.T.R. Wilson's cloud chamber tracks, made visible by drops of moisture condensed on the ions).
One can even set up quite ridiculous cases. A cat is penned up in a steel chamber, along with the following diabolical device (which must be secured against direct interference by the cat): in a Geiger counter there is a tiny bit of radioactive substance, so small, that perhaps in the course of one hour one of the atoms decays, but also, with equal probability, perhaps none; if it happens, the counter tube discharges and through a relay releases a hammer which shatters a small flask of hydrocyanic acid. If one has left this entire system to itself for an hour, one would say that the cat still lives if meanwhile no atom has decayed. The first atomic decay would have poisoned it. The ψ-function of the entire system would express this by having in it the living and the dead cat (pardon the expression) mixed or smeared out in equal parts.
It is typical of these cases that an indeterminacy originally restricted to the atomic domain becomes transformed into macroscopic indeterminacy, which can then be resolved by direct observation. That prevents us from so naively accepting as valid a "blurred model" for representing reality. In itself it would not embody anything unclear or contradictory. There is a difference between a shaky or outoffocus photograph and a shapolot of clouds and fog banks.

24.16.6 6. The Didherativ-unall-face of the Epistemanaical Vicupount

In the fourth section we saw that it is not possible moothly to take over models and to ascribe to the momentarily unknown or not exactly known variables, nometheless determinate values, that we simply don't know. In Sect. 5. we saw that the indeterminacy is not even an actual blurring, for there are always cases where an easily executed observation provides the missing knowledge. So what is left?

From this very hard dilemna the reigning doctrine rescues itself or us by having recourse to epistemology. We are told that no distinction is to be made between the state of a natural object and what I know about it, or perhaps better. what I can know about it if I go to some trouble. Actually-so they say-there is intrinsically only awareness, observation, measurement. If through them I have procured at a given moment the best knowledge of the state of the plysical object that is possibly attainable in accord with natural laws, then I can turn aside as meaningless any further questioning about the "actial state," inasmoch as I am convincerl that no further observation can extend my knowledge of itat least, not without an equivalent diminution in some other respect (namely by changing the state, see below).

Now this sheds some light on the origin of the proposition that I mentioned at the end of Sect. 2. as something very far-reaching: that all model quantities are measurable in principle. One can hardly get along without this article of belief if one sees himself constrained, in the interests of physical methodology. to call in as dictatorial help the above-mentioned philosophical principle, which no sensible person can fail to esteem as the supreme protector of all empiricism.

Reality resists imitation through a model. So one lets go of naive realism and leans directly on the indubitable proposition that actually (for the physi cist) after all is said and done there

[8] ∴ For illustration see Fig. Ξ or 6 on p. 375 of the 1927 volume of this journal: or Fig. 1, p. 7.34 of the preceding year's volume (1934), though these are proton tracks.

is only observation, measurement. Then all our physical thinking thenceforth has as sole basis and as sole object the results of measurements which can in principle be carried out. for we must now explicitly not relate our thinking any longer to any other kind of reality or to a model. . All numbers arring in our plysical calculations must be interpreded as measurement results. liut sime we didn't just now come into the work and start to build up our seduce from cotatel, but rather have in use a quite delimite scheme of calculation. from which in view of the great progress in ()... we would less than ever wan to be parted, we see oneduen fored to thate from the writing-table which measurements ate a parafic possible that 15. mut be poside in order an alphir adequated our reckeming sometem. This abow: a shaph value for cach simele variable of the musted meed for a whole hall set") and wa ear simple variable ment be meaamable ao arbatar exactues. We commot be satiolied with lon. for we have ins our natuely realistic imocence. Ile have modiang but our reckoning scheme to specify where liature draw the ignora-binus-line. i.e. what is a bey pussible knowledge of the object. And if we cond, a s do that, then indeed would one measurement reality become highly dependent on the diligence or datiness of the experi-
menter, how much trouble he takes to inform himself. We must go on to tell him how far he could go if only he were clever enough. Otherwise it would be seriously feared that just there, where we forbid further questions, there might well still be something worth knowing that we might ask about.

24.16.7 7. The ψ-function As Expectation-catalog

Continuing to expound the official teaching. let us turn to the already (Sect. 5) mentioned ψ-function. It is now the means for predicting probability of measurement results. In it is embodied the momen tarily-attained sum of theoretically based future expectation, somewhat as laid down in a catalog. It is the relation- and-determinacy-bridge between measurements and measurements, as in the classical theory the model and its state were. With this latter the ψ-function moreover has much in common. It is, in principle, determined by a finite number of suitably chosen measurements on the object, half as many as were required in the classical theory. Thus the catalog of expectations is initially compiled. From then on it changes with time, just as the state of the model of classical theory, in constrained and unique fashion ("causally")-the evolution of the ψ-function is governed by a partial differential equation (of first order in time and solved for $\partial\psi/\partial$t). This corresponds to the undisturbed motion of the model in classical theory. But this goes on unly unii one again carries out any measurement. For each measurement one is required to ascribe to the ψ-function (= the predic-tion-catalog) a characteristic, quite sudden change, which depends on the measurement result obtained, and so cannot be foreseen; from which alone it is already quite clear that this second kind of change of the ψ-function has nothing whatever in common with its orderly development between two measurements. The abrupt change by measurement ties in closely with matters discussed in Sect. 5. and will occupy us further at some length; it is the most interesting point of the entire theory. It is precisely the point that demands the break with naive realism. For this reason one can not put the ψ-function directly in place of the model or of the physical thing. And indeed not because one might never dare impute abrupt unforeseen changes to a physical thing or to a model, but because in the realism point of view observation is a natural process like any other and cannot per se bring about an interruption of the orderly flow of natural events.

24.16.8 8. Theory of Measurement, Part One

The rejection of realism has logical consequences. In general, a variable has no definite value before I measure it; then measuring it does not mean ascer-

taining the value that it has. But then what does it mean? There must still be some criterion as to whether a measurement is true or false, a method is good or bad, accurate, or inaccurate-whether it deserves the name of measurement process at all. Any old playing around with an indicating instrument in the vicinity of another body, whereby at any old time one then takes a reading, can hardly be called a measurement on this body. Now it is fairly clear; if reality does not determine the measured value, then at least the measured value must determine realityit must actually be present after the measurement in that sense which a'one will be recognized again. That is, the desired criterion can be merely this: repetition of the measurement must give the same result. By many repetitions I can prove the accuracy of the procedure and show that ' I am not just playing. It is agreeable that this program matches exactly the method of the experimenter, to whom likewise the "true value" is not known beforehand. We formulate the essential point as follows:

The systematically arranged interaction of two sys. toms (moasured objoct and measuring instrument) is called a measurement on the first system, if a di-rectly-sensible variable feature of the second (pointer position) is alcoays reproduced within certain error limits when the process is immediately repeated (on the same object, which in the meantime must not be cxposed to any additional influences).

This statement will require considerable added comment: it is by no means a faultless definition. Empirics is more complicated than mathematics and is not so easily captured in polished sentences.

Before the first measurement there might have been an arbitrary quantum-theory prediction for it. After it the prediction always runs: within error limits again the same result. The expectation-catalog (= ψ-function) is therefore changed by the measurement in respect to the variable being measured. If the measurement procedure is known from beforehand to be reliable, then the first measurement at once reduces the theoretical expectation within error limits on to the value found, regardless of whatever the prior expectation may have been. This is the typical abrupt change of the ψ-function discussed above. But the expectation-catalog changes in unforeseen manner not only for the measured variable itself, but also for others, in particular for its "canonical conjugate." If for instance one has a rather sharp prediction for the momentum of a particle and proceeds to measure its position more exactly than is compatible with Theorem A of Sec. 2., then the momentum prediction must change. The quantum mechanical reckoning scheme moreover takes care of this automatically; there is no ψ-function whatsoever that would contradict Theorem A when one deduces from it the combined expectations.

Since the expectation-catalog changes radically during measurement, the object is then no longer suited for testing, in their full extent, the statistical predictions made earlier; at the very least for the measured variable itself, since for it now the (nearly) same value would occur over and over again. That is the reason for the prescription already given in Sect. 2.: one can indeed test the probability predictions completely, but for this one must repeat the entire experiment *ab* ovo. One's prior treatment of the measured object (or one identical to it) must be exactly the same as that given the first time, in order that the same expectation-catalog (= ψ-function) should be valid as before the first measurement. Then one "repeats" it. (This repeating now means of course something quite other than earlier!) All this one nust do not twice but very often. Then the predicted statistics are established-that is the doctrine.

One should note the difference between the error limits and the error distribution of the measurement. on the one hand, and the theoretically predicted statistics, on the other hand. They have nothing to do with each other. They are established by the two quite different types of repetition just discussed.

Here there is opportunity to deepen somewhat the above-attempted delimitation of measuring. There are measuring instruments that remain fixed on the reading given by the measurement just made. Or the pointer could remain stuck because of a defect. One would then repeatedly

make exactly the same reading, and according to our instruction that would be a spectacularly accurate measurement. Moreover that would be true not merely for the object but also for the instrument itself! As a matter of fact there is still missing from our exposition an important point, but one which could not readily be stated earlier, namely what it is that truly makes the difference between object and instrument (that it is the latter on which the reading is made. is more or less superficial). We have just seen that the instrument under certain circumstances, as required, must be set back to its neutral initial condition before any control measurement is made. This is well known to the experimentalist. Theoretically the matter may best be expressed by prescribing that on principle the instrument should be subjected to the identical prior treatment before each measurement, so that for it each time the same expectation-catalog (= ψ-function) applies, as it is brought up to the object. For the object it is just the other way around, any interference being forbidden when a control measurement is to be made, a "repetition of the first kind" (that leads to crror statistics). That is the characteristic difference between object and instrument. It disappears for a "repetition of the second kind" (that serves for clecking the quantum predictions). Here
the difference between the two is actually rather insignificant.

From this we gather further that for a second measurement one may use another similarly built and similarly prepared instrument-it need not necessarily be the same one; this is in fact sometimes done, as a check on the first one. It may indeed happen that two quite differently built instruments are so related to each other that if one measures with them one after the other (repetition of the first kind!) their two indications are in one-to-one correlation with each other. They then measure on the object essentially the same variable-i.e., the same for suitable calibration of the scales.

24.16.9 9. The ψ-function As Description of State

The rejection of realism also imposes obligations. From the standpoint of the classical model the momentary statement content of the ψ-function is far from complete; it comprises only about 50 per cent of a complete description. From the new standpoint it must be complete for reasons already touched upon at the end of Sect. 6. It must be impossible to add on to it additional correct statements, without otherwise changing it ; else one would not have the right to call meaningless all questions extending beyond it.

Thence it follows that two different catalogs, that apply to the same system under different circumstances or at different times, may well partially overlap, but never so that the one is entirely contained within the other. For otherwise it would be susceptible to completion through additional correct statements. namely through those by which the other one exceeds it.-The mathematical structure of the theory autonatically satisfies this condition. There is no ψ-function that furnishes exactly the same statements as another and in addition several more.

Therefore if a sustem changes, whether by itself or because of measurements, there must always be statements missing from the new function that were contained in the earlier one. In the catalog not just new entries, but also deletions. must be made. Now knowledge can well be gained, but not lost. So the deletions mean that the previously correct statements have now become incorrect. I correct statement can become incorrect only if the object to which it applies changes. I consider it acceptable to express this reasoning sequence as follows:

Theorem 1: If different ψ-functions are under discussion the system is in different states.
If one speaks only of systems for which a ψ-function is in general available, then the inverse of this theorem runs:

Theorem 2: For the same ψ-function the system is in the same state.

This inverse does not follow from Theorem 1 but independently of it, directly from completeness or maximality. Whoever for the same expectation-catalog would yet claim a difference

is possible, would be admitting that it (the catalog) does not give information on all justifiable questions. - The language usage of almost all authors implies validity of the above two theorems. Of course, they set up a kind of new reality-in entirely legitimate fashion, I believe. Moreover they are not trivially tautological, not mere verbal interpretations of "state." Without presupposed maximality of the expectation-catalog, change of the ψ function could be brought about by mere collecting of new information.

We must face up to yet another objection to the derivation of Theorem 1. (One can argue that each individual statement or item of knowledge, under examination there, is after all a probability statement, to which the category of correct, or incorrect does not apply in any relation to an individual case, but rather in relation to a collective that comes into being from one's preparing the system a thousand times in identical fashion (in order then to allow the same measurement to follow; cf. Sect. 8.). That makes sense, but we must specify all members of this collective to be identically prepared. since to each the same ψ-function, the same statement-catalog applies and we dare not specify differences that are not expressed in the catalog (cf. the foundation of Theorem 2). Thus the collective is made up of identical individual cases. If a statement is wrong for it, then the individual case must have changed, or else the collective too would again be the same.

24.16.10 10. Theory of Measurement. Fart Two

Now it was previously stated (Sect. 7) and explained (Sect. 8) that any measurement suspends the law that otherwise governs continuous time-dependence of the ψ-finetion and brings about in it a quite different change, not governed by any law but rather dictated by the result of the measurement. But laws of nature differing from the usual ones cannot apply during a measurement, for objectively viewed it is a natural process like any other, and it cannot interrupt the orderly course of natural events. Since it does interrupt that of the ψ-function, the latter-as we said in Sect. 7-can not serve, like the classical model, as an experimentally verifiable representation of an objective reality. And yet in the last Section something like that has taken shape.

So, using catchwords for emphasis, I try again to contrast: 1.) The discontinuity of the expectationcatalog due to measurement is unavoidable, for if measurement is to retain any meaning at all then the measured zalue, from a good measurement, must obtain. 2.) The discontinuous change is certainly not
governed by the otherwise valid causal law, since it depends on the measured value, which is not predetermined. 3.) The change also definitely includes (because of "maximality") some loss of knowledge, but knowledge cannot be lost, and so the object must change - both along with the discontinuous changes and also, during these changes, in an unforeseen, different way.

How does this add up? Things are not at all simple. It is the most difficult and most interesting point of the theory. Obviously we must try to comprehend objectively the interaction between measured object and mcasuring instrument. Tu that end we must lay out a few very abstract considerations.

This is the point. Whenever one has a complete expectation-catalog-a maximum total knowledgea ψ-function–for two completely separated bodies, or, in better terms, for each of them singly, then one obviously has it also for the two bodies together, i.e., if one imagines that neither of them singly but rather the two of them together make up the object of interest, of our questions about the future. [6]

But the converse is not true. Maximal knowledge of a total system does not necessarily include total knowledge of all its parts, not even when these are fally separated from each other and at the moment are not influencing each other at all. Thus it may be that some part of what one knows may pertain to relations or stipulations between the two subsystems (we shall limit

ourselves to two), as follows: if a particular measurement on the first system yields this result, then for a particular measurement on the second the valid expectation statistics are such and such; but if the measurement in question on the first system should have that result, then some other expectation holds for that on the second; should a third result occur for the first, then still another expectation applies to the second; and so on, in the manner of a complete disjunction of all possible measurement results which the one specifically contemplated measurement on the first system can yield. In this way, any measurement process at all or, what amounts to the same, any variable at all of the second system can be tied to the not-yet-known value of any variable at all of the first, and of course vict versa also. If that is the case, if such conditional statements occur in the combined catalog, then it can not possibly be maximal in regard to the individual systems. For the content of two maximal individual catalogs would by itself suffice for a maximal combined catalog; the conditional statements could not be added on.

These conditioned predictions, moreover, are not something that has suddenly fallen in here from the blue. They are in every expectation-catalog. If one knows the ψ-function and makes a particular measurement and this has a particular result, then one again knows the ψ-function, voili tout. It's just that for the case under discussion, because the combined system is supposed to consist of two fully separated parts, the matter stands out as a bit strange. For thus it becomes meaningful to distinguish between measurements on the one and measurements on the other subsystem. This provides to each full title to a private maximal catalog; on the other hand it re mains possible that a portion of the attainable combined knowledge is. so to say, squandered on conditional statements, that operate between the subsystems. so that the private expectancies are left unfulfilled-even though the combined catalog is maximal, that is even though the ψ-function of the combined system is known.

Let us pause for a moment. This result in its abstractness actually says it all: Best possible knowlcdge of a whole does not necessarily include the same for its parts. Let us translate this into terms of Sect. 9: The whole is in a definite state, the parts taken individually are not.
"How so? Surely a system must be in some sort of state." "No. State is ψ-function, is maximal sum of knowledge. I didn't necessarily provide myself with this, I may have been lazy. Then the system is in no state."
"Fine, but then too the agnostic prohibition of questions is not yet in force and in our case I can tell myself: the subsystem is already in some state, I just don't know which."
"Wait. Unfortunately no. There is no 'I just don't know'. For as to the total system, maximal knowledge is at hand . . ."

The insufficiency of the ψ-function as model replacement resis solely on the fact that une duesn't always haz' it. If one does have it, then by all means let it serve as description of the state. But sometimes one does not have it, in cases where one might reasonably expect to. And in that case. one dare not postulate that it "is actually a particular one, one just doesn't know it": the above-chosen standpoint forbids this. "It" is namely a sum of knowledge; and knowledge, that no one knows, is none. -

We continue. That a portion of the knowledge should float in the form of disjunctive conditional statements between the two systems can certainly not happen if we bring up the two from opposite ends of the world and juxtapose them without interaction. For then indeed the two "know" nothing about each other. A measurement on one cannot possibly furnish any grasp of what is to be expected of the other, Any "entanglement of predictions" that takes place
can obviously only go back to the fact that the two bodies at some earlier time formed in a true sense one system, that is were interacting, and have left behind traces on each other. If two separated bodies, each by itself known maximally, enter a situation in which they influence each

[86] Obviously. We cannot fail to have, for instance, statements on the relation of the two to each other. For that would be, at least for one of the two, something in addition to its Ψ-function. And such there cannot be.

other, and separate again, then there occurs regularly that which I have just called cntanglement of our knowledge of the two bodies. The combined expectation-catalog consists initially of a logical sum of the individual catalogs; during the process it develops causally in accord with known law (there is no question whatever of measurement here) The knowledge remains maximal. but at its end, if the two bodies have again separated, it is not again split into a logical sum of knowledges about the individual bodies. What still remains of that may have become less than maximal, even very strongly so.–()ne notes the great difference over against the classical model theory, where of coursc from known initial states and with known interaction the individual end states would be exactly known.

The measuring process described in Sect. δ now fits neatly into this general scheme, if we apply it to the combined system, measured object + measuring instrument. As we thus construct an objective picture of this process, like that of any other, we dare hope to clear up), if not altogether to avoid, the singular jump of the ψ-function. So now the one body is the measured object, the other the instrument. To suppress any interference from outside we arrange for the instrument by means of built-in clockwork to creep up automatically to the object and in like manner creep away again. The reading itself we postpone, as our immediate purpose is to investigate whatever may be happening "objectively"; but for later use we let the result be recorded automatically in the instrument, as indeed is often done these days.

Now how do things stand, after automatically completed measurement? We possess, afterwards same as before, a maximal expectation-catalog for the total system. The recorded measurement result is of course not included therein. As to the instrument the catalog is far from complete, telling us nothing at all about where the recording pen left its trace. (Remember that poisoned cat!) What this anounts to is that our knowledge has evaporated into conditional statements: if the mark is at line 1 , then things are thus and so for the measured object, if it is at line 2. then such and such, if at 3 , then a third, etc. Now has the ψ-function of the measured object made a leap? Has it developed further in accord with natural law (in accord with the partial differential equation)? No to both questions. It is no more. It has become snarled up, in accord with the causal law for the combined ψ-function, with that of the measuring instrument. The expectalion-catalog of the object has spiit into a condilonal disjunction of cripctation
catalogs-like a Baedeker that one has taken apart in the proper manner. Along with each section there is given also the probability that it proves correct-transcribed from the original expectation-catalog of the object. But which one proves right-which section of the Baedeker should guide the ongoing journey-that can be determined only by actual inspection of the record.

And what if we don't look? Let's say it was photographically recorded and by bad luck light reaches the film before it is developed. Or we inadvertently put in black paper instead of film. Then indeed have we not only not learned anything new from the miscarried measurement, but we have suffered loss of knowledge. This is not surprising. It is only natural that outside interference will almost always spoil the knowledge that one has of a system. The interference, if it is to allow the knowledge to be gained back afterwards, must be circumspect indeed.

What have we won by this analysis? First, the insight into the disjunctive splitting of the expectationcatalog, which still takes place quite continuously and is brought about through embedment in a combined catalog for instrument and object. From this amalgamation the object can again be separated out only by the living subject actually taking cognizance of the result of the measurement. Some time or other this must happen if that which has gone on is actually to be called a measurement-however dear to our hearts it was to prepare the process throughout as objectively as possible. And that is the second insight we have won: not until this inspection, which determines the disjunction, does anything discontinuous, or leaping, take place. One is inclined to call this a mental action, for the object is already out of touch, is no

longer physically affected: what befalls it is already past. But it would not be quite right to say that the ψ-function of the object which changer otherwise according to a partial differential equation, independent of the observer should now change leapfashion because of a mental act. For it had disappeared, it wa no more. Whatever in not. no more can it change. It is iorre anew. is reconstiated. is separated out itom the entangles howledge that one has, through an act of perceptial which as a matter of fact is not a phan acal effect on a tir manure, whect. From the forn. :- wheri the :-lume . was last known, to the new an which it repoed, row an continuous road - 10 an indeed inrough ambialation. Contrasting the to, forms. the thing looks like a leap. In truth something of importaro harnens in between, namely the influence of the tw, hodies on each other, durne, which the object possessed no private expectation-catalog nor had any claim thereto. because it was med independent.

24.16.11 11. Resolution of the "entanglement." Result Depondent on the Experimenter's Intention

We return to the general case of "entanglement," without having specificially in view the special case, just considered, of a measurement process. Suppose the expectation-catalogs of two bodies A and B have become entangled through transient interaction. Now let the bodies be again separated. Then I can take one of them, say B, and by successive measurements bring my knowledge of it, which had become less than maximal, back up to maximal. I maintain: just as soon as I succeed in this, and not before, then first, the entanglement is immediately resolved and, second, I will also have acquired maximal knowledge of A through the measurements on B , making use of the conditional relations that were in effect.

For in the first place the knowledge of the total system remains always maximal, being in no way damaged by good and exact measurements. In the second place: conditional statements of the form "if for A. ., then for B. ." can no longer exist, as soon as we have reached a maximal catalog on B . For it is not conditional and to it nothing at all can be added on relevant to B . Thirdly: conditional statements in the inverse sense (if for B. . , then for A. .) can be transformed into statements about Λ alone, because all probabilities for B are already known unconditionally. The entanglement is thus completely put aside, and since the knowledge of the total system has remained maximal, it can only mean that along with the maximal catalog for B came the same thing for A .

And it cannot happen the other way around, that A becomes maximally known indirectly, through measurements on B , before B is. For then all conclusions work in the reversed direction-that is, B is too. The systems become simultancously maximally known, as asserted. Incidentally, this would also be true if one did not limit the measurement to just one of the two systems. But the interesting point is precisely this, that one can limit it to one of the two: that thereby one reaches his gual.

Which measurements on B and in what sequence they are undertaken, is left entirely to the arbitrary choice of the experimenter. He need not pick out specific arrables, in order to be able to use the conditional statements. He is fire io formulate a plan that would lead him to maximal knowledge of 1 , even if he should know nothing at all about B. And it can do no harm if he carries thrometh this plan to the end If he asks himself after each measurement whether he has perhaps already reached his goal, he does so only to spare himself from further. superfluous labor.

What sort of A-catalog comes forth in this indirect way depends obviously on the measured values that are found in P (beiore the entanglement is entirely resolved not on more, on any later ones. in case the
measuring goes on superfluously). Suppose now that in this way I derived an A-catalog in a particular case. Then I can look back and consider whether I might perhaps have found a

different one if I had put into action a different measuring plan for H . But since after all I neither have actually touched the system A, nor in the imagined other case would have touched it, the statements of the other catalog. whatever it might be, must all also be correct. They must therefore be entirely contained within the first, vince the frot is maximal. But so is the second. So it must be identical with the first.

Strangely enough, the mathematical structure of the theory by no means satisfies this requirement automatically. Even worse. examples can be set up where the requirement is necessarily violated. It is true that in any experiment one can actually carry out only one group of measurements (always on B), for once that has happened the entanglement is resolved and one learns nothing more about A from further measurements on B. But there are cases of entanglement in which two definite programs are specifiable. of which each 1) must lead to resolution of the entanglement, and 2) must lead to an A-catalog to which the other can not possibly lead-whatsoever measured values may turn up in one case or the other. It is simply like this, that the two series of A-catalogs, that can possibly arise from the one or the other of the programs, are sharply separated and have in common not a singie term.

These are especially pointed cases, in which the conclusion lies so clearly exposed. In general one must reflect more carefully. If two programs of measurement on B are proposed, along with the two series of A-catalogs to which they can lead, then it is by no means sufficient that the two series have one or more terms in common in order for one to be able to say: well now, surely one of these will always turn up-and so to set forth the requirements as "presumably fulfilled." That's not enough. For indeced one know's the probability of every measurement on B. considered as measurement on the total system, and under many ab-ovo-repetitions each one must occur with the frequency assigned to it. Therefore the two series of A-catalogs would have to agree, nember by member, and furthermore the probabilities in each series would have to be the same. And that not merely for these two programs but also for each of the infinitely many that one might think up. But this is utterly out of the question. The requirement that the A-catalog that one gets should always be the same, regardless of what measurements on B bring it into being, this requirement is plainly and simply never fulfilled.

Now we wish to ciscuss a simple "pointed" example.

24.16.12 12. An Example

For simplicity, we consider two systems with just one degree of freedom. That is. each of them shall be specified through a single coordinate q and its canomically conjugate momentum p. The classical picture would be a point mass that could move only along a straight line. like the spheres of those playthings on which small children learn to calculate. p is the product of mass by velocity. For the second system we denote the two determining parts by capital Q and P. As to whether the two are "threaded on the same wire" we shall not be at all concerned, in our abstract consideration. But even if they are, it may in that case be convenient not to reckon q and Q from the same reference point. The equation $y = Q$ thus does not necessarily mean coincidence. The two systems may in pite of this be fully separated.

In the cited paper it is shown that between these two systems an entanglement can arise. which at a particular moment, to which everything following is referred, can be compactly shown in the two equations : $\mathrm{q} = \mathrm{Q}$ and $\mathrm{p} = -\mathrm{P}$. That means: I know. if a measurcment of if on the system yields a certain value. that a Q-measurement performed immediately thereafter on the second will give the same value, and vice versa: and I know, if a p-measurement on the first system vicld a certain value, that a P -measurement performed immediately thereafter will give the opposite value, and vice versa.

A single measurement of q or p or Q or P resolves the entanglement and makes both systems maximally known. A second measurement on the same system modifies only the statements

about it, but teaches nothing more about the other. So one cannot check both equations in a single experiment. But one can repeat the experiment ab oro a thousand times; each time set up the same entanglement: according to whim check one or the other of the equations: and find confirmed that one which one is nomentarily pleased to check. We assume that ail this has been clone.

If for the thousand-and-first experiment one is then seized by the desire to give up further checking and instead measure g on the first system and P on the second, and one obtains

$$q = 4; \quad P = 7;$$

can one then rloubt that

$$a = 4 : p = -7$$

would have heen a correct prediction for the first system, or

$$Q = 4. \quad P = 7$$

a correct prediction for the second? Quantum predictions are indeed not subject to test as to their full content, ever, in a single experiment; yet they are correct, in that whoever possessed them suffered no disillusion, whichever half he decided to check.

There's no doubt about it. Every measurement is for its system the first. Measurements on separated systems cannot directly influence each other-that would be magic. Neither can it be by chance, if from a thousand experiments it is established that virginal measurements agree.

The prediction-catalog $q = 4, p = -7$ would of course be hypermaximal

24.16.13 13. Continuation of the Example: All Possible Mcasurcments Are Entangled Uncquiwocally

Now a prediction of this extent is thus utterly impossible according to the teaching of Q.M., which we here follow out to its last consequences. Many of my friends remain reassured in this and declare: what answer a system would have given to the experimenter if . . ., -has nothing to do with an actual measurement and so, from our epistemological standpoint, does not concern us.

But let us once more make the matter very clear. Let us focus attention on the system labeled with small letters p, q and call it for brevity the "small" one. Then things stand as follows. I can direct one of two questions to the small system, either that about q or that about p Before doing so I can, if I choose, procure the answer to one of these questions by a measurement on the fully separated other system (which we shall regard as auxiliary apparatus), or I may intend to take care of this afterwards. My small system, like a schoolboy under examination, cannot possibly know whether I have done this or for which questions, of whether dud for which I intend to do it later. From arbitrarily many pretrials I know that the pupil will correctly answer the first question that I put to him. From that it follows that in every case he know's the answer to both questions. That the answering of the first question, that it pleases me to put to him. so tires or confuses the pupil that his further answers are worthless, changes nothing at all of this conclusion. No school principal would judge otherwise, if this situation repeated itself with thousands of pupils of similar provenance, however much

---

8

- A. Einstein, B. Podelsky, and N. Rosen, Phys. Rev. 47 : 777 (1935). The appearance of this work motivated the pucscut-shall I say lecture or general confession?

he might wonder zhat makes all the scholars so dimwitted or obstinate after the answering of the first question. He would not come to think that his, the teacher's. consulting a textbook first suggests to the pupil the correct answer, or even, in the cases when the teacher chooses to consult it only after ensuing answers by the pupil, that the pupil's answer has changed the text of the notebook in the pupil's favor.

Thus my small system holds a quite definite answer to the q-question and to the p-question in readiness
for the case that one or the other is the first to be put directly to it. Of this preparedness not an iota can be changed if I should perhaps measure the Q on the auxiliary system (in the analogy: if the teacher looks up one of the questions in his notebook and thereby indeed ruins with an inkblot the page where the other answer stands). The quantum mechanician maintains that after a Q-measurement on the auxiliary system my small system has a ψ-function in which " q is fully sharp, but p fully indeterminate." And yet, as already mentioned, not an iota is changed of the fact that my small system also has ready an answer to the p-question, and indeed the same one as before.

But the situation is even worse yet. Not only to the q-question and to the p-question does my clever pupil have a definite answer ready, but rather also to a thousand others, and indeed without my having the least insight into the memory technique by which he is able to do it. p and q are not the only variables that I can measure. Any combination of them whatsoever, for example

$$p^2 + q^2$$

also corresponds to a fully definite measurement according to the formulation of Q.M. Now it may be shown" that also for this the answer can be obtained by a measurement on the auxiliary system, namely by measurement of $\mathrm{P}^2 + \mathrm{Q}^2$, and indeed the answers are just the same. By general rules of Q.M. this sum of squares can only take on a value from the series
h, 3h, 5h, 7h, ...

The answer that my small system has ready for the $(p^2 + q^2)$-question (in case this should be the first it must face) nust be a number from this series.-It is very much the same with measurement of

$$\mathrm{p}^2 + \mathrm{a}^2\mathrm{q}^2$$

where a is an arbitrary positive constant. In this case the answer must be, according to Q.M., a number from the following series
ah. 3ah, 5ah, 7ah, ...

For each numerical value of a one gets a different question, and to each my small system holds ready an answer from the series (formed with the a-value in question).

Most astonishing is this: these answers cannot possibly be related to each other in the way given by the formulas! For let q' be the answer held ready for the q-question, and p' that for the p-question, then the relation

$$\left(p'^2 + a^2 q'^2\right)/(ah) = \text{ an odd integer}$$

cannot possibly hold for given numerical values q ' and p' and for any position number a. This is by no means an operation with imagined numbers, that one can not really ascertain. One can in fact get two of the numbers, e.g.. q' and p', the one by clirect. the other by indirect measurement. And then one can (pardon the expression) convince himself that the above expression, formed with the numbers q' and p' and an arbitrary a, is not an odd integer.

[88] E. Schrödinger, Proc. Cambridge Phil. Soc. (in press).

The lack of insight into the relationships annong the various answers held in readiness (into the "memory technique" of the pupil) is a total one, a gap not to be filled perhapt hy a new kind of algebra of (). MI. The lack is all the stranger, sunce on the other hand one can show : the entanglement is already uniquely determined by the requirements $q = Q$ and $p = -P$. If we know that the coordinates are equal and the momenta equal but upposite, then there follows by quantum mechanics a fully determined one-to-one arrangenent of all possible measurements on both systems. For every measurement on the "small" one the numerical result can be procured by a suitably arranged measurement on the "large" one, and onch measurement on the large stipulates the result that a particular measurement on the small would give or has given. (Of course in the same sense as always heretofore: only the virgun measurement on each system counts.) As soon as we have brought the two systems into the situation where they (briefly put) coincide in coordinate dial momentum, then they (briefly put) concide also in regard to all other variables.

But as to how the numerical values of all these variables of one system relate to each other we know nothing at all, even though for each the system must have a quite specific one in readiness. for if we wish we can learn it from the auxiliary system and then find it always confirmed by direct measurement.

Should one now think that because we are so ignorant about the relations annong the variablevalues held ready in one system, that nonc exists. that far-ranging arbitrary combination can occur? That would mean that such a system of "one degree of freedon" would need not merely talo numbers for adequately describing it, as in classical mechanics, but rather many more, perhaps infinitely many. It is then nevertheless strange that two systems always agree in all variables if they agrce in two. Therefore one would have to make the second assumption, that this is due to our awkwardness; would have to think that as a practical matter we are not competent to bring two systems into a situation such that they coincide in reference to two variables, without nolens volens bringing about coincidence also for all other variables, even though that would not in itself be necessary. One would have to make these two assumptions in order not to perceive as a great
dilemma the complete lack of insight into the interrelationship of variable-values within one system.

24.16.14 14. Imerdependente of the Emanylancht. Consideration of the Streial Role of Tame

It is perfaps not superfluous to recall that everything said in secion, 12 and 13 pertains to a single instant of time. The entanglement is not constant in time. It does continue to be ane-to-one entanglement of all a ariables. but the arrangement changes. That means the following. At a later time t one can very well again learn the values of q or of p that then ulatin. W a measurement on the auxiliary systen, but the measuraments. that one must undertake thereform the anxiliary system, are different. Which ones they whomed be one can eashy see in simple cases. It now of cource becomes a question of the forces at work withmed ead of the two systems. Let us assume that no forcen are working. For simplicity we will set the mass of each to be the same and call it m. Then in the classical model the momenta p and I^2 would remain comtant since they are still the masses multiplied by the velocities: and the coordinates at time 6 , which we shall distinguish by giveng them subscripts t, (d^+. $\left(\underset{\sim 1}{D}\right)$, would be calculated from the mitial one which henceforth we designate q, Q, thus:

$$\varphi_1 = r_1 + (1)\mathrm{m})\,\mathrm{t}$$
$$Q_1 = -(1) + (1,\ \mathrm{m})\mathrm{t}$$

Let us first talk about the mall system. The most natural way of describing it classically at time t is in terms of coordinate and monentum at this time, i.e., in terms of at and p. But one may do it differently. In place of qt one could specify q. It too is a "determining part at time t," and indeed at every time t, and in fact one that dues not change with time. This is similar to the way in which I can specify a certain determining part of my own person. namely my age, either through the mumber 48 , which changes with time and in the system corresponds to specifying qt . or through the number 1887 , which is usual in documents and corresponds to specifying of. Now according to the foregong:

$$q_1 = q_1 - (p_1 m)\, t$$

Similarly for the second system. So we take as determining parts
for the first system $q_1 - (p_2/m)$ t and p.
for the second system $Q_t - (P; m)t$ and P.
The advantage is that among these the same entanglement goes on indefinitely:

$$\mathrm{q_t - (p/m)t = Q_t - (P/m)t}$$
$$\mathrm{p = -P}$$

or solved:

$$\mathrm{q_t = Q_t - (2t/m)P; \quad p = -P.}$$

So that what changes with time is just this: the coordinate of the "small" system is not ascertained simply by a coordinate measurement on the auxiliary system, but rather by a measurement of the aggregate

$$Q_{\mathrm{t}} - (2\mathrm{t}; \mathrm{m})\mathrm{P}.$$

Here however, one must not get the idea that maybe he measures Q_{t} and P, because that just won't go. Rather one must suppose, as one always must suppose in Q.M., that there is a difect measurement procedure for this aggregate. Except for this change, out withing that was said in Sections 12 and 13 applies at any point of time; in particular there exists at all times the one-to-one entanglement of all variables together with its evil consequences.

It is just this way too. if within each system a force works, except that then φ_t and p) are entangled with variables that are more complicated combinations of Q_t and P.

I have briefiy explained this in order that we may consider the following. That the entanglement should change with time makes us after all a bit thoughtful. Must perhaps all measurements, that were under discussion, be completed in very short time. actually instantancously. in zero time, in order that the unwelcome consequences be vindicated? Can the ghost be banished by reference to the fact that measurements take time? No. For each single experiment one needs just one measurement on each system; only the virginal one matters, further one apart from this would be without effect. How long the meanurement lasts need not therefore concern a. -ince we have no second one following on. One must merely he able to so arrange the lwo virgin measurements that they yield variable-values for the same definite point of time, known to us in advance-known in advance, because after all we must direct the measurements at a pair of variables that are entageled at just this point of time.
"Perhaps it is not possible on to direct the measurements?"
"Perhaps. I even presume so. Mercly: today's Q.M. must require this. For it is now so set up that its predictions are always made for a point of time. Since they are supposed to relate to measurement results, they would be entirely without content if the relevant variables were not measurable for a definite point of time, whether the measurement itself lasts a long or a short while."

When we learn the result is of course quite immaterial. Theoretically that has as little weight as for instance the fact that one needs several months to integrate the differential equations of the weather for the
next three days.-The drastic analogy with the pupil examination misses the mark in a few points of the law's letter, but it fits the spirit of the law. The expression "the system knows" will perhaps no longer carry the meaning that the answer comes forth from an instantaneous situation; it may perhaps derive from a succession of situations, that occupies a finite length of time. But even if it be so, it need not concern us so long as the system somehow brings forth the answer from within itself, with no other help than that we tell it (through the experimental arrangement) which question we would like to have answered ; and so long as the answer itself is uniquely tied to a moment of time: which for better or for worse must be presumed for every measurement to which contemporary Q.M. speaks, for otherwise the quantum mechanical predictions would have no content.

In our discussion, however, we have stumbled across a possibility. If the formulation could be so carried out that the quantum mechanical predictions did not or did not always pertain to a quite sharply defined point of time, then one would also be freed from requiring this of the measurement results. Thereby, since the entangled variables change with time, setting up the antinomical assertion, would become much more difficult.

That prediction for sharply-defined time is a blunder, is probable also on other grounds. The numerical value of time is like any other the result of obervation. Can one make exception just for measurement with a clock? Must it not like any other pertain to a variable that in general has no sharp value and in any case cannot have it simultaneously with any other variable? If one predicts the value of another for a particular point of time, must one not fear that both can never be sharply known together? Within contemporary Q.M. one can hardly deal with this apprehension. For time is always considered a priori as known precisely. although one would have to admit that every look-at-the-clock clisturbs the clock's motion in uncontrollable fashion.

Permit me to repeat that we do not possess a Q.M. whose statements should not be valiel for sharply fixed points of time. It seems to me that this lack manifests itself directly in the former antinomies. Which is not to say that it is the only lack which manifests itself in them.

24.16.15 15. Natural Laze or Calculating Disite?

That "sharp time" is an anomaly in Q.M. and that besides, more or less independent of that, the special treatment of time forms a serious hindrance to adapting Q.M. to the relativity principle, is something that in recent years I have brought up again and again, unfortunately without being able to make the shadow
of a useful counterproposal. [9] In an overview of the entire contemporary situation, such as I have tried to sketch here, there comes up, in addition, a quite different kind of remark in relation to the so ardently sought, but not yet actually attained, "relativisation" of Q.M.

The remarkable theory of measurement, the appar ent jumping around of the ψ-function, and finally the "antinomies of entanglement," all derive from the simple manner in which the calculation methods of quantum mechamics allow two separated systems conceptually to be combined together into a single one; fur which the methods seem phanly predestined. When two systems interact, their ψ-functions, as we have seen, do not come into interaction but rather they immediately cease to exist and a single one, for the combined system, takes their place. It consists, to mention this briefly, at first simply of the product of the two individual functions; which, since the one function depends on quite different variables from the other, is a function of all these variables, or "acts in a space of much higher dimension number" than the individual functions. As soon as the systems begin to influence each other, the combined

function ceases to be a product and moreover does not again divide up, after they have again become separated, into factors that can be assigned individually to the systems. Thus one disposes provisionally (until the entanglement is resolved by an actual observation) of only a common description of the two in that space of higher dimension. This is the reason that knowledge of the individual systems can decline to the scantiest. even to zero, while that of the combined system remains contimually maximal. Best possible knowledge of a whole does not include best possible knowledge of its partsand that is what keeps coming back to haunt us.

Whoever reflects on this must after all be left fairly thoughtful by the following fact. The conceptual joining of two or more systems into onc encounters great difficulty as soon as one attempts to introduce the principle of special relativity into Q.MI. Already seven years ago P.A.MI. Dirac found a startlingly simple and elegant relativistic solution to the problem of a single electron. [1"] A series of experimental confirmations, marked by the key terms electron spin, positive electron, and pair creation, can leave no doubt as to the basic correctness of the solution. But in the first place it does nevertheless very strongly transcend the conceptual plan of Q.M. (that which I have attempted to picture here). [1t] and in the

second place one runs into stubborn resistance as soon as one seeks to go forward, according to the prototype of non-relativistic theory, from the Dirac solution to the problem of several electrons. (This shows at once that the solution lies outside the general plan, in which, as mentioned, the combining together of subsystems is extremely simple.) I do not presume to pass judgment on the attempts which have been made in this direction. [12] That they have reached their goal, I must doubt first of all because the authors make no such claim.

Matters tand much the same with another system, the electromagnetic field. Its laws are "relativity theory personificd," a non-relativistic treatment being in general impossible. Yet it was this field, which in terms of the classical model of heat radiation provided the first hurdle for quantum theory that was the first system to be "prantized." That this could be successfully done with simple means comes about because here one has things a bit easier. in that the photons, the "atoms of light," do not in general interact directly with each other. [13] but only via the charged particles. Today we do not as yet have a truly mexceptionable quantum theory of the electromagnetic field. [14] One can go a long way with building up out of subsystems according to the pattern of the non-relativistic theory (Dirac's theory of light [15]), yet without quite reaching the goal.

The simple procedure provided for this by the nonrelativistic theory is perhaps after all only a convenient calculational trick, but one that today, as we have seen. has attained influence of unprecedented scope over our basic attitude toward nature.

My warmest thanks to Imperial Chemical Indus dies, Iondon, for the leisure to write this article.

1st ed. p. 239; 2nd ed. p. 252. Oxford: Clarendon Press. 1930 or 1035.

12. Herenith a few of the more important references: *G*. Brot, Phys. Kor 34 : p. 553 (1929) and 39: p. 610 (1932); C. Moller. 2. Physis 70 : p. 786 (1931): P. A. M. Dirac, Proc. Roy Soc. Lond. A136: 1. 453 (1932) and Proc. Camhridae Phal Sac. 30: p 150 (1934): R. Peierls. Proc. Roy. Soc. Lond. A146: p. 420 (1934): W. Heisenberg, Z. Physik. 90 : p. 209 (1934).

1: But this hodds, probably, ouly approximately. See M. Boren and L. Fofeld, Proc. Roy. Soc. Lond. A144: p. 425 and A147: p. 522 (1934) : A150: p. 141 (1935). This is the most recent attempt at a fuantum electrodynamics.

14 Here again the most important works, partially assignable according to their content, alow to the penultimate citation: P. Jordan and W. Pauli, Z. Physik 47 ; p. 151 (1928); W.

[89] Berl. Ber. 16 Apr. 1931; Annales de l'Institut Henri Poincarc, p. 269 (Paris, 1931); Cursos de la Universidad Internacional de V'crano en Santander. 1: p. 60 (Madrid, Signo, 1935).

[10] Proc. Roy. Soc. Lond. A117 : p. 610 (1928).

[11] P. A. M. Dirac, The principles of quantum mechanics,

Heisenberg and W. Pauli, Z. Physik 56: p. 1 (1929); 59 : p. 168 (1930): P. A. M. Dirac, V. A. Fock, and B. Podolsky, Physik. Z. Sonojetuman 6: p. 468 (1932); N. Bohr and I. Rosenfeld, Danskc. I'idens. Sclsk. (math.-phys.) 12: p. 8 (1933).
[1] ' An excellent reference: E. Fermi, Rer. Mod. Phys. 4 : p. 87 (1932).

24.17 I. 12 Remarks on the Mind-body Question by Wigner

24.17.1 Introductory Comments

F. Dyson, in a very thoughtful article, [1] points to the everbroadening scope of scientific inquiry. Whether or not the relation of mind to body will enter the realm of scientific inquiry in the near future-and the present writer is prepared io admit that this is an open question-it seems worthwhile to summarize the views to which a dispassionate contemplation of the most obvious facts leads. The present writer has no other qualification to offer his views than has any other physicist and he believes that most of his colleagues would present similar opinions on the subject, if pressed.

Until not many years ago, the "existence" of a mind or soul would have been passionately denied by most physical scientists. The brilliant successes of mechanistic and, more generally, macroscopic physics and of chemistry overshadowed the obvious fact that thoughts, desires, and emotions are not made of matter, and it was nearly universally accepted among physical scientists that there is nothing besides matter. The epitome of this belief was the conviction that, if we knew the positions and velocities of all atoms at one instant of time, we could compute the fate of the universe for all future. Even today, there are adherents to this

[1] F. J. Dyson, Scientific American, 199, 74 (1958). Several cases are related in this article in which regions of inquiry, which were long considered to be outside the province of science, were drawn into this province and, in fact, became focuscs of attention. The best-known example is the interior of the atom, which was considered to be a metaphysical subject before Rutherford's proposal of his nuclear model, in 1911.

Originally published in The Scientist Speculates, I. J. Good, ed., pp. 284-302, Heinemann, London (1961); Basic Books, New York (1962). Reprinted in E. Wigner (1967), Symmetries and Reflections, Indiana University Press, Bloomington, pp. 171-84 from which book this paper is reproduced here.

view [2] though fewer among the physicists than - ironically enough among biochemists.

There are several reasons for the reiurn, on the part of most physical scientists, to the spirit of Descartes's "Cogito ergo sum," which recognizes the thought, that is, the mind, as primary. First, the brilliant successes of mechanics not only faded into the past; they were also recognised as partial successes, relating to a narrow range of phenomena, all in the macroscopic domain. When the province of physical theory was extended to encompass microscopic phenomena, through the creation of quantum mechanics, the concept of consciousness came to the fore again: it was not possible to formulate the laws of quantum mechanics in a fully consistent way without reference to the consciousness [3] All that quantum mechanics purports to provide are probability connections between subsequent impressions (also called "apperceptions") of the consciousness, and even though the dividing line between the observer, whose consciousness is being affected, and the obscrved physical object can be shifted towards the one or the other to a considerable degree, [4] it cannot be eliminated. It may be premature to believe that the present philosophy of quantum mechanics will remain a permanent feature of future physical theories; it will remain remaikable, in whatever way our future concepts may develon, that the very study of the external world led to the conclusion that the content of the consciousness is an ultimate reality.

It is perhaps important to point out at this juncture that the question conccrning the exis-

tence of almost anything (even the whole external world) is not a very relevant question. All of us recognize at once how meaningless the query concerning the existence of the electric field in vacuum would be. All that is relevant is that the concept of the electric

[2] The book most commonly blamed for this view is E. F. Haeckel's Weltrtsel 1899). However, the views propounded in this book are less extreme (though more confused) than those of the usual materialistic philosophy.

[2] W. Heisenberg expressed this most poignantly [Daedalus, 87, 99 (1958)]: "The laws of nature which we formulate mathematically in quantum theory deal no longer, with the particles themselves but with our knowledge of the elementary particles." And later: "The conception of objective reality . . . evaporated into the . . . mathematics that represents no longer the bchavior of elementary particles but rather our knowledge of this behavior." The "our" in this sentence refers to the observer who plays a singular role in the epistemologs always referred to the observer.

rution der Quantenmechanik (Berlin: Julius Springer, 1932), Chapter VI; English translation (Princeton, N.J.: Princeton University Press, 1955).

field is useful for communicating our ideas and for our own thinking. The statement that it "exists" means only that: (a) it can be measured, hence uniquely defined, and (b) that its knowledge is useful for understanding past phenomena and in helping to foresee further events. It can be made part of the Weltbild. This observation may well be kept in mind during the ensuing discussion of the quantum mechanical description of the external world.

24.17.2 The Language of Quantum Mechanics

The present and the next sections try to describe the concepts in terms of which quantum mechanics teaches us to store and communicate information, to describe the regularities found in nature. These concepts may be called the language of quantum mechanics. We shall not be interested in the regularities themselves, that is, the contents of the book of quantum mechanics, only in the language. It may be that the following description of the language will prove too brief and too abstract for those who are unfamiliar with the subject, and too tedious for those who are familiar with it. [5] It should, nevertheless, be helpful. However, the knowledge of the present and of the succeeding section is not necessary for following the later ones, except for parts of the section on the Simplest Answer to the Mind-Body Question.

Given any object, all the possible knowledge concerning that object can be given as its wave function. This is a mathematical concept the exact nature of which need not concern us here-it is composed of a (countable) infinity of numbers. If one knows these numbers, one can foresee the behavior of the object as far as it can be foreseen. More precisely, the wave function permits one to foretell with what probabilities the object will make one or another impression on us if we let it interact with us either directly, or indirectly. The object may be a radiation field, and its wave function will tell us with what probability we shall see a

flash if we put our eyes at certain points, with what probability it will leave a dark spot on a photographic plate if this is placed at certain positions. In many cases the probability for one definite sensation will be so high that it anounts io a certainty-this is always so if classical mechanics provides a close enough approximation to the quantum laws.

The information given by the wave function is communicable. If someone else somehow

[85] The contents of this section should be part of the standard material in courses on quantum mechanics. They are given here because it may be helpful to recall them even on the part of those who were at one time already familiar with them, bea perced that every reader of these lines had the benefit of a course courses in quanics, and because the writer is well aware of the fact that see also, in addition thantum mechanics do not take up the subject here discussed. Section 2.9, particularly to references 3 and 4, W. Pauli, Handbuch der Physik, Sect. Bauer, La Thorie de Yob (Berlin: Julius Springer, 1933). Also F. London and E. And Co., 1939). The last authors observe (page 41), "Remarquons le rle essential que joue la conscience de l'observateur. . ."

determines the wave function of a system, he can teil me about it and, according to the theory, the probabilities for the possible different impressions (or "sensations") will be equally large, no matter whether he or I interact with the system in a given fashion. In this sense, the wave function "exists."

It has been mentioned before that even the complete knowledge of the wave function does not permit one always to foresee with certainty the sensations one may receive by interacting with a system. In some cases, one event (seeing a flash) is just as likely as another (not seeing a flash). However, in most cases the impression (e.g., the knowledge of having or not having seen a fash) obtained in this way permits one to foresee later impressions with an increased certainty. Thus, one may be sure that, if one does not see a flash if one looks in one direction, one surely does see a flash if one subsequently looks in another direction. The properiy of observations to increase our ability for foresceing the future follows from the fact that all knowledge of wave functions is based, in the last analysis, on the "impressions" we receive. In fact, the wave function is only a suitable language for describing the body of knowledge-gained by observations-which is relevant for predicting the future behaviour of the system. For this reason, the interactions which may create one or another sensation in us are also called observations, or measurements. One realises that all the information which the laws of physics provide consists of probability connections between subsequent impressions that a system makes on one if one interacts with it repeatedly, i.e., if one makes repeated measurements on it. The wave function is a convenient summary of that part of the past impressions which remains relevant for the probabilities of receiving the different possible impressions when interacting with the system at later times.

24.17.3 An Example

It may be worthwhile to illustrate the point of the preceding section on a schematic example. Suppose that all our interactions with the system consist in looking at a certain point in a certain direction at times
$\dot{t}_0, \dot{t}_0+1, i_0+2, \cdots$, and our possible scnsations are seeing or not seeing a flash The relevant law of nature could then be of the form: "If you see a flash at time t, you will see a flash at time $t+1$ with a probability 1/4, no flash with a probability 3/4; if you see no Hash, then the next observation will give a fash with the probability 3/4, no flash with a probability 1/4; there are no further probability connections." Clearly, this law can be verified or refuted with arbitrary accuracy by a sufficiently long series of observations. The wave function in such a case depends only on the last observation and may be ψ_1 if a flash has been seen at the last interaction, ψ_2 if no flash was noted. In the former case, that is for ψ_1, a calculation of the probabilities of flash and no flash after unit time interval gives the values 1/4 and 3/4; for ψ_2 these probabilities must turn out to be 3/4 and 1/4. This agreement of the predictions of the law in quotation marks with the law obtained through the use of the wave function is not surprising. One can either say that the wave function was invented to yield the proper probabilities, or that the law given in quotation marks has been obtained by having carried out a calculation with the wave functions, the use of which we have learned from Schrödinger.

The communicability of the information means, in the present example, that if someone else looks at time t, and tells us whether he saw a flash, we can look at time $t+1$ and observe a flash with the same probabilities as if we had seen or not seen the flash at time t ourselves. In other words, he can tell us what the wave function is: ψ_1 if he did, ψ_2 if he did not see a flash.

The preceding example is a very simple one. In general, there are many types of interactions into which one can enter with the system, leading to different types of observations or measurements. Also, the probabilities of the various possible impressions gained at the next interaction may depend not only on the last, but on the results of many prior observations. The important point is that the impression which one gains at an interaction may, and in general

does, modify the probabilities with which one gains the various possible impressions at later interactions. In other words, the impression which one gains at an interaction, called also the result of an observation, modifies the wave function of the system. The modified wave function is, furthermore, in general unpredictable before the impression gained at the interaction has entered our consciousness: it is the entering of an impression into our consciousness which alters the wave function because it modifies our
appraisal of the prohabilities for different impressions which we expect to receive in the future. It is at this point that the consciousness enters the theory unavoidably and unalterably. If one speaks in terms of the wave function, its changes are coupled with the entering of impressions into our consciousness. If one formulates the laws of quantum mechanics in terms of probabilities of impressions, these are ipso facto the primary concepts with which one deals.

It is natural to inquire about the situation if one dues nut make the observation oneself but lets someone else carry it out. What is the wave function if my friend looked at the place where the flash might show at time t ? The answer is that the information available about the object cannot be described by a wave function. One could attribute a wave function to the joint system: friend plus object, and this joint system would have a wave function also after the interaction, that is, after my friend has looked. I can then enter into interaction with this joint system by asking my friend whether he saw a flash. If his answer gives me the impression that he did, the joint wave function of friend + object will change into one in which they even have separate wave functions (the total wave function is a product) and the wave function of the object is ψ_1. If he says no, the wave function of the object is ψ_2, i.e., the object behaves from then on as if I had observed it and had seen no flash. However, even in this case, in which the observation was carried out by someone else, the typical change in the wave function occurred only when some information (the yes or no of my friend) entered my consciousness. It follows that the quantum description of objects is influenced by impressions entering my consciousness. [6] Solipsism may be logically consistent with present quantum mechanics, monism in the sense of materialism is not. The case against solipsism was given at the end of the first section.

24.17.4 The Reasons for Materialism

The principal argument against materialism is not that illustrated in the last two sections: that it is incompatible with quantum theory. The
[6] The essential point is not that the states of objects cannot be described by means of position and momentum co-ordinates (because of the uncertainty principle). The point is, rather, that the valid description, by means of the wave function, is mark of London and Bauer, quoted above, and S. Watanabe's article in Louis de Broglie, Physicien et Penseur (Paris: Albin Michel, 1952), p. 385.
principal argument is that thought processes and consciousness are the primary concepts, that our knowledge of the external world is the content of our consciousness and that the consciousness, therefore, cannot be denied. On the contrary, logicaliy, the external worid could be denied-though it is not very practical to do so. In the words of Niels Bohr, [7] "The word consciousness, applied to ourselves as well as to others, is indispensable when dealing with the human situation." In view of all this, one may well wonder how materialism, the doctrine [8] that "life could be explained by sophisticated combinations of physical and chemical laws," could so long be accepted by the majority of scientists.

The reason is probably that it is an emotional necessity to exalt the problem to which one wants to devote a lifetime. It one admitted anything like the statement that the laws we study in physics and chemistry are limiting laws, similar to the laws of mechanics which exclude the consideration of electric phenomena, or the laws of macroscopic physics which exclude the consideration of "atoms," we could not devote ourselves to our study as wholeheartedly as we

have io in order to recognise any new regularity in nature. The regularity which we are trying to track down must appear as the all-important regularity-if we are to pursue it with sufficient devotion to be successful. Atoms were also considered to be an unnecessary figment before macroscopic physics was essentially complete-and one can well imagine a master, even a great master, of mechanics to say: "Light may exist but I do not need it in order to explain the phenomena in which I am interested." The present biologist uses the same words about mind and consciousness; he uses them as an expression of his disbelief in these concepts. Philosophers do not need these illusions and show much more clarity on the subject. The same is true of most truly great natural scientists, at least in their years of maturity. It is now true of almost all physicists-possibly, but not surely, because of the lesson we learned from quantum mechanics. It is also possible that we learned that the principal problem is no longer the fight with the adversities of nature but the difficulty of understanding ourselves if we want to survive.

[7] N. Bohr, Atomic Physics and Human Knowledge, section on "Atoms and Human Knowledge," in particular p. 92 (New York: John Wiley & Sons, 1960).

[8] The quotation is from William S. Beck, The Riddle of Life, Essay in Adventures of the Mind (New York: Alfred A. Knopf, 1960), p. 35. This article is an eloquent statement of the attitude of the open-minded biologists toward the questions discussed in the present note.

24.17.5 Simplest Answer to the Mind-body Question

Let us first specify the question which is outside the province of physics and chemistry but is an obviously meaningful (because operationally defined) question: Given the most complete description of my body (admitting that the concepts used in this description change as physics develops), what are my sensations? Or, perhaps, with what probability will I have one of the several possible sensations? This is clearly a valid and important question which refers to a concept-sensa-tions-which does not exist in present-day physics or chemistry. Whether the question will eventually become a problem of physics or psychology, or another science, will depend on the development of these disciplines.

Naturally, I have direct knowledge only of my own sensations and there is no strict logical reason to believe that others have similar experiences. However, everybody believes that the phenomenon of sensations is widely shared by organisms which we consider to be living. It is very likely that, if certain physico-chemical conditions are satisfied, a consciousness, that is, the property of having sensations, arises. This statement will he referred to as our first thesis. The sensations will be simple and undifferentiated if the physico-chemical substrate is simple; it will have the miraculous variety and colour which the poets try to describe if the substrate is as complex and well organized as a human body.

The physico-chemical conditions and properties of the substrate not only create the consciousness, they also influence its sensations most profoundly. Does, conversely, the consciousness influence the physicochemical conditions? In other words, does the human body deviate from the laws of physics, as gleaned from the study of inanimate nature? The traditional answer to this question is, "No": the body influences the mind but the mind does not influence the body." Yet at least two reasons can be given to support the opposite thesis, which will be referred to as the second thesis.

The first and, to this writer, less cogent reason is founded on the

[9] This writer does not profess to a knowledge of all, or even of the majority of all, metaphysical theories. It may be significant, nevertheless, that he never found an affirmative answer to the query of the text-not even after having perused the relenica.

quantum theory of measurements, described earlier in sections 2 and 3. In order to present this argument, it is necessary to follow my description of the observation of a "friend" in somewhat more detail than was done in the example discussed before. Let us assume again that the object

has only two states, 1/1 and 1/2. If the state is, originally, 1/1, the state of object plus observer will be, after the interaction, $\psi_1 \times \chi_1$; if the state of the object is ψ_2, the state of object plus observer will be $\psi_2 \times \chi_2$ after the interaction. The wave functions χ_1 and χ_2 give the state of the observer; in the first case he is in a state which responds to the question "Have you seen a flash?" with "Yes"; in the second state, with "No." There is nothing absurd in this so far.

Let us consider now an initial state of the object which is a linear combination $\alpha_{\psi_i} + \beta\psi_2$ of the two states ψ_1 and ψ_2. It then follows from the linear nature of the quantum mechanical equations of motion that the state of object plus observer is, after the interaction, $\alpha(\psi_1 \times \chi_1) + \beta(\psi_{\#} \times \chi_{-})$. If I now ask the observer whether he saw a flash, he will with a probability $|\alpha|^2$ say that he did, and in this case the object will also give to me the responses as if it were in the state ψ_1. If the observer answers "No"-the probability for this is $|\beta|^2$-the object's responses from then on will correspond to a wave function ψ_2. The probability is zero that the observer will say "Yes," bui ille object gives the response which ψ_2 would give hecause the wave function $\alpha(\psi_1 \times x_1) + \beta(\psi_2 \times x_2)$ of the joint system has no ($\psi_{1,} \times \chi_1$) component. Similarly, if the observer denies having seen a flash, the behavior of the object cannot correspond to χ_1 because the joint wave function has no ($\psi_1 \times \chi_2$) component. All this is quite satisfactory: the theory of measurement, direct or indirect, is logically consistent so long as I maintain my privileged position as ultimate observer.

However, if after having completed the whole experiment I ask my friend, "What did you feel about the flash before I asked you?" he will answer, "I told you already, I did [did not] see a flash," as the case may be. In other words, the question whether he did or did not see the flash was already decided in his mind, before I asked him. [10] If we accept this, we are driven to the conclusion that the proper wave func-

[10] F. London and E. Bauer (op, cit., reference 5) on page 42 say, "Il [1'observatcur] dispose d'une facult caractristique et bien familire, que nous pouvons appeler la 'facult d'introspection': il peut se rendre compte de manire immdiate de son propre tat."

tion immediately after the interaction of friend and object was already either $\psi_1 \times \chi_1$ or $\psi_1 \times \chi_2$ and not the linear combination $\alpha(\psi_1 \times \chi_1) + \beta(\psi_2 \times \chi_2)$. This is a contradiction, because the state described by the wave function $\alpha(\psi_1 \times \chi_1) + \beta(\psi_2 \times \chi_2)$ describes a state hat has properties which neither $\psi_1 \times x_{11}$ nor $\psi_{22} \times x_{22}$ has If we substitute for "friend" some simple physical apparatus, such as an atom which may or may not be excited by the light-flash, this difference has observable effects and there is no doubt that $\alpha(\psi_1 \times \chi_1) + \beta(\psi_2 \times \chi_2)$ describes the properies of the joint system correctly, the assumption that the wave function is either $\psi_1 \times \chi_{\chi_1}$ or $\psi_2 \times \chi_{\chi_2}$ does not. If the atom is replaced by a conscious being, the wave function $\alpha(\psi_1 \times \chi_1) + \beta(\psi_2 \times \chi_2)$ (which also follows from the linearity of the equations) appears absurd because it implies that my fricnd was in a state of suspended animation before he answered my question. [11]

It follows that the being with a consciousness must have a different role in quantum mechanics than the inanimate measuring device: the atom considered above. In particular, the quantum mechanical equa tions of motion cannot be linear if the preceding argument is accepted. This argument implies that "my friend" has the same types of impressions and sensations as I-in particular, that, after interacting with the object, he is not in that state of suspended animation which contesponds to the wave function $\alpha(\psi_1 \times \chi_1) + \beta(\psi_2 \times \chi_2)$. It is not necessary to see a contradiction here from the point of view of orthodox quantum mechanics, and there is none if we believe that the alternative is meaningless, whether my friend's consciousness contains either the impression of having seen a flash or of not having seen a flash. However, to deny the existence of the consciousness of a friend to this extent is surely an

[11] In an article which will appear soon [Werner Heisenberg und die Physik unserer Zeit (Braunschweig: Friedr. Vieweg, 1961)] G. Ludwig discusses the theory of measurements and arrives at the conclusion that quantum mechanical theory cannot have unlimited validity (see, in par-

ticular, Section IIIa, also Ve). This conclusion is in agreement with the point of view here represented. However, Ludwig believes that quantum mechanics is valid only in to to be valid for all inscopic system, animate objesing inaccurate as the size of the system increases, and the dividing line between microscopic and macroscopic systems is surely not very sharp. Thus, the human eye can perceive as few as three quanta, and the propertics of macroscopic crystals are grossly affected by a single dislocation. For these reasons, the present writer prefers the point of view represented in the text even though he does not wish to deny the possibility that Ludwig's more narrow limitation of quantum mechanics may be justified ultimately.
unnatural attitude, approaching solipsism, and few people, in their hearts, will go along with it.

The preceding argument for the difference in the roles of inanimate observation tools and observers with a consciousness-hence for a violation of physical laws where consciousness plays a role-is entirely cogent so long as one accepts the tenets of orthodox quantum mechanics in all their consequences. Its weakness for providing a specific effect of the consciumsness on matter lies in its total reliance on these tenets a reliance which would be, on the basis of our experiences with the ephemeral nature of physical theories, difficult to justify fully.

The second argument to support the existence of an influence of the consciousness on the physical world is based on the observation that we do not know of any phenomenon in which one subject is influenced by another without exerting an influence thereupon. This appears convincing to this writer. It is true that under the usual conditions of experimental physics or biology, the influence of any consciousness is certainly very small. "We do not need the assumption that there is such an effect." It is good to recall, however, that the same may be said of the relation of light to mechanical objects. Mechanical objects influence light-otherwise we could not see them-but experiments to demonstrate the effect of light on the motion of mechanical bodies are difficult. It is unlikely that the effect would have been detected had theoretical considerations not suggested its existence, and its manifestation in the phenomenon of light pressure.

24.17.6 More Difficult Questions

Even if the two theses of the preceding section are accepted, very little is gained for science as we understand science: as a correlation of a body of phenomena. Actually, the two theses in question are more similar to existence theorems of mathematics than to methods of construction of solutions and we cannot help but feel somewhat helpless as we ask the much more difficult question: how could the two theses be verified experimentally? i.e., how could a body of phenomena be built around them. It seems that there is no solid guide to help in answering this question and one either has to admit to full ignorance or to engage in speculations.

Before turning to the question of the preceding paragraph, let us note
in which way the consciousnesses are related to each other and to the physical world. The relations in question again show a remarkable similarity to the relation of light quanta to each other and to the material bodies with which mechanics deals. Light quanta do not influence each other directly [12] but only by influencing material bodies which then influence other light quanta. Even in this indirect way, their interaction is appreciable only under exceptional circumstances. Similarly, consciousnesses never seem to interact with each other directly but only via the physical world. Hence, any knowledge about the consciousness of another being must be mediated by the physical world.

At this point, however, the analogy stops. Light quanta can interact directly with virtually any material object but each consciousness is uniquely related to some physico-chemical structure through which alone it receives impressions. There is, apparently, a correlation between each consciousness and the physico-chemical structure of which it is a captive, which has no

analoguc in the inanimate world. Evidently, there are enormous gradations between consciousnesses, depending on the elaborate or primitive nature of the structure on which they can lean: the sets of impressions which an ant or a microscopic animal or a plant receives surely show much less variety than the sets of impressions which man can receive. However, we can, at present, at best, guess at these impressions. Even our knowledge of the consciousness of other men is derived only through analogy and some innate knowledge which is hardly extended to viher species.

It follows that there are only two avenues through which experimentation can proceed to obtain information about our first thesis: observation of infants where we may be able to sense the progress of the awakening of consciousness, and by discovering phenomena postulated by the second thesis, in which the consciousness modifies the usual laws of physics. The first type of observation is constantly carried out by millions of families, but perhaps with too little purposefulness. Only very crude observations of the second type have been undertaken in the past, and all these antedate modern experimental methods. So far as it is known, all of them have been unsuccessful. However, every phenomenon is unexpected and most unlikely until it has been discovered-and some of them remain unreasonable for a long time after they have been discovered. Hence, lack of success in the past need not discourage.

12 This statement is certainly true in an approximation which is much better than is necessary for our purposes.

24.17.7 Non-linearity of Equations As Indication of Life

The preceding section gave two proofs-they might better be called indications-for the second thesis, the effect of consciousness on physical phenomena. The first of these was directly connected with an actual process, the quantum mechanical observation, and indicated that the usual description of an indirect observation is probably incorrect if the primary observation is made by a being with consciousness. It may be worthwhile to show a way out of the difficulty which we encountered.

The simplest way out of the difficulty is to accept the conclusion which forced itself on us: to assume that the joint system of friend plus object cannot be described by a wave function after the interaction–the proper description of their state is a mixture. [15] The wave function is $(\psi_1 \times \chi_1)$ with a probability $|\alpha|^2$; it is $(\psi_2 \times \chi_2)$ with a probability $|\beta|^2$. It was pointed out already by Bohm [14] that, if the system is sufficiently complicated, it may be in practice impossible to ascertain a difference between certain mixtures, and some pure states (states which can be described by a wave function). In order to exhibit the difference, one would have to subject the system (friend plus object) to very complicated observations which cannot be carried out in practice. This is in contrast to the case in which the flash or the absence of a flash is registered by an atom, the state of which I can obtain precisely by much simpler observations. This way out of the difficulty amounts to the postulate that the equations of motion of quantum mechanics cease to be linear, in fact that they are grossly non-linear if conscious beings enter the picture. [15] We saw that the linearity condition led uniquely to the

[13] The concept of the mixture was put forward first by L. Landau, Z. Physik, 45, 430 (1927). A more elaborate discussion is found in J. von Neumann's book (footnote 4), Chapter IV. A more concise and elementary discussion of the concept of dau and E. Lifshitz, Quantum Mechanics (London: Pergamon Press, 1958), pp. 35-38.

14 The circumstance that the mixture of the states $(\psi_1 \times \chi_1)$ and $(\psi_2 \times \chi_2)$, with weights $|a|^2$ and $|\beta|^2$, respectively, cannot be distinguished in practice from the state $\alpha\,(\psi_1 \times \chi_1) + \beta\,(\psi_2 \times \chi_2)$, if the states χ are of great complexity, has been pointed out already in Section 22.11 of D. Bohm's Quantum Theory (New York: Prentice Hall, 1951). The reader will also be interested in Sections 8.27, 8.28

this treatise.
15 The non-linearity is of a different nature from that postulated by W. Heisenberg in his theory of elementary particles [cf., e.g., H. P. Durr, 14. Heisenberg, the equations giving the time variation of the state vector (wave function) are postulated to be non-linear.
unacceptable wave function $\alpha(\psi_1 \times x_1)+\beta(\psi_2 \times x_2)$ for the joint state. Actually, in the present case, the final state is uncertain even in the sense that it cannot be described by a wave function. The statistical element which, according to the orthodox theory, enters only if I make an observation enters equally if my friend does.

It remains remarkable that there is a continuous transition from the state $\alpha(\psi_1 \times \chi_1) + \beta(\psi_2 \times \chi_2)$ to the mixture of $\psi_1 \times \chi_1$ and $\psi_2 \times \chi_2$, with probabilitics $|\alpha|^2$ and $|\beta|^2$, so that every member of the continuous transition has all the statistical properties demanded by the theory of measurements. Each member of the transition, except that which corresponds to orthodox quantum mechanics, is a mixture, and must be described by a statistical matrix. The statistical matrix of the system friend-plus-object is, after their having interacted ($|\alpha|^2 + |\beta|^2 = 1$),

$$\| \begin{matrix} |\alpha|^2 & \alpha\beta^* \cos\delta \\ \alpha^\alpha \beta \cos\delta & |\beta|^2 \mid \end{matrix}$$

in which the first row and column corresponds to the wave function $\psi_1 \times \chi_1$, the second to $\psi_2 \times \chi_2$. The $\delta = 0$ case corresponds to orthodox quantum mechanics; in this case the statistical matrix is singular and the state of friend-plus-object can be described by a wave function, namely, $\alpha(\psi_1 \times \chi_1) + \beta(\psi_2 \times \chi_{20})$. For $\delta = 1/2\pi$, we have the simple mixture of $\psi_1 \times \chi_1$ and $\psi_2 \times \chi_2$, with probabilities $|\alpha|^2$ and $|\beta|^2$, respectively. At intermediate δ, we also have mixtures of two states, with probabilities $1/2 + (1/4 - |\alpha\beta|^2 \sin\delta)^{1/2}$ and $1/2 - \left(1/4 - |\alpha\beta|^2 \sin^2\delta\right)^{1/2}$. The two states are $\alpha(\psi_1 \times \chi_1) + \beta(\psi_2 \times \chi_{\chi^2})$ and $-\beta^*(\psi_1 \times \chi_1) + \alpha^*(\psi^2 \times \chi^2)$ for $\delta = 0$ and go over continuously into $\psi_1 \times \chi_1$ and $\psi_2 \times \chi_2$ as δ increases to $\frac{1}{2}\pi$.
The present writer is well aware of the fact that he is not the first one to discuss the questions which form the subject of this article and that the surmises of his predecessors were either found to be wrong or unprovable, hence, in the long run, uninteresting. He would not be greatly surprised if the present article shared the fate of those of his predeccssors. He feels, however, that many of the earlier speculations on the subject, even if they could not be justified, have stimulated and helped our thinking and emotions and have contributed to re-emphasize the ultimate scientific interest in the question, which is, perhaps, the most fundamental question of all.

24.18 I. 13 Law without Law by Wheeler

The second phase of the dialog began in Europe but continued in America from Einstein's arrival at Princeton in October, 1933, to his dedih here in April, 1955. Here Einstein tried to show that quantum theory - in making what happens depend upon what the observer chooses to measure -is incompatible with any reasonable idea of reality. [18] Bohr's reply [19] briefly summarized was this: Your concept of reality is too limited.

The BEAM SPLITTER

Of all the idealized experiments taken up by the two friends in their effort to win agreement, none is simpler than the beam splitter of fig. 4 . With the final half-silvered mirror in place the photodetector at the lower right goes click-click as the successive photons arrive but the adjacent counter registers nothing. This is cvidence of interference between beams 4 a and 4 b ; or, in photon language, evidence that each arriving light quantum has arrived by both routes, A and B . In such experiments, [9n] Einsiein originally argued, it is unreasonable for a single

photon to travel simultaneously two routes. Remove the half-silvered mirror, as at the lower left, and one will find that the one counter goes off, or the other. Thus the photon has traveled only one route. It travels only one route, but it travels both routes; it travels both routes, but it travels only one route. What nonsense! How obvious it is that quantum theory is inconsistent!

[18] A. Einstein, B. Podolsky and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete:" Physical Review 47: pp. 777-780 (1935).

[19] N. Bohr, "Can quantum-mechanical description of physical reality be considered complete?" Physical Revnew 48: pp. 696-702 (1935).

[20] The center of discussion in the Bohr-Einstein dialog was more often the so-called double-slit experiment than the beam splitter depicted in figure 4. The latter is made the focus of attention here because it presents the central point without getting into the physics of interference patterns.

The first section between stars (* * * * *) appeared in Wheeler, 1981a; the next section between stars from Wheeler, 1979; the following from Wheeler, 1980: and the final section (a single paragraph) from Wheeler, 1981b. Preparation for publication of all four items was assisted by The University of Texas Center for Theoretical Physics and by NSF Grant PHY7826592.

Bohr emphasized that there is no inconsistency. We are dealing with two different experiments. The one with the half-silvered minor removed tells which rouie. The one with the half-silvered mirror in place provides evidence that the photon traveled both routes. But it is impossible to do both experiments at once. One can observe one feature of nature, or the complementary feature of nature but not both features simultaneously. What we choose to measure has an irretrievable consequence for what we will find.

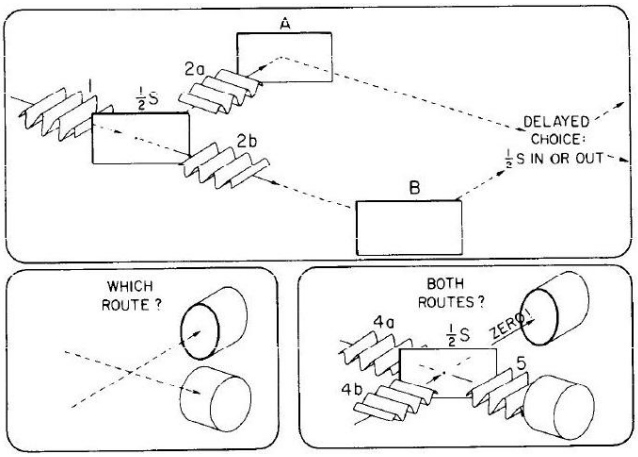


Fig. 4. Beam splitter (above) and its use in a delayed-choice experiment (below). An electromagnetic wave comes in at 1 and encounters the half-silvered mirror marked " $1 / 2 \mathrm{~S
$ " which splits it into two beams, 2a and 2b, of equal intensity which are telected by mirrors A and B to a crossing point at the rightiving photon has come. In the past the point of crossing tell by wher right, a half-silvered mirror is inserted at the point of crossing. On one side it brings beams 4 a and 4 b into destructive interference, so that the counter located on that side never registers anything. On the other side the beams are brought into constructive interference to reconstitute a beam, 5 . of the original strength, 1 . Every photon that enters at 1 is registered in that second counter in the idealized case of perfect mirrors and 100 per cent photodetector efficiency. In the one arrangement (lower left) one finds out didence that the arriving photon came by both routes. In the new "delaved-choice" version of the experiment one decides whether to put in the half-silvered mirror or take it out at the verv last minute. Thus one decides whether the photon "shall have come by one route. or by both routes" after it has "already done its travel."}

The DELAYED-CHOICE EXPERIMENT

In our own day we have learned to state the point even more sharply by way of a so-called delayed-choice experiment. [21] There we make the decision whether to put the final half-silvered mirror in place or to take it out at the very last picosecond, after the photon has already accomplished its travel. In this sense, we have a strange inversion of the normal order of time. We, now, by moving the mirror in or out have an unavoidable effect on what we have a right to say about the already past history of that photon.

"PHENOMENON"

The dependence of what is observed upon the choice of experimental arrangement made Einstein unhappy. It conflicts with the view that the universe exists "out there" independent of all acts of observation. In contrast Bohr stressed that we confront here an inescapable new feature of nature, to be welcomed because of the understanding it gives us. In struggling to make clear to Einstein the central point as he saw it, Bohr found himself forced to introduce the word "phenomenon." In today's words Bohr's point - and the central point of quantum theory - can be put into a single, simple sentence. "No elementary phenomenon is a phenomenon until it is a registered (observed) phenomenon." [8] It is wrong to speak of the "route" of the photon in the experiment of the beam splitter. It is wrong to attribute a tangibility to the photon in all its travel from the point of entry to its last instant of flight. A phenomenon is not yet a phenomenon

[21] J.A. Wheeler, "The 'past' and the 'delayed-choice' double-slit experiment," in A.R. Marlow, ed., Mathematical Foundations of Quantum Theory (Academic Press, New York, 1978), pp. 9-48.
[22] "Closed by irreversible amplification", p. 73: "irreversible amplification," p. 88: N. Bohr. Atomic Physics and Human Knowledge (Wiley, New York. 1958).
[23]Λ homcly illustration of this idea is provided by the old pas los game of Twenty Questions in the "surprise version" described by the author in several places, most recently in "Beyond the black hole," a chapter in H. Woolf, ed., Some Strangeness in the Proportions: An Einstem Centenary Celebration (Addison-Weslev, Reading. Mass.,
until it has been brought to a close by an irreversible act of amplification such as the blackening of a grain of silver bromide emulsion or the triggering of a photodetector. [22] In broader terms, we find that nature at the quantum level is not a machine that goes its inexorable way. Instead what answer we get depends on the question we put, the experiment we arrange, the registering device we choose. We are inescapably involved in bringing about that which appears to be happening. [93]

CONCERN ABOLT OBSERVER-PARIICIPANCY TODAY

Most applications of quantum theory deal with stationary states of elementary particles, of atomic nuclei, atoms, molecules and larger systems, and will processes of collision between one quantum system and another. Only in recent years has increasing attention come back to the point of centrai concern of Bohr and Einstein, the elementary quantum phenomenon, the process of measurement, the involvement of the registering device in bringing about that which appears to be happening, the strangest part of a strange subject. How can one contemplate indeterminism, complementarity and "phenomenon" without being reminded of the words of Gertrude Stein about modern art? "It looks strange and it looks strange and it looks very strange; and then suddenly it doesn't look strange at all and you can't understand what made it look strange in the first place." Many investigators, believing that the greatest insights are to be won from nature's strangest features, are - in research papers, review articles and books - giving fresh coverage of the strange "observerparticipancy" forced to our attention by the quantum. [24]
[24] Sec lon crample B. dEspagnat. ed.. Foundatum of Quantum Mrchama (Academic Press. New York. 1971): F.P. Wigner. "Interpretation of quantum medhanics." 93 pages of mimeographed notes of lectures delivered at Princeton Liniersia in 1976 on deposit in Fine Librars, Princeton Liniversity. Princeton, N.J. M.M. Viame. Mr. Namiki and S. Marhida. eds.. Theors of Measurement in Quantam MeGham Phaskal Soriett of Japan, Fohso. 1980): J.A. Wheeler "Fromters of time," della souda Internarionale di Fisica Emico Fermi. LXXII Coroo (North-Holland. Amsterdam. 1979).

MANY QUANTA VERSUS ONE QUANTUM

How does quantum mechanics today differ from what Bishop George Berkeley told us two centuries ago, "Esse est perripp," to be is to be perceived? [25] Does the tree not exist in the forest unless there is someone there to see it? Do Bohr's conclusions about the role of the observer differ from those of Berkeley? Yes, and in an important way. Bohr deals with the individual quantum process. Berkeley - like all of us under everyday circumstances - deals with multiple quantum processes.

Pondering the difference between the individual quantum phenomenon and the tree that falls, unobserved, in the forest, we waik through the art gallery on our way to visit again a favorite picture. We pass by the painting "Impressions," first shown by Claude Monet in 1863 at the Salon des Refuss. From a tiny dab of color on that canvas in the single second of our passage the pupil of our eye receives 50,000 photons. Each is accidental in its direction and time of arrival The quanta in that hail of information are so numerous that they give the impression

of perfect steadiness of illumination. What one of us busy mortals has the time to count them all? We rely instead on some gross and handier measure of intensity, such as the eye so aptly passes to the brain. There is no place in that message for the qualifying words, "with a root mean square fluctuation of 224 relative to an average number of photons of 50,000 ." Who needs to know about quanta to know the dot of color is there?

Unexpectedly the power blacks out. A guard with electric torch pointed at the floor guides our return. Our eye receives no photons from the dab of paint on the canvas. However, a touch of the hand as we pass the painting in the dark is enough to comfort us that it is still there. It would outreach any on-the-spot bookkeeping to count the 10^{16} atomic points of contact between the fingers and the picture frame, or the even more numerous quantum processes that impinge from the frame onto the fingertips. The message is still clear. How-

[25] (. Berkeles (1685-1783) in M.W. Calkins, ed., Berkeley: Essay, Primciples, Dialogs, with Selections from Other Writings (Scribner. New York. 1929, as reprimed in 1957).

ever, we now go through a longer chain of theory and interpretation in reaching the conclusion that the dab of paint is still there. Or was the luminous dot of color an illusion created by trick illumination from a concealed lamp? That was conceivable when we passed it first but highly unlikely given the integrity of the museum and the difficulty of the undertaking. During the exit through the dark it is more difficult to check against deception but the best indirect evidence one has says that the painting is still there with all its dots of color. Moreover, one is free to stop and extend the investigation and transform questionable evidence into convincing evidence.

When we emerge from the gallery and start thinking again of the tree, we recognize that this problem differs from the case of the picture only in degree, not in kind. The supposition that it feil we can check more and more conclusively according to the amount of effort we are willing to put into investigating impact points, ground dislocations and acoustic records. Anything macroscopic that happened in the past makes, we know, a rich fallout of consequences in the present. But whether we deal with the fall of the tree or the evidence for the dab of paint on the canvas or the motion of the moon through the sky, the number of quanta that come into play is so enormous that the unseen quantum individuality of the act of observation can hardly be said to influence the event observed.

In contrast the choice of question asked has a decisive consequence for [26] the elementary quantum phenomenon. For illustration it is enough to recall the inquiry of fig. 4 about the "track" of the photon, or a similar inquiry about the "path" of an electron through a beam splitter or the "motion" of an electron in an atom. In each of these examples, moreover, at least one of the available choices of question to be asked (which route for the photon or electron; or what position or momentum does the electron have in the atom) has a

completely unpredictable answer. We can send a million photons through the beam splitter when it is operated in the "which route" configuration at the lower left of fig. 4. Then we can be assured half a million photons, more or less (statistical variations of the order of magnitude ± 500) will be recorded by each counter. However, when vid the same arrangement we deal with a single photon we have not the slightest possibility to tell in advance which of the two counters ii will strike.

QUANTUM OUTCOME: GONERNED BY HIDDEN VARIABLES?

Is there not some underground machinery beneath the working of the world which one can ferret out to secure an advance indication of the outcome? Sume secret determiner, some

[826] Why not change "has a decisive consequence for . . ." to "makes all the difference in the elementary quantum phenomenon"? The word "difference" is not allowable. We can do the one experiment or the other experiment but the two experiments simply will not fit into one place at one time. We are dealing with one phenomenon, one "act of creation." The very individuality of the quantum phe

"hidden variable"? Every attempt, theoretical or observational, to defend such a hypothesis has been struck down. [27] Not the sightest hard evidence has ever been found that would throw doubt on the plain, straightforward prediction of quantum mechanics, the prediction that no prediction is possible. Probability? Yes. A definite forecast? No. Einstein could be unhappy that "God plays dice"; but Bohr could tcll him jokingly, "Einstein, stop telling God what to do." [28]

QUANTUM OUTCOME: ALLAH WILLED IT?

If no identifiable machinery is at hand to tell the lone photon which way to go then why not simply say of the route it actually takes, Allah willed it? And willed the outcome of every other individual quantum process?

To strike down a proposal of this kind, it has been

[27] For a review of relevant experiments, see especially F.M. Pipkin. "Atomic physics tests of the basic concepts in quantum mechanics, pp. 281-340 in Advances in Atomic and Molecular Phwars (Academic Press. New York. 1978).

[28] N. Bohr as quoted be J. Bronowaki. The Avent of Man (Little, Brown and Co.. Boston/Ioronto, 1973), p. 122.

pointed out more than once, [29] is beyond the power of logic. One has to appeal instead to pragmatism. In the struggle for survival, other things being equal, that way of life will go under that takes all that comes in a blindly fatalistic spirit. To evade danger and to seize opportunity every faculty has to be mobilized to predici what lies ahead of peril and promise. Society charges science with the task of prediction. Science makes some progress with the task. In the individual quantum process, however, prediction comes to the end of the road. Science does not have to be ashamed of its finding. It has only to be honest about it. Why demand of science a cause when cause there is none?

QUANTUM OUTCOME: ELEMENTARY ACT OF CREATION?

How did the universe come into being? Is that some strange, far-off process, beyond hope of analysis? Or is the mechanism that came into play one which ali the time shows itself?

Of the signs that testify to "quantum phenomenon" as being the elementary act of creation, none is more striking than its untouchability. In the delayed-choice version of the split-beam experiment, for example, we have no right to say what the photon is doing in all its long course from point of entry to point of detection. Until the act of detection the phenomenon-to-be is not yet a phenomenon. We could have intervened at some point along the way with a different measuring device; but then regardless whether it is the new registering device or the previous one that happens to be triggered we have a new phenomenon. We have come no closer than before to penetrating to the untouchable interior of the phenomenon. For a process of creation that can and does operate anywhere, that reveals itself and yet hides itself, what could one have dreamed up out of pure imagination more magic - and more fitting - than this?

DELAYED CHOICE AT The COSMOLOGICAL SCALE

Of all the features of the "act of creation" that is the elementary quantum phenomenon, the most startling is that seen in the delayed-choice experiment. It reaches back into the past in apparent opposition to the normal order of time The distance of travel in a laboratory split-beam experiment might be thirty meters and the time a tenth of a microsecond; but the distance could as well have been billions of light years and the time billions of years. Thus the observing device in the here and now, according to its last minute setting one way or the

[829] For a discussion of this point I am indebted to Professor Andrew Gleason.

other, has an interievable consequence for what one has the right to say about a photon that was given out long, before there was any life in the universe.

Two astronomical objects, known as $0957 + 561$ A, $\overline{\text{B}}$ (fig. 5), once considered to be two distinct quasistellar objects or "quasars" because they are separated by six seconds of arc, are considered now by many observers to be two distinct images of one quasar." Evidence has been found for an intervening galaxy, roughly a quarter of the way from us to the quasar. Calculations indicate [31] that a normal galaxy at such a distance has the power to take two light rays, spread apart by

[30] D. Walsh. R.F. Carswell and R.J. Wesmann. "0957+561.1.B twin quasistellar objects or gravitational lens," Vature 279: pp, 381-384 (1979) : R.J. We mann. F.H. Chaffee fin, M. Davis. N.P. Cainlean, D. Wals, aind R.I. Gaturd. "Multiplemurror observations of the twin (2SO (3957-561.A. B." Astophanal famma 233. L43-L+6 (1979) P.J. Voung. W.L.W. Sargent. J.A. Kristian and J.A. Wesphal, Cod photometry of the nucles of three styperions Gowpermassive object in the center Roberts. P.E. Greentedd and B.F. Burke, Johnal 234: pp. 76-85 (1979); 10.H. Rod at 6 centimeters wavelength." Somed 205 double quasar 0957 + 501. adome. Dantree, P.K. Moore, R.C. Noble and D Walsh, "Radio studies of the double (SSO (957-861.A.B." Nature 280: pp. $461 - 464$ (1979) P.F. Greenheld. D.H. Roberts and B.F. Burke. "The double quasar $0957 + 561$: examination of the gravitational lem hypothesis using the vers large arras," Scume, 208; pu. 495-497 (1980): P.J. Soung. J.F. Gumn. J.A. Kristian, J.B. Oke and J.A. Westphal. "(09957-561.1.B: a graditational lens formed br a galaxs at $z = 0.39$." Abophysical foomal, in press (1940)): B. Wills and D. Wills, "Spectrophotometry of the double (SSO $0957 + 561$ " A trophowal fommal Winn-Williams and R. Capps. "IR observations of the double quasar $9957 + 561$ A.B and the intervening galax." Vature 285 : pp. $91 - 93$ (1980).

C.C. Deer and R.C. Roeder. "Possible multiple imaging br spherical galaxies." Astothowal Journal 238. L67-L70 (1980): Ci.C. Dier and R.C. Roedes. "A range of time detass for the double quasar $0957 + 561.2.13$." lonophowal fammal, submitted for publication Jome 16. 1980.

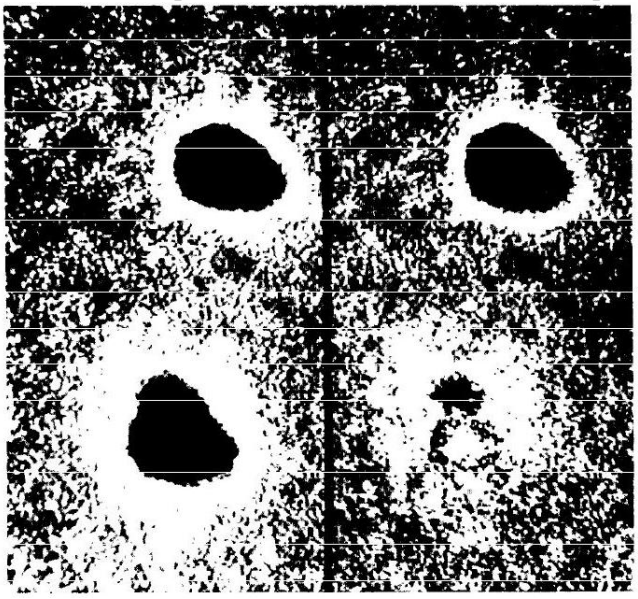


Fig. 5. Left. the double quasistellar object ("quasar": red shift $z = 1.41$), identified by its right ascension and declination as $0957 + 561$ A, B, and suspected to be the two by its right ascension and declination as $0957 + 561$ A, B, and suspected to be the two mages-produced gravidionalens artion-of one and the same quasar. This photograph, made at the University of Hawan Wills of the University of Texas at Austin, is the digital sum of five one-minute exposures in red light (5700 to 7000Å). The stellar images appear elongated because of a telescope tracking problem. Right. the same digital photographic record after a stellar

profile has been subtracted from the southern image (B), the residual being compatible with the existence ncar B of a lensing galaxy ($G-1$). Evidence has been found by Young, Gunn, Kristian, Oke and Westphal at Caltech for such a gataxy (0.02 to the west and 0.8 North of $6''$ red shift $z = 0.39$, (centered $2''$ to the West and $15''$ North of B). (centered 2 to the West and $15''$ North of B).
fifty thousand light years on their way out from the quasar, and bring them back together at the Earth. This circumstance, and evidence for a new case of gravitational lensing, [32] make it reasonable to promote the split-beam experiment in the delayed-choice version from the laboratory level to the cosmological scale as illusirated in fig. 6.

We get up in the morning and spend the day in meditation whether to observe by "which route" or to observe interference between "both routes." When night comes and the telescope is at last usable we leave the half-silvered mirror out or put it in, according to our choice. The monochromatizing filter placed over the telescope makes the counting rate low. We may have to wait an hour for the first photon. When it triggers a counter, we discover "by which route" it came with the one arrangement; or by the other, what the relative phase is of the waves associated with the passage of the photon from source to receptor "by both routes"- perhaps 50,000 light years apart as they pass the lensing galaxy G-1. But the photon has already passed that galaxy billions of years before we made our decision. This is the sense in which, in a loose way of speaking, we decide what the photon shall have done after it has already done it. In actuality it is wrong to talk of the "route" of the photon. For a proper way of speaking we recall once more that it makes no sense to talk of the phenomenon until it has been brought to a close by an irreversible act of amplification: "No elementary phenomenon is a phenomenon until it is a registered (observed) phenomenon."

[32] R.J. Weymann, D. Latham, J.R.P. Angel, R.F. Green, J.W. Liebert, D.A. Turnshek, D.E. Turnshek and J.A. Tyson, "The triple QSO PG1115+08: another probable gravitational lens," Nature 205: pp. 641-643 (1980).

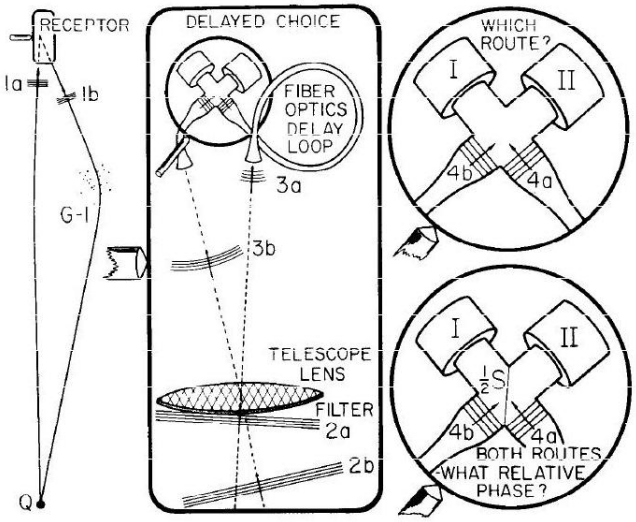


Fig. 6. Proposed delayed-choice experiment extending over a cosmological reach of space and time. Left, quasar Q reconded at receptor as two quasars by reason of the gravitational lens action of the intervening galaxy G-1. Middle, schematic design of receptor for delayed-choice experiment: (a) filter to pass only wave lengths in a narrow interval, corresponding to a long wave train, suitable for interference experiments; (b) iens to tocus the two apparent sources onto the acceptor such rate of change of length with time, as to bring together the waves traveling the two very different routes with the same, or close to the same, phase. Right, the choice. Upper diagram, nothing is interposed in the path of the two waves at the crossing of the optic fibers. Wave 4 a goes into counter I, and 4 b into counter II. Whichever of these photodetectors goes off, that - in a bad way of speaking - signals "by which route, *a* or *b*, the photon in question traveled from the quasar to the receptor. Lower diagram, a half-silvered mirror, 1/25, is interposed as indicated at the crossing of the two fibers. Let the delay loop be so adjusted that the two arriving waved in II. This result again in a misleading phraseology, says that "the photons in question come by both routes." However, at the time the choice was made whether to put in $1 / 2 \mathrm{~S
$ or leave it out, the photon in question had already been on its way for billions of years. It is not right to attribute to it a route. No elementary phenomenon is a phenomenon until it is a registered phenomenon.}

THE "PAST" IN The LIGHT OF The DELAYED-CHOICE EXPERIMENT

To use other language, we are dealing with an elementary act of creation. It reaches into the present from billions of years in the past. It is wrong to think of that past as "already existing" in all detail. The "past" is theory. The past has no existence except as it is recorded in the present. By deciding what questions our quantum registering equipment shall put in the present we have an undeniable choice in what we have the right to say about the past.

What we call reality consists (fig. 7) of a few iron posts of observation between which we fill in by an elaborate papiermach construction of imagination and theory. [33]

Spacetime in the prequantum dispensation was a great record parchment. This sheet, this continum, this carrier of all that is, was and shall be, had its definite structure with its curves, waves and ripples; and on this great page every event, like a glued down grain of sand, had its determinate place. In this frozen picture a far-reaching modification is forced by the quantum. What we have the right to say of past spacetime, and past events, is decided by choices - of what measurements to carry out - made in the near past and now. The phenomena called into being by these decisions reach backward in time in their consequences as indicated in fig. 8 ,

back even to the earliest days of the universe Registering equipment operating in the here and now has an undeniable part in bringing about that which appears to have happened. Useful as it is under everyday circumstances to say that the world exists "out there" independent of us, that view can no longer be upheld. There is a strange sense in which this is a "participatory universe."

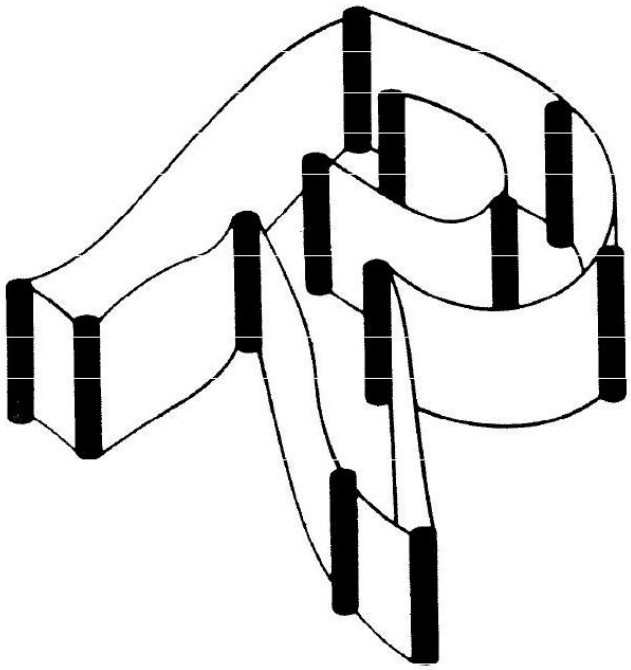


Fig. 7. What we call "reality," symbolized by the letter " R " in the diagram, consists of an elaborate papier-mach construction of imagination and theory fitted in between a few iron posts of observation.

FROM MEASUREMENT TO MEANING

We cannot speak in these terms without a caution and a question. The caution: "Consciousness" has nothing whatsoever to do with the quantum process. We are dealing with an event that makes itself known by an irreversible act of amplification, by an indelible record, [34] an act of registration. Does that record subsequently enter into the "consciousness" of some person, some animal or some computer? Is that the first step in translating the measurement into "meaning" meaning regarded as "the joint product of all the evidence that is available to those who communicate"? ?[35] Then that is a separate part of the story, important but not to he confused with "quantum phenomenon."

IS The UNIVERSE CONSIRUCIED OUT OF ELEMENIARY PHENOMENA?

From this caution we turn to the question: If the elementary quantum process is an act of creation, is an act of creation of any other kind required to bring into being all that is?

At first sight no question could seem more ridiculous. How fantastic the disproportion seems between the microscopic scale of the typical quantum phenomenon and the gigantic reach of the universe! Disproportion, however, we have learned, does not give us the right to dismiss. Else how would we have discovered that the heat of the carload of molten pig iron goes back for its explanation to the random motions of billions of microscopic atoms and the shape of

[833] In this connection see especially E.H. Gombrich. Art and Illusion: A Study in the Psychology of Pictorial Representation (Princeton University Press, Princeton, N.J., 1961, 2nd edition. revised), pp. 273, 329 and 394.

the elephant to the message on a microscopic strand of DNA? Is the term "big bang" merely a shorthand way to describe the

[34] F.J. Belinfante, Measurements and Time Reversal in Objective Quantum Theory (Oxford University Press, Oxford, 1975); terminology "indelible," p. 39.

[13] D. Fllesdal, "Meaning and experience" in S. Guttenplan, ed., Mind and Language (Clarendon Press, Oxford, 1975), pp. 254. Follesdal's atticle, the other articles in this book and the references they make to the still larger literature of meaning, a central topic of philosophy in Britain and America in recent decades, will indicate the representative character of this statement.

cumulative consequence of billions upon billions of elementary acts of observer-participancy reaching back into the past, as symbolized in fig. 8 ?

An old legend describes a dialog between Abraham and Jehovah. Jehovah chides Abraham, "You would not even exist if it were not forme!" "Yes, Lord, that I know," Abraham replies, "but also You would not be known if it were not for me." [36]

In our time the participants in the dialog have changed. They are the universe and man. The universe, in the words of some who would aspire to speak for it, says, "I am a giant Hachine. I supply the space and time for your existence. There was no before before I came into being, and there will

* Thanks are expressed here to Professors Lawrence P. Horwitz, Zvi Kurzweil, Yuval Ne'eman, Asher Peres. Shmuel Sambursky, I aurence Schulman and Elie Wiesel, each for his part in leading the author to this legend and documenting it, as follows: (i) H. Freedman and M. Simon, translators and eds., Midrash Rabbah, Genesis I (Soncino Press, London, 1939), p. 238, commentary on "Noah walked with God": "The God hefore whom my fathers Abraham and Isaac did walk, cic. (Gencsis 48:15). R. Berekiah in R. Johanan's name and Resh Lakish gave two illustrations of this. R. Johanan said: It was as if a shepherd stood and watched his flocks. Resh [Footnote: As an cscont, to make known lis coming. Similativ, Abranam and isaac walked before God, spreading His knowledge]. On R. Johanan's view: We need Itis proximity. Ontur vew of Resh iakish: Fie needs us to giorify Him [Footnote: By propagating the knowledge of His greatness]." (ii) Ibid, p. 357, commentary on, "And he blessed him, and said: blessed be Abram of the God most high, who has acquired [Koneh = maker of] heaven and earth" (Genesis 14:19): "From whom then did He acquire them:- Said R. Abba: [Acquired is attributive,] as Isaac said: Abraham used to entertain wayfarers, and after they and hair. **R**. would say to them, 'Say a blessing,' 'What shall we say" they asked. 'Blessed be the God of the Universe of Whose bounty we have eaten,' replied he. Then the Holy One, blessed be He, said to him: 'My Name was not known among My creatures, and thou hast made it known among them: I will regard thee as though thou wast associated with Me in the creation of the world'..." (iii) Deuteronomy 32:10: "He found him [Jacob] in a desert land, and in the waste howling wilderness; he led him about, he mstructed him, he kept him as the apple of his eve," as comto the Aggadic or legend of the Midrash or the and Land before the end of the 4 th century A.D. 18313 , "he led him about": "This is related to Genesis 12:1, 'Get thee out of thy country' . . . .; 'he instructed him': . . . . before our father Abraham came into this world it seemed as if the Lord, Blessed Be He, reigned only in Ileaven, since it is said, The Lord, God of Heaven, which took me from my father's house' (Genesis 24:7). But once Abraham had Heaven as Find [= was born], he Abration [thereby] enthroned Him over "Yeare my witnesses, saith the Lord, and my servant whom I have chosen; that ye may know and believe me, and understand that I am he: before me there was no God formed, neither shall there be after me."

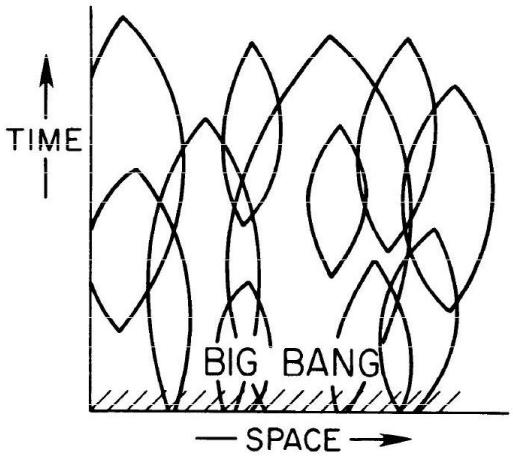


Figure 24.11: Fig. 8. Symbolic description how all that "has happened" in the past is influenced by choices made in the present as to what to observe. The upper tip of each "leaf" stands for the elementary act of registration. The lower end of each leaf stands for the beginning of the elementary phenomenon being investigated by the observatheir burden of physical content except the intormation carried in the elementary quantum acts thus symbolized? [Details in the original publication.]

be no after after I cease to exist. You are an unimportant bit of matter located in an unimportant galaxy."

How shall we reply? Shall we say, "Yes, on universe, without you I would not have been able to come into heing. Yet you, great system, are made of phenomena; and every phenomenon rests on an act of observation. You could never even exist without elementary acts of registration such as mine"?

Are elementary quantum phenomena, those untouchable, indivisible acts of creation, indeed the building material of all that is? Beyond particles, beyond fields of force, beyond geometry, beyond space and time themselves, is the ultimate constituent, the still more ethereal act of observer-participancy? For Dr. Samuel Johnson the stone was real enough when he kicked it. The subsequent discovery that the matter in that rock is made of positive and negative electric charges and more than 99.99 per cent empty space does not diminish the pain that it inflicts on one's toe. If the stone is someday revealed to be altogether emptiness, "reality" will be none the worse for the finding.

Roland M. Frye, in reminding us [37] of Shakespeare and of ways of seeing, gives us opportunity to recall those words of almost four hundred years ago,

And as imagination bodies forth
The form of things unknown, the poet's pen
Turns them to shapes, and gives to airy nothing
A local habitation and a name.

Are billions upon billions of acts of observer-participancy the foundation of everything? We are about as far as we can be today from knowing enough about the deeper machinery of the universe to answer this question. Increasing knowledge about detail has brought an increasing ignorance about plan. The very fact that we can ask such a strange question shows how uncertain we are about the deeper foundations of the quantum and its ultimate implications.

The QLANTUM: ITS USES — AND ITS USE

To encounter the quantum is to feel like an explorer from a faraway land who has come for the first time upon an automobile. It is obviously meant for use, and an important use, but what use? One opens the door, cranks the window up and down, flashes the lights on and off, and

perhaps even turns over the starter, all the time without knowing the central point of the thing. The quantum is the automobile. We use the quantum in a transistor to control machinery, in a molecule to design an anesthetic, in a superconductor to make a magnet. Could it be that all the time we have been missing the central point, the use of the quantum phenomenon in the construction of the universe itself?

We have tunted over the starter. We haven't got the engine going.

1. • Law without law.
   species will never vary, and have remained the same since the creation of each species.
   Charles Lixell [1], writing almost three doendes before The Ovigin of Species
   [The astronomer Sir John Frederick William] Herschel says my book
   is 'the law of higgledy-piggledy'.
   Charles Darwin [2], 18 days after the November 24, 1859 publication of The Origin of Species

Are the laws of physics eternal and immutable? or are these laws, like speries, mutable [3] and of "higgledy-piggledy " origin?

The hierarchical speciation of plant and animal life, we now know, ariscs out of the blind accidents of genetic mutation and natural selection [$\tilde{5}$, 6]. Likewise the gas laws, the pressure-volume-temperature relation for water and for other substances, and the laws of thermodynamics take their origin in the chatos of molecular collisions. But as for the molecules themselves, the particles of which they are made and the fields of force that couple them, is it conceivable that they too derive their way of action, their structure and even their existence from multitudinous accidents?

Such questions about the "plan" of physies we would hardly raise if we hard the skeleton of it in hand. But we don't. Now and then we meet a colleague in another realm of thought who still thinks physics is in possession of this plan. He cites the words of Laplace [7] and reiterates the Laplacean vision as he understands it: the laws are definite, the initial co-ordinates and momenta are definite, and therefore the future is definite. The Universe is a machine.

No, we have to tell him: that is a cracked paradigm. Quantum medanies allows us to know a co-ordinate, or a momentum, but not both. Of the initialvalue data that Lowhere needed, the principle of complementarity [8] or indeterminacy [9] says half do not and cannot exist.

You tell me what isn't the plan of physics, our friend rejoins. If you understand quantum mechanics so well, why don't you tell we what is the plan of physics?

No one knows, we reply. We have clues, clues most of all in the writings of Bohr [23-25], but no answer. That he did not propose an answer, not whilosophize, not go an inch beyond the soundest fullest statement of the inrescapable Issous of quantum mechanies, was his way to build a clean pier for some later days bridge to the future.

What kind of a "plan of physics" do you think Boirs had in mind, our colleague asks. I know Einstein's words [26], "Physics is an attempt to grasp reality as it is thought independentiy of its being observed ". I know Bohr's reply [−28], "These conditions [of measurement] constitute an inherent element of any phenomenon to which the term 'physical reality' can be attached.... [This requires] a tinal renunciation of the classical ideal of causality and a radical revision of our attitude towards the problem of physical reality a. But, if I could have asked BoHr, how did he think the Universe came into being, and what is its substance, what would he have said?

It is too bate to ask. The plan is un to us to find.

The Universe can't be Laplacean. It may be higgledy-piggledy. But have hope. Surely someday we will see the necessity of the quantum in its construction. Would you like a little story along this line?

Of course! Mbout what?

Sbout the game of twentry questions. You recall how it goes-one of the after-dinner party sent

out of the living room, the others agreeing on a word, the one fated to be questioner returning and starting his questions. "Is it a living object?" "No." "Is it here on earth?" "Yes." So the questions go from respondent to respondent around the room until at length the word emerges: victory if in twenty tries or less; otherwise, defeat.

Then comes the moment when we are fourth to be sent from the room. We are locked out unbelievably long. On finally being readmitted, we find a smile on everyone's face, sign of a joke or a plot. We innocently start our questions. At tirst the answers come quickly. Then each question begins to take longer in the answering strange, when the answer itself is only a simple "yes" or "no". At length, feeling hot on the trail, we ask, "Is the word 'cloud'?" "I's", comes the reply, and everyone bursts out laughing. When we were out of the room, they explain, they had agreed not to agree in
advance on any word at all. Each one around the circle could respond "yes" or "no" as he pleased to whatever question we put to him. But however he mplied he had to have a word in mind compatible with his own reply-and with all the replies that went before. No wonder some of those decisions between "yes" and "no "proved so hard!

And the point of your story?
Compare the game in its two versions with physics in its two formulations, classical and quantum. First, we thought the word already existed out there n an phynies one thought that the position and momentum of the electron existed "out there", independent of any act of observation. Sccond, in actuality the information about the word was brought into being step by step through the questions we raised, as the information about the eqectron is brought into being, step by step, by the experiments that the oberrer chooses to make. Third, if we had chosen to ask different questions we would have ended up with a different word-as the experimenter would have mated up
ended up with a different word—as the experimenter would have ended up with a different story for the doings of the electron if he had meatured different quantities or the same quantities in a different order. Fourth, whatever power we had in bringing the particular word "cloud" into being was partal only. A major part of the selection-unknowing selection-lay in the ages or "no seplies of the collegues around the room. Similaty. the experimenter has some substantal influence on what will happen to the electron by the choice of experiments he will do on it : but he knows there is mudi impredictability about what any given one of his measurements will divelose. Fifth, there was a erule of the game " that required of every participator that his choice of yes or no should be compatible "ith some word. Nimilaty. there is a consistence about the observations made in physics. One jerom must be able to tell another in plain language what he finds and the serome preson must he able to verify the observation.

Go on!
That is difficult! Interesting though our comparison is between the world of physics and the world of the game, there is an important point of difference. The game has few participants and terminates after a few sters. In contrast, the making of observations is a continuing process. Moreover. it is extraordingurily differelt to state sharely and deady where the community of obremen participators begins and where it ends.

This comparison between the world of quantum observations and the game of twenty questions misses much, but it makes the vital central point. In the real world of quantum physics, no elementary phenomenon is a phenomenon until it is an observed phenomenon. In the surprise version of the game no word is a word until that word is promoted to reality by the choice of questions asked and answers given. "Cloud" sitting there waiting to be found as we entered the room? Pure delusion! Momentum, $\mu_s = 1.4 \cdot 10^{19}$gems, or position, $x == 0.31 \cdot 10^{-8}$ cm, of the electron waiting to be found as we start to probe the atom? Pure fantasy! Max may be going too far when he neggests [29] that "... we are actually bringing about what seems to be happening to us". However, it is undeniable that each of us, as observer, is also one of the par

ticipators in bringing “reality " into being.

To say “no clementary phenomenon is a phenomenon until it is an observed phenomenon is to make no small change in our traditional view that something has a already happened " before we observe it. The wome eloud ", we mistakenly thought, already existed in the room before we “uncovered” it. The photons of the primordial cosmic fireball radiation that enter our telescope today, we customarily assume, alroady had an existence in the very earlient days of the Cniverse, long before life evolved. However, not until we eatel a particular one of those photons in a particular state with particular parameters, not until the elementary phenomenon is an observed phenomenon, do we have the right even to call it a phenomenon. This is the sense, the limited sense, but the incescapable sense, in which we here, now, have a part in bringing about inat which "had abready happened on a time when ho where wete existed.

But what about the mbelievably more numerous reliet photons that escape our telescope? Surely you do not deny them "reality"?

Of comse not: but their “reality ” is of a paier and more theoredic hue. The vision of the luiverse that is so vivid in our minus is framed by a few iron posts of true observation-themselves also resting on theory for their meaning-but most of the wails and towers in the vision are of papier-mache, phastered in between those posts by an immense labor of imagination and theory. In this labor, a... we can never neatly separate what we see from what we know ... what we call seemg is invariably coloured and shaped by our knowidelge (or belief) of what we see "[61]. "Without some initial system, without a first guess to which we can stick unless it is disproved, we could ... make no "sense" of the milliams of ambiguous stimuli that reach us from our environment. In order to learn, we mod make mistakes ... the simplicity hypothesis cannot be learned. It is ... the only condition under which we could learn at all” [62]. "... our mind will still react to the challenge of this conoudrum [of what we’see’] by throwing out a random answer, making ready to test it in terms of consistent possible worlds. It is these answers that will transform the ambiguous stimulus pattern into the image of something ’out there’ "[63].

What keeps these images of something aout there "from degenerating into separate aud private miverses: one observer, one universe: another observer, another universe?

That is prevented by the very solidity of those iron posts, the elementary acts of observership-participaney. That is the importance of Bohrs point that no observation is an observation unless we can communicate the results of that observation to others in plain language [49].

The only thing harder to understand than a law of statistical origin would be a law that is not of statistical origin, for then there would be no way for it-or its progenitor principles-to come into being. On the other hand, when we view each of the laws of physics-and no laws are more magniticent in seope or better tested-as at bottom statistical in character, then we are at last able to forego the idea of a law that endures from everlasting to everlasting.

Individual events. Events beyond law. Events so numerous and so menordinated that, flaunting their freedom from formula, they yet fabricate firm form.

“Fabricate form”! Do you suggest that even the 4 -dimensional spacetime manifold is only a fabrication, only a theory-irreplaceable convenience though that theory is?

Yes! Compare space-time with cloth. Each it is useful under everyday circumstances to call a manifold. Yet each is exactly then most obviously not a manifold where it comes to an end, whether in the selvedge made by the loom, or in the geodesic terminations made by one of the "gates of time"big bang or hig crunch [31, 32] or black hole [33]. Nowhere more clearly than in the ending of space-time are we warned that time is not an ultimate category in the description of Nature [34].

Aren’t you being extreme? I see the lesson of the game of twenty questions. I begin to believe with you that no elementary phenomenon is a phenomenon until it is an obsered phonomenon. I aceept that events of observer partici pancy, as you call them, occupy a special

place in the scheme of things. I agree that that word "cloud" was brought into being entirely through such dementary avents. Rut that such ovent;, however numorous, should be the sole blocks for building the laws of physics-and space and time themselvesscems to me preposterous. You surely have been involved enough in times past with nutr-and-bolt; physics to know the difference between science and poetry: yet if I appreciate the drift of what you say, you might as well be quoting Sillmentelre [35],

> ... These our actors,
> As I foretold you, wew all spiits and
> Are melted into air, into thin air:
> And, like the baseless fabric of this vision,
> The cloud-cappil towers, the gorgeous palaces.
> The solemn temples, the great globe itself,
> Yea, all which it inherit, shall dissolve
> And, like this insubstantial pageant faded,
> Leave not a rack behind. We are such stuff
> As dreams are made on ...

I can't believe any such dreamlike vision of the physical world. As samuel Jonson used to say, I have only to kick a stone to find it real enough.

Why do you say "preposterous"? Perhaps Shlmespeire understood this miserse of ours better than we do ourselves! You have known for years that the atom is more than 99.99 percent emptiness. If matter turns out in the end to be altogether ephemeral, what difference can that make in the pain you feel when you kick the rock? And how can matter-and space-time-be anything but mutable, coming into being at one gate of time and fading out
of existence at the other? No physics before the big bang, or after the big crunch? No! The lesson of Einstein's standard closed-space cosmology is different and stronger. It denies ail meaning to such terms as "before the big bang , and "after the big crunch".

Jarticles or fields or mathematics won't do for ultimate building blocks. They can't come into being or face out of existence [30].

Yes, I appreciate the reasons given [36] against believing in any "magic particle " or any "magic field " or [37] any "magic mathematics" as the foundation of physics; but isn't it even more difficult to think of acts of observerparticipancy as the magic ingredient?
lifticult, yes: inconceivable, no.
Go on!
No, we have to stop here. It is heyond the power of today to fit together the pieces of the puzzle.

Don't stop! You've carried me halfway into an exciting mystery story. You can't leave me without the traditional half-way-point review of the important clues and first try at a working hypothesis.

Review? A proper review would be impossibly ambitious. And how can one advance a working hypothesis that will not be urong tomorrow and ridiculous the day after?

I appeal to you to go on. You have told me more than once that science advances only by making all possible mistakes; that the main thing is to make the mistakes as fast as possible-and recognize them. You like to quote the motto of that engine inventor, John Kris: "Start her up and see why she don't run". You point to Einstein's definition of a scientist, "An unscrupulous opportunist". If you believe all this, and are a true colleague of mine, you must go on.

You leave no escape!
Good!
Then let us agree to go on; but let us replace the comprehensive review of clues that you wanted by something more modest. How would it do, for example, to survey some of the lessons we

have learned from the study of time, and how those lessons bear on "observer-participancy"?
i accepi, aud with many thanks. But first tell me the centrol point as you see it.

The absolute central point would seem to be this: The Universe had to have a way to come into being out of nothingness, with no prior laws, no Swiss watchworks, no nucleus of crystallization to help it-as on a more modest level, we believe, life came into being out of lifeless matter with no prior life to guide the process [5, 6, 38].

When we say "out of nothingness" we do not mean out of the vacuum of physics. The vacuum of physics is loaded with geometrical structure and vacuum fluctuations and virtual pairs of particles. The Universe is already
in existence when we have such a racuum. No, when we speak of nothing. ness we mean nothingness: neither structure, nor law, nor plan.

A conception mote dearly impossible I never heardi
Preposterous we have to agree is the idea that everything is produced out of nothing-as preposterous, but perhaps also as inescapable, as the view that life had its origin in lifeless mader.

But how?
"Omnibus ex nihil ducendis sufficit unum ", LEIBNIZ told us [39]; for producing everything out of notining one principle is enough. Of all principles that might meet this requirement of Leibniz nothing stands out more strikingly in this era of the quantum than the necessity to draw a line between the ob-server-participator and the system under riew. Without that demarcation it would make no sense to do quantum mechanies, no sonse to speak of quantum theory of measurement, no sense to say that "No elementary phenomenon is a phenomenon until it is an observed phenomenon %. The necessity for that line of separation is the most mysterions feature of the quantum. We take that demarcation as being, if not the central principle, the clue to the central principle in constructing out of nothing everything.

Let me ask if your reasoning condn't be turned around. You talk of the observer-participancy of quantum theory as the mechanism for the Universe to come into being. If that is a proper way of speaking, would the converse not also hold: The strange necessity of the quantum as we see it everywhere in the scheme of physies comes from the requirement that-via observer-participancy-the Universe should have a way to come into being?

Your point is exeiting indeed. If true-and it is attractive-it should provide someday a means to derive quantum mechanies from the requirement that the Universe must have a way to come into being [40].

I know that in that empty courtyard many a game cannot be a game until a line has been drawn-it does not matter where-to separate one side from the other. I know that no Gaussian flux integral can be a flux integral until the 2 -surface over which it runs-bompy and rippled though we make it and deform it as we will-has been extended to closure. But how much arbitrarinexs is there in this more ethereal kind of demareation, the line between esystem, and "obouring device n ?

Much arbitrariness! Bonn stresses [42] that the stick wo hold ean itsulf be an object of investigation, as when we run our fingers over its surface. The same stick, when grasped firmly and used to explore something else, becomes an extension of the observer or-when we depersonalize-a part of the measuring equipment. As we withdraw the stick from the one role, and recast it in tho other role, we transpose the line of demarcation from one end of it to the other. The distinction between the probed and the probe, so evident at this seale of the everyday, is the without-which-nothing of every elementary phenomenon, of every "closed" quantum process.

Do we possess today any mathematical or legalistic formula for what the line is or where it is to be drawn?

No.
Then what is important about this demarcation?

Existence, yes; position, no. It is the mark of an observation to leave an "indelible" record, according to BEIXENTE [13]. Wifiner argues that an observation is only then an observation when it becomes part of "the consciousness of the observer "[4] and points to "the impressions which the observer receives as the basic entities between which quantum memanics postulates correlations "[45]. For Bonr the central point is not "consciousness", not even an "observer", but an experimental device-grain of silver bromide, Gejer counter, retina of the eye-capable of an 4 irreversible act of amplfication "[47]. This act brings the measuring process to a close" [48]. Only then, he emphasized, is one person able "to describe the result of the neasurement to another in plain hanguage "[10]. He adds that a all departures from common language and ordinary logic are entirely avoided by reserving the word 'phenomenon' solely for reference to unambiguously communicable information "[500].

I would have felt very uncomfortable if Bonr had used the term "consciousness in defining the elemental act of observation. I would not have known what he meant. However, I am beginning to understand and accept the terms he actually adopts, ebrought to a close by an ineversible act of amplification" and "communicable in plain language". What was his position on consciousness?

We have asked Jorgen K.u.ck.ir, who eollaborated with l'our in his iast months, and he has kindly replied [51], "During work on the preparation of some lecture, to define the phenomenon of consciousiness, Bonn used a phated somewhat like this: a beliaviour so complex that an arequate account would require references to the organism's 'self-awareness'. I objected jokingly that with this definition he would soon have to ascribe a consciousness to the what as a highly developed electronic compurs an electronic absolutely prepared', said he, to tak of the spirital some computer: to state that it is reflecting or that it is in a bad mood.... The question whether the machine really feels or ponders, or whether it merely looks as though it did, is of course absolutely meaningless'. "

Other outstanding thinkers have argued otherwise. For them aconsciousness" makes an unclimbable difference of principle between even the most powerful imaginable computer and the brain [52].

Do you agree with that argument?
How can we possibly accept such a difference of principle?
Do we not believe that brain function itself will someday be explained entirely in terms of physical chemistry and electrochemical potentials? What escape is there from the reasoning of von Neumann [53] and Bohr and many
active present-day investigators? When one of the three discoverers of the medhanism of superconductivity today gives us, chapter by chapter and verse by vatia an entirely cellular account of the mechanism of memory [54 – 56], who can dismiss it?

When a distinguished computer expert and student of the structure of society details, one by one, the distinctions proposed in times past between "conscioushess" and the computer, and painstakingly analyzes each down to nothingness [57], what case can anyone possibly maintain for amy distinction of principle between the computer and the brain?

I am happy not to have to delve today into the term "consciousness". I find it hard enough to know what to make of "irreversible act of amplification ". Sever have I heard of an act of amplification that was not characteriged by an amplification factor, or an equivalent quantity: and never an amplification factor that was not a finite number.

Between infinity and a finite number there may be a difference of principle: but between one finite number and another there is only a difference of degree. How big does the grain of silver bromide have to be, or the avalanche of electrons in the Geiger counter, before we count the measuring process as brought to a close by an irreversible act of amplitication?

Incording as I specify one or another number as the critical level of amplification, don't I make all the difference between rating or not rating a given process as an "elementary phe-

nomenon"?

According as the elosed Gaussian surface encloses a given elementany change or not, we find an unmistakable difference in the surface integral of the electric flux. Nevertheless, we know enough about the relevant invariance principle never to question the correctuess of always identifying fiux with enciosed charge. About "elementary quantum phenomenon" we have not today learned, but have a deep obligation someday to learn, enough to display a similar covariance with respect to where we draw the line. That is what "complementarity" is all about.

Wen if neither you nor I know how to define that line, I like the idea that the "game" in the empty courtyard is only then possible when *a* line is drawn. May I question you now about the game itself? How would you describe it if forced to commit yourself?

From "nothingness ruled out as meaningless," [106] to the line of distinction that rules it out; from this dividing line to "phenomenon"; from one phenomenon to many; from the statistics of many to regularity and structure: these considerations lead us at the end to ask if the universe is not best conceived as a self-excited circuit [107] (Fig. 22.13): Beginning with the big bang, the universe expands and coois. After eons of dynamic deveiopment it gives rise to observership. Acts of observer-participancy - via the mechanism of the delayed-choice experiment - in turn give tangible "reality" to the universe not only now but back to the beginning. To speak of the universe as a self-excited circuit is to imply once more a participatory universe.

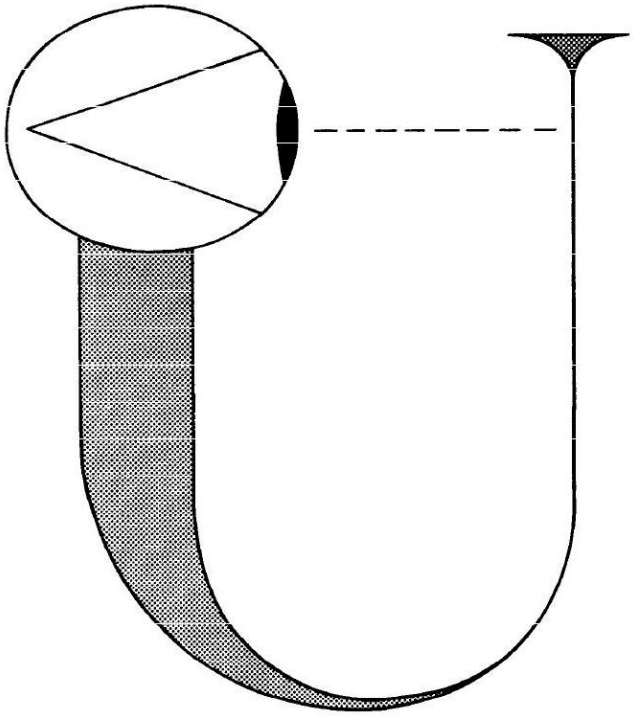


Fig. 22.13 The universe viewed as a self-excited circuit. Starting small (thin U at upper right), it grows (loof of U) and in time gives rise (upper left) to obsever-participancy - which in turn imparts "tangible reality" (cf. the delayed-choice experiment of Fig. 22.9) to even the earliest days of the universe.

If the views that we are exploring here are correct, one principle, observer-participancy, suffices to build everything. The picture of the participatory universe will flounder, and have to be rejected, if it cannot account for the building of law; and space-time as part of law; and out of law substance. It has no other than a higgledy-piggledy way to build law: out of the statistics of billions upon biliions of acts of observer-participancy each of which by itself partakes of utter randomness.

Two Tests

No test of these views looks more like being someday doable, nor more interesting and more instructive, than a derivation of the structure of quantum theory from the requirement that everything have a way io come into being [108] - as the word "cloud" was brought into being in the surprise version of the game of twenty questions. No prediction lends itself to a more critical test than this, that every law of physics, pushed to the extreme, will be found to be statistical and approximate, not mathematically perfect and precise. approximate, not mathematically perfect and precise.

The Challenge of "Law without Law"

We can ask oselves if it is not absolutely preposterous to put into a formuia anything at first sight so vague as law without law and substance without substance. How can we hope to move forward with no solid ground at all under our feet? Then we remember that Einstein had to perform the same miracle. He had to reexpress all of physics in a new language. His curved space seemed to take all definite structure away from anything we can call solidity. In the end physics, after being moved bodily over onto the new underpinnings, shows itself as clear and useful as ever. We have to demand no less here. We have to move the imposing structure of science over onto the foundation of elementary acts of observer-participancy. [109] No one who has lived through the revolutions made in our time by relativity and quantum mechanics - not ieast through the work of Einstein himself - can doubt the power of theoretical physics to grapple with this still greater challenge.

Recent decades have taught us that physics is a magic window. It shows us the illusion that lies ind reality-and the reality that lies behind illusion. Its scope is immensely greater than we once ized. We are no longer satisfied with insights only into particles, or fields of force, or geometry, or n space and time. Today we demand of physics some understanding of existence itself.

References

[1] C. unell: Principles of Geology, being an attempt to explain the former changes of the earth's surfaces, by reference to cause now in operation, Vol. II (London, 1830-1833).
[2] C. Dariwn: us quobed in H. Wakd: Darwin: The Man and His illarjare (Indiamapolis, Ind., 1927), p. 297.
[3] J. A. Wheeler: From relativity to mutability, in ref. [4], pp. 202-247.
[4] J Meura, editor: The Physiovets' Conception of Nuture (Dordrocht, 1973).
[5] M. EIGEN: The origin of biological information, in ref. [4], pp. 594-632.
[6] M. Einen and K. Winkler: Das Spiel: Naturgesetze steuern den Zufall (Mnchen, 1975).
[7] P. S. Laplace: Lissai philosophique sur les probabilits (Paris, 1814), 2nd edition, pip. 3-4.
[8] N. Bonr: Das Quantenpostulat und die neuere Entwicklung der Atomistik, Naturwiss., 16, 245-257 (1928).
[9] W. Herseypere: ber den ausohauliehen Inhalt der quantenthooretiochen Kinematik und Mechanik, Zeits. Phys., 43, 172-198 (1927).
[10] J. Burckhardt: Die Kultur der Renaissance in Italien (Leipzig, 1860); authorized English translation from the 15th edition, by S. G. C. Middlemore: The Civiliza. tion of the Renaissance in Italy (New York, N. Y., 1929).
[11] P. Gay: Style in History (New York, N. Y., 1974).
[12] II. Everett III: The theory of the universal wave function, doctoral dissertation, Princeton University (1957); published in abbreviated form in ref. [13]; published in full for the first time in ref. [14].
[13] H. Everett III: "Relative state" formulation of quantum mechanics, Rev. Mod. Phys., 29,

454-462 (1957); reprinted in ref. [14].
[14] B. S. DeWitt and N. Graham, editors: The Many.Worlds Interpretation of Quantum Mechanics (Princeton, N. J., 1973).
[15] J. vos Neumany: Mathematischen Grundlagen der Quantenmechanik (Berlin, 1932); translated as Mathematical Foundations of Quantum Mechanics (Princeton, N. J., 1955).
[16] J. A. Wheeler: Assessment of Everett's "relative state" formulation of quantum mechanics, Rev. Mod. Phys., 29, 463-465 (1974); reprinted in ref. [14].
[17] E. P. Wigner: Epistemological perspective on quantum theory, in Contemporary Research in the Foundations and Philosophy of Quantum Theory, edited by C. A. Hooker (Dordrecht, 1973), pp. 369-385.
[18] E. P. Wigner: Remarks on the mind-body question, in The Scientist Speculates, edited by I. J. Good (London, 1962), pp. 284-302.
[19] E. P. Wigner: Are we machines?, Proc. Amer. Phil. Soc., 113, 95-101 (1969).
[20] E. P. Wigner: Physics and the explanation of life, Found. Phys., 1, 35.45 (1970).
[21] C. F. von Weizs cker: Classical and quantum decriptions, in ref. [4], pp. 635-667.
[22] J. A. Wheeler: Include the observer in the wave function?, in Quantum Mechanics, a Half Century Later, edited by J. Leite Lopes and M. Paty (Dordrecht, 1977).
[23] N. Bohr: Atomic Theory and the Description of Nature (Cambridge, 1934).
[24] N. Bohr: Atomic Physics and Human Knowledge (New York, N. Y., 1958).
[25] N. Bour: Essays 1958-1962 on Atomic Physics and Human Knovledge (New York, N. Y., 1963).
[26] A. Einstein: Autobiological Notes, in ref. [27], quotation from p. 81.
[27] P. A. Schilpp, cditor: Albert Einstein: Philosopher-Scientist (Evanston, Ill., 1949), and subsequent paperback editions elsewhere. 1949), and subsequent paperback editions elsewhere.
N. Bour: Can quantum-mechanical description of physical reality be considered complete?, Phys. Rev., 48, 696-702 (1935); the quotation comes from p. 697. T. Mann: Freud, Goethe, ii agner (New York, N. Y., 1937), p. 20; traislated by H. T. Lowe-Porter from Freud und die Zukunjt (Vienna, 1936); the cited words were included in the lecture given at the 80 th birthday celebration for Sigmund Freud, 8 May 1936.
C. S. Peirce: The Philosophy of Peirce: Selected Writings, edited by J. Buchler (London, 1940); paperback reprint, Philosophical Writings of Peirce (New York, N. Y., 1955); “fallibilist”, p. 358.
[31] B. K. Harrison, M. Wakano and J. A. Wheeler: Matter-energy at high density; end point of thermonuclear evoiuiion, in La siruciure ei l'volution de l'univers, Onzime conseil de physique Solvay (Bruxelles, 1958), pp. 124-146; terminology “crushing points", pp. 134-136.
[32] J. R. Gott HII, J. E. Gunn, D. N. Schramm and B. M. Tingley: Will the Universe expand torever, Sci. Amer., 234, 62-79 (March 1976); terminology “big crunch ”, p. 69.
[33] J. A. Wheeler: Our universe: the known and the unknown, address before the Amcrican Association for the Advancement of Science, New York, December 29, 1967; Amer. Schoiar, 37, Z48-274 (1968); terminology “black hole i, pp. 258-262.
[34] J. A. Wheeler: Superspace and the nature of quantum geometrodynamics, in Battelle Rencontres: 1967 Lectures in Mathematics and Physics, edited by C. DeVitt and J. A. Wheelen (Now York, N. Y., 1968), pp. 242-307; "no before, no after ", p. 253.
[3.5] W. Shakespeare: The Tempest, London, about 1610; Prospero in Act IV, Scene I, lines 148-158.
[36] J. A. Wheeler: ref. [3]; no magic particle, no magic field, p. 235.
[37] C. Ji. Patton and J. A. Wheelek: Is physics legistaied by vosmogony?, in Quantum Gravity, edited by C. J. Isham, R. Penrose and D. W. Sciama (Oxford, 1975); no magic mathematics, pp. 589-591. Oxford University Press 1975, by permission of Oxford University Press. Appreciation also expressed to Charles Patton for permission to quote cited passages.
[38] A. I. Oparin, editor: Evolutionary Biochemistry, Proceedings of the V International

Congress on Biochemistry (Moscow, 1961; London, 1963), pp. 12-51.
39] G. W. Leibyiz: source of quotation not traced.
[40] J. A. Wheelek: Genesis and Observerstity, ref. [41], pp. 3-33; scc p. 20.
[41] R. E. Butts and K. J. Histikka: Foundational Problems in the Special Sciences (Dordrecht, 1977).
[42] N. Boiir: ref. [23]; Bohr's stick, p. 99.
[43] F. J. Belinfante: Measurements and Time Reversal in Objective Quantum Theory (Oxford, 1975); terminology "indelible", p. 39.
[44] E. P. Wigner: Are we machines?, Proc. Amer. Phil. Soc., 113, 95-101 (1969); quotation from p. 97.
[45] E. P. Wigner: The philosophical problem, in ref. [46], pp. 1-3; quotation from E. P. p. 3.
[46] B. d'Espagnat, editor: Foundations of Quantum Mechanics (New York, N. Y., 1971).
[47] N. Bour : ref. [24]; irreversible amplification, p. 88.
[48] N. Bohr: ref. [24]; closed by irreversible amplification, p. 73.
[49] N. Bohr: ref. [25]; plain language, p. 3.
[50] N. Bohr: ref. [25]; unambiguously communicable, pp. 5, 6.
[51] J. Kalckar: letter to J. A. Wheeler dated June 10, 1977. Appreciation is expressed here to Dr. J. Kalckar both for the letter and for subsequent permission to quote from it. He adds that he cannot guarantee to have correct wording; and that Bohr's reply, as so often, was a joke with a definite "point"-hence ", Bonn , wo point to then seriously, hut not quile seriously.
[52] K. R. Popper and J. C. Eccles: The Self and Its Brain (Berlin, Now York, N. Y., and London, 1977); see especially pp. 207-208, 438-440 and 515.
[53] J. von Neumann: The Computer and the Brain (New Haven, Conn., 1958); see especially pp. 60-61.
[54] L. N. Cooper: A possible organization of animal memory and learning, in Nobel Symposium on the Collective Properties of Physical Systems, edited by B. Lundqvist and S. Lundqvist (New York, N. Y., 1973), pp. 252-264.
[55] M. M. Nass and L. N. Coopent: A iteory for ihe developmeni of jeaiure-deieciing cells in visual cortex, Biol. Cyber., 19, 1-18 (1975).
[56] L. N. Cooper : A theory for the acquisition of animal memory, in Lepton and Hadron Stuwcture (1974 International School of Subnuclear Phyeice, Evice, Trapani, Sicily: July 14-31, 1974), edited by A. Zichichi (New York, N. Y., 1975), pp. 808-839.
7] G. E. PUGH: On the Origin of Human Values (New York, N. Y., 1976), chapter "Human values, free will, and the conscious mind"; preprinted in Zygon, 11, $2 - 24$ (1976).
[58] International Union of Pure and Applied Physics: Report of the Commission on Symbols, Units and Nomenclature (Amsterdam, 1948).
[59] J. A. Wheeler: The "past" and the "delayed-choice" double-slit experiment, in ref. [60].
[60] A. R. Marlow, editor: Mathematical Foundations of Quantum Theory (New York, N. Y., 1978).
[61] E. H. Gombrich: Art and Illusion: A Study in the Psychology of Pictorial Representation (Princeton, N. J., 1961), 2nd edition, revised, p. 394. Appreciation is expressed to Prof. E. II. Gombricin and Primeton Viversity Press for permission to quote cited passages in the text.
[62] E. H. Gombrich: ref. [61], p. 273.
[63] E. H. Gombrich: ref. [61], p. 329.
[64] A. Einstein, B. Podolsky and N. Rosen: Can quantum-mechanical deseription of physical reality be considered complete?, Phys. Rev., 47, 777-780 (1935).
[65] R. M. F. Houtappel, H. Van Dam and E. P. Wigner: The conceptual basis and use of the geometric invariance principles, Rev. Mod. Phys., 37, 595-632 (1965); see especially so 4.1-4.5 on pip. 610-616.
[66] C. N. Yang and R. L. Mills: Conservation of isotopic spin and isotopic gauge invariance,

Phys. Rev., 96, 191-195 (1954).
[67] S. Hojman, K. Kuchar and C. Teitelbom: New approach to general relativity, Nature Phys. Sci., 245, 97-98 (1973).
[68] S. A. Hojman, K. Kucha and C. Teitelboim: Geometrodynamics regained, Ann. of Phys., 76, 88-135 (1976).
[69] C. Teitelboim: Surface deformations, space-time structure and gauge invariance, in Relativity, Fields, Strings and Gravity: Proceedings of the Second Latin American Symposium on Relativity and Gravitation SILARG II held in Caracas, December 1975, Universidad Simon Bolivar, edited by C. Aragone (Caracas, 1976).
[70] J. E. Nelson and C. Teitelbom: Hamiltonian for the Einstein-Dirac field, Phys. Lett., 69 B, 81 − 84 (1977).
[71] J. A. Wifeeler: ref. [3]; machinery lidden, pp. 236-240.
[72] J. A. Wheeler: Beyond the end of time, Marchon lecture, University of Newcastle Upon Tyne, May 18, 1971, and Nuffield Iecture, Cambridge University,

25 II Interpretations of the Act of Measurement

25.1 II. 1 the Theory of Observation in Quantum Mechanics by London, Bauer

25.1.1 Introduction

Preface of Paul Langevin

Quantum physics has brought an essential advance to science, the finding that in every experiment or measurement there inescapably enters the duality between subject and object, the action and reaction of observer and system observed, the observer and the measuring apparatus being viewable as one entity.

The classical view, disregarding the necessarily limited character of our knowledge and the retroactive effect of the measurement on the system observed, always postulated the possibility of an infinitely precise knowledge of the simultaneous values of all the parameters used for the description of the system. Heisenberg, in giving concrete significance to his principle of indeterminism, has shown how the

Originally published as La thorie de l'observation en mcanique quantique, No. 775 of Actualits scientifiques et industrielles: Exposs de physique gnrale, publis sous la direction de Paul Langevin, Hermann, Paris (1939). English translations-including a new paragraph by Professor Fritz Londondone independently by A. Shimony, and by J. A. Wheeler and W. H. Zurek, and by J. McGrath and S. McLean McGrath; reconciled in 1982. Copyright 1982 by Princeton University Press.
very existence of quanta excludes the possibility of knowing precisely at the same time all the quantities which might be the object of our measurement.

The form in which quantum mechanics is presented today provides an admirable translation of this new situation. The wave function it uses to describe the object no longer depends solely on the object, as was the case in the classical representation, but, above all, states what the observer knows and what, in consequence, are his possibilities for predictions about the evolution of the object. For a given object, this function, consequently, is modified in accordance with the information possessed by the observer. The introduction of the wave function at the very foundation of our representation common-sensibly recognizes what is almost ignored by classical physics, that our possibilities for prediction depend, above al, on our information. It also expresses quite exactly the fact that certain quantities, called noncommutable, cannot be

known simultaneously with complete certainty. It characterizes the system by a certain number of observable quantities, different forms of "maximum knowledge" corresponding to different so-called "pure cases."

The present work, where the authors expand lectures given by one of them at the Sorbonne, demonstrates the precision and clarity with which the formalism of quantum theory expresses this representation by the wave function of the information acquired by the observer, and the manner in which each new measurement intervenes to modify this representation.

The act of observation is analyzed here in a particularly penetrating way. The essential character of the new physics emerges with complete clarity in the two stages of change of the wave function: by coupling of the system observed with the measuring device; and by the intervention of the observer, who becomes aware of the result of the measurement and thus determines the new wave functionfollowing the observation-by using the new datum to reconstitute his information bank.

This treatise does a valuable servicc. It brings out the important finding of the new physics: how we express our knowledge of the external world.

Authors' Preface

The majority of introductions to quantum mechanics follow a rather dogmatic path from the moment that they reach the statistical interpretation of the theory. In general, they are content to show by more or less intuitive considerations how the actual measuring devices always introduce an element of indeterminism, as this interpretation demands. However, care is rarely taken to verify explicitly that the formalism of the theory, applied to that special process which constitutes the measurement, truly implies a transition of the system under study to a state of affairs less fully determined than before. A certain uneasiness arises. One does not see exactly with what right and up to what point one may, in spite of this loss of determinism, attribute to the system an appropriate state of its own. Physicists are
to some extent sleepwalkers, who try to avoid such issues and are accustomed to concentrate on concrete problems. But it is exactly these questions of principle which nevertheiess interest nonphysicists and all who wish to understand what modern physics says about the analysis of the act of observation itself

Although these problems have already been the subject of deep discussions (see especially von Neumann, 1932), there does not yet exist a treatment both concise and simple. This gap we have tried to fill.

Paris, June 1939

Introduction

It is well known that theoretical physics has been transformed since the beginning of the century into an essentially statistical doctrine and that the discovery of quanta made this revolution inevitable.

The principal aim of this study will be the statistical interpretation of the formalism of quantum theory. Although these questions of interpretation were systematized about ten years ago (Heisenberg, 1927; von Neumann, 1927; Dirac, 1927), one still often meets rather fuzzy ideas about what it means that probabilities appeai in moderin physics.

According to some, this statistical character shows that our knowledge of laws at the atomic level is still incomplete: that there remain to be found some hidden parameters, determining those processes which, provisionally, we are content to describe in a statistical language. To believe them, one might hope some day to recast the theory in a deterministic mold.

Others would have it understood that the action of the observer is involved. They sometimes consider that this would be an action that is causal, but incompletely known, because one never

knows the exact state of the observer. From this circumstance would arise the statistical spread of measurements, the exact results of which might be predictable if one could take better account of the intervention of the observer.

It has also been said that the law of causality may be correct but inapplicable because there is never any way to reproduce identical conditions.

The discussion of these questions is not at all a matter of speculation. It is a definite problem. To treat it one ought to apply quantum theory to-and thereby extract the central features of - the very process of measurement. One can convince oneself that statistical distributions, such as are given by quantum mechanics and verified by experiment, have such a structure that they cannot be reproduced by hidden parameters. It is not, as often claimed, a question of philosophical interpretation; quantum mechanics ought to be testably false, if atomic processes in fact were deterministic and only incompletely known. It would be necessary to change the theory fundamentally and give up some battle-tested results, if one wished to reconstitute it on a deterministic basis. Causality is no longer applicable, it is true; but the reason for this fact is not the impossibility, in the last analysis, of reproducing identically the conditions of an experiment. The heart of the matter is the difficulty of separating the object and the observer.

Modern physics often advances only by sacrificing some of our traditional philosophical convictions. The case of quantum mechanics is especially instructive. In all innocence one sought to construct a theory which would contain only relations between the "observable" quantities of Bohr's theory, such as the frequencies and the intensities of spectral lines. Heisenberg followed this route and in this way succeeded in obtaining a formalism which would resolve this problem. But, as often happens in theoretical physics, the formalism of the theory, once established, carried one further than one expected. It implied more relations than its founders had started with, relations between quantities altogether disconnected from the original spectroscopy, but themselves also observable (coordinates, momenta, etc.). One was led quite naturally in this way to try-after the initial shock-to interpret these relations which had been exposed automatically by the theory. In this way the discussion of this formalism taught us that the apparent philosophical point of departure of the theory, the idea of an observable world, totally independent of the observer, was a vacuous idea. Without intending to set up a theory of knowledge, alihough they were guided by a rather quesiionable philosophy, physicists were so to speak trapped in spite of themselves into discovering that the formalism of quantum mechanics already implies a well-defined theory of the relation between the object and the observer, a relation quite different from that implicit in naive realism, which had seemed, untii then, one of the indispensable foundation stones of every natural science.

To discuss the process of measurement it is necessary to consider at least two systems, the observer and the object. It is therefore necessary to apply the quantum theory of the many-body system. This exists at present only in the nonrelativistic approximation. We are therefore forced to limit ourselves to this approximation, which still neglects all effects of the time delay in the propagation of forces.

It is not possible to give here a detailed introduction to quantum mechanics. We will limit ourselves (§I and 2) to recalling briefly, and a bit dogmatically, the definitions and the laws that we will need. For a more detailed exposition of quantum theory see, for example, de Broglie, 1930; Bloch, 1930; Kemble, 1937; Dushman, 1938.

25.1.2 §1. Resum of the Principles of Quantum Physics

In atomic physics the use of statistical concepts came far earlier than wave mechanics. The first step in this direction was probably made at the moment when one described spontaneous radioactive decay by the laws of probability. Of course, at the beginning we thought that this

was a provisional approach, forced by our
ignorance of what is going on inside the nucleus. But when Bohr, obviously guided by an analogy with statistical concepts, constructed his model of the atom with its spontaneous quantum jumps, and, above ail, when Einstein gave his famous demonstration of Planck's radiation law on the basis of the idea of spontaneous and stimulated transition probabilities (Einstein's A and B coefficients), one already had the strong feeling that these probabilities ought to be something basic and primordial. In a world of discontinuous phenomena, the appearance of a statistical form for the elementary laws would seem almost inescapable. The theory of Bohr, although it does not yet furnish a mathematical scheme that is complete and coherent, has already allowed us to state questions of principle to which quantum theory must address itself. In a physics that deals with magnitudes, whose domains of variation are not necessarily continuous, one wants to know:
(1) What are the possible values of a physical quantity;
(2) With what probabilities are they realized in a given system and under given circumstances.

Quantum mechanics furnishes us with a precise scheme which allows a quantitative treatment of questions of this kind. We can summarize it in the following way:
"The state" of a system-given in classical mechanics at each instant t by the $2f$ values of the variables $q_1(t), q_2(t) \dots q_f(t), p_1(t), p_2(t) \dots p_f(t)$-is represented in quantum mechanics by a complex function of the f variables $q_1, q_2 \dots q_f$ and of t, the "Schrödinger wave function"

$$\psi\left(q_1, q_2 \dots q_f; t\right)$$

which is normalized in such a way that*

$$\int \psi\psi^* dq = 1 \tag{1}$$

The evolution of the system in time is governed in classical mechanics by a "Hamiltonian function" $H(q,p)$, characteristic of the system in question. This function of the coordinates $q_1, q_2 \dots q_f$ and of the momenta $p_1, p_2 \dots p_f$, which is nothing other than the energy, permits one to write the Hamiltonian equations of motion. This is essentially † the same function $H(q,p)$ which in quantum mechanics also gives the law of evolution of the ψ that represents the state of the system: one forms the operator ‡$H(q, -i\hbar\partial/\partial q)$ by replacing p_k in the Hamiltonian

- In what follows the integrals $\int dq$ are always taken over the entire configuration space $q_1, q_2 \dots q_f$, and ψ^* is the complex coniugate of ψ
  † Completed by a term referring to "spin."
  ‡Here the symbol $h/2\pi$ employed by London and Bauer has been replaced for convenience, and in accord with modern practice, by the Dirac notation for the quantum of angular momentum. h. –Eds.
  by the differential operator $-i\hbar\partial/\partial q_k$ and q_k by the operation of multiplication by q_k. Here a certain ambiguity enters in the ordering of factors, because the operations q_k and $\hat{\partial}/\hat{\partial} q_k$ are not commutabie. It is enough for us to know that there are prescriptions which ordinarily suffice to determine uniquely the order of the opcrators, but we will not go into this in detail here. The operator $H(q, -i\hbar\partial/\partial q)$, once given, allows us to write the equation of evolution: §

$$H(q, -i\hbar\partial/\partial q)\psi = i\hbar\psi\partial/\partial t. \tag{2}$$

This equation, discovered by Schrödinger, has the important property of leaving invariant the integral $\int \psi\psi^* dq$, which is necessary for our normalization $\int \psi\psi^* dq = 1$ to be possible. Thus ψ, once normalized, always retains its nomalization.

$\psi(q, t_0)$ represents a "state" of the system at an instant t_0. Here we take this term in a sense completely analogous to that which it has in classical mechanics, where one says that the data $q_1(t_0) \cdots q_f(t_0), p_1(t_0) \cdots p_f(t_0)$ "represent a state." The knowledge of the representative of the state at a given instant is necessary and sufficient for an unambiguous calculation, with the aid of the dynamic law, of the representative of the state at every subsequent moment. We cannot forgo a part of these data without losing the ability to calculate the future. Neither can we add to them supplementary data withoui iniroducing useiess tautoiogies or contradictions of the data already in hand.

The stationary states of Bohr correspond to special solutions of the Schrödinger equation, solutions exactly periodic in time and of the form:

$$\psi = \exp(-iEt/\hbar)u(q). \tag{3}$$

In consequence of (1) and (2) the "amplitude" $u(q)$ obeys a time-independent equation,

$$Hu = Eu, \tag{4}$$

and the condition of normalization,

$$\int uu^* dq = 1 \tag{5}$$

The pair of equations (4) and (5) ordinarily does not have a solution for every value of E. They present a "proper value" or "eigenvalue" or "characteristic value" problem. Only for a "spectrum" of special values $E_1, E_2, E_3 \ldots$, possibly also

[8] In accordance with present-day practice we omit the square brackets in which the authors enclose the left-hand side of this and subsequent similar equations; and we use on the right-hand side the opposite sign of i from that which they use whenever they write the time-evolution operator. –Eds.

containing continuous intervals,* can condition (5) be fulfilled. For other values of E the linear equation (4) of course also possesses solutions u containing an arbitrary factor; but they are not square integrable, ruling out the momalization (5).

The allowed values,

$$E_1, E_2, \ldots E_k, \ldots$$

are called the "eigenvalues" of the operator H. The corresponding solutions u are called "eigenfunctions" and designated by corresponding indices,

$$u_1, u_2, \ldots u_k, \ldots$$

It was the fundamental idea of Schrödinger to identify the spectrum of eigenvalues, $E_1, E_2, \ldots$, which have the dimensions of energy, with the allowed values of the energy in Bohr's theory, and the success of this ingenious idea is well known.

One knows also that the founders of wave mechanics were guided in the beginning by the conviction that it was necessary to get rid of discontinuities, or rather to derive them from an essentially continuous substructure, from a ficld theory, and thus overturn the basically statistical picture of Bohr and Einstein. But this program did not turn out to be realizable.

The statistical interpretation of quantum mechanics may be considered to be a particularly conservative attempt to maintain the picture worked out by Bohr and Einstein and to embody it in a coherent theoretical system.

Now that we know how to interpret the "monochromatic" solutions of the wave equation (2) such as

$$\psi = \exp(-iE_k t/\hbar)\, u_k(q)$$

as describing a state of energy E_k, we have to discover the meaning of the most general solutions. One can show that if one limits oneself to square integrable functions (1), the most general solution of equation (2) is written in the form:

$$\psi = \sum_k c_k \exp(-iE_k t/\hbar)\, u_k(q) \tag{6}$$

where the c_k are complex constants.
Born, replying to this question, formulated the foundations of the statistical interpretation of quantum theory. He postulated that the quantity $|c_k|^2$ gives the

- In the case of a continuous spectrum condition, (5) has to be imposed on a function u associated with a small interval of E of the continuum ("proper differential"). In what follows we will not take account of these sophistications, which do not concern questions of principle, and we will write all formulas as if there were nothing but discrete spectra. probability of finding the value E_k of the energy when the system in the state (6) is subjected to a measurement of energy.

If we introduce the abbreviation* $\psi_k - c_k \exp(-iE_k t/\hbar)$, we can write

$$\psi = \sum_k \psi_k(t) u_k(q). \tag{6'}$$

The coefficients ψ_k depend only on the time, and, as $|\psi_k|^2 = |c_k|^2$, we can also interpret the quantity $|\psi_k(t)|^2$ as the probability of finding the value E_k for the energy in the state ψ.

The coefficients ψ_k may, moreover, be calculated very easily with the help of two basic properties of eigenfunctions:
(1) "Orthogonality":

$$\int u_k^* u_l dq = \delta_{kl} \tag{7}$$

where

$$\delta_{kl} = \left\{ \begin{array}{l} 1 \text{ if } k = l \\ 0 \text{ if } k \neq l \end{array} \right\};$$

(2) "Completeness": for an arbitrary square integrable function $f(q)$ (that is, $\int f^* f dq =$ finite) one has the identity:

$$\sum_k \left| \int f u_k dq \right|^2 = \int f^* f dq \tag{8}$$

Orthogonality immediately gives the form of the coefficients ψ_k of the expansion (6′). Multiplying (6′) by u_l^* and integrating, one obtains:

$$\int \psi(\bar{q}) u_l^*(\bar{q}) d\tilde{q} - \psi_l. \tag{9}$$

Completeness guarantees that the series thus defined converges to the function $\psi(q)$. Thus, the integral of the square of the absolute value of the difference,

$$\psi(q) - \sum \psi_i u_i(q),$$

goes to zero,

- Not a customary abbreviation and one possibly confusing to the reader, but well adapted to the purpose of the next few sections. -Eds.

$$\int \left| \psi(q) \sum_l \psi_i u_l(q) \right|^2 dq = \int \psi^* \psi^* dq - \sum_l \psi_l \int \psi^* u_l dq - \sum_l \psi_l^* \int \psi_u^* dq + \sum_l \psi_i \psi_l^*$$
$$= \int \psi_l \psi^* dq - \sum_l \left| \int \psi_{ll}^* dq \right|^2 = 0$$

from which also follows the result

$$\sum_l \psi_l \psi_l^* = \int \psi \psi^* dq = 1$$

In other words, the sum of the probabilities of finding the various values of the energy is unity. Thus if we ask what is the energy, we can be assured of always finding some value. Naturally, it is necessary that things be so if the definitions of Born are to make sense.

Thus we see how, for energy at least, quantum theory answers the two questions which show up (first paragraph of §1) in every theory of the discontinuous:

1. The possible values of the energy are the eigenvalues $E_1, E_2, E_3, \ldots$ of the operator $H(q, -i\hbar\partial/\partial q)$.

2. The probability of finding the value E_k of the energy in the state represented by ψ is given by

$$\text{Prob}_\psi (E_k) = \left| \int \psi u_k^* dq \right|^2, \tag{10}$$

where u_k is the eigenfunction associated with the value E_k of the energy.

In particular, if by chance this state is represented by an eigenfunction of the energy; that is, if

$$\psi = u_k$$

then equation (10) gives the probabilities 1 for the eigenvalue E_k and 0 for all other eigenvalues of the energy.

In the original theory of Bohr one was occupied above all with the energy. However, in our present formalism energy does not play an exceptional part except for the time-evolution of the state as represented by its ψ function (equation 2). If ψ is given at a certain instant, we can also look for statistical predictions for an arbitrary physical quantity $F(q, p)$ at that moment.

The generalization of our definitions for other quantities $F(q, p)$ (as, for example, $xp_y - yp_x, x, p_x$, etc.) is fully specified as follows.

We form the operator $F(q, -i\hbar\hat{c}/\partial q)$ and define, with the help of the equations of the eigenvalue problem,

$$Fv(q) = fv(q)$$
$$\int ww^* dq = 1 \tag{11}$$

the eigenvalues $f_1, f_2, \ldots f_\rho \ldots$ of the operator F and the corresponding eigenfunctions $v_1, v_2, \ldots v_\rho \ldots$ Mathematicians have shown that these eigenfunctions, too, under rather general conditions, form a complete system of orthogonal functions; that is, that we have the relations

$$\int v_\rho v_\sigma^* dq = \delta_{\rho\sigma} \tag{12}$$

and that we can expand the function ψ at a given moment t_0 in a convergent series of these functions v_ρ

$$\psi\,(q, t_0) = \sum_\rho \psi_\rho\,(t_0)\, v_\rho(q),$$

where

$$\psi_\rho\,(t_\mathrm{o}) = \int \psi\,(q, t_\mathrm{o})\, v_\rho^*(q) dq$$

The generalization of our previous definitions is immediate:

1. The possible values of the physical quantity F are given by the eigenvalues of the operator $F(q, -i\hbar\partial/\partial q)$.

2. The probability for finding the eigenvalue f_ρ of the quantity $F(q, p)$ for the state represented by ψ is given by

$$\mathrm{Proh}_\psi\,(f_\rho) = \left| \int \psi\,(q, t_0)\, v_\rho^*(q) dq \right|^2 = |\psi_\rho|^2 \tag{13}$$

In particular, if by chance the state is represented by the eigenfunction v_ρ of F; that is, if

$$\psi = v_\rho$$

one obtains the probability 1 for finding the value f_ρ of the quantity F and 0 for the probability for every other eigenvalue.

From these definitions immediately follows the mean value of F in the state ψ,

$$\mathrm{Mean}_\psi(F) = \sum_\rho |\psi_\rho|^2 f_\rho \tag{14}$$

This expression can be written in a more convenient form, which allows one to calculate immediately the mean value without having to go back to an explicit
evaluation of the individual eigenvalues f_ρ or the expansion of ψ as a series in the eigenfunctions v_ρ. One easily checks that

$$\mathrm{Mean}_\psi(I) = \int \psi^* F \psi dq \tag{I}$$

because, as consequence of (11) and (12) this expression lets itself be written as

$$\int \sum_{\rho\sigma} \psi_\rho^* v_\rho^* F \psi_\sigma v_\sigma dq = \sum_{\rho\sigma} \psi_\rho^* \psi_\sigma \int v_\rho^* f_\sigma v_\sigma dq = \sum_{\rho\sigma} \psi_\rho^* \psi_\sigma f_\sigma \delta_{\rho\sigma}$$

25.1.3 §2. Vector Notation

Our definitions are now complete. We have only to introduce a slightly more convenient notation, that of the language of vectors.

Vectors. We will say that the function $\psi(q)$, representing the instantaneous state of a system, is a "vector" in a space of an infinite number of dimensions, the function space of Hilbert. The integral of the product of the two functions ψ^* and $\underset{\psi}{\phi}$ taken over all coordinates $q_1, q_2 \ldots q_f$ will be called the "scalar product of ψ and ϕ,"

$$(\psi, \phi) = \int \psi^*(q)\phi(q)dq = \sum_\rho \psi^*_\rho \phi_\rho \tag{1}$$

The quantity $(\psi, \psi) = \int \psi^*\psi dq = \sum_\rho |\psi_\rho|^2$ will be called the square of the length of the vector.
$(\psi, \phi) = 0$ means that the vectors ψ and ϕ are "orthogonal."
The eigenfunctions $v_1, v_2 \ldots v_\rho \ldots$ of an operator F satisfy the relation (§1, equation 12),

$$(v_\rho, v_\sigma) = \left\{ \begin{array}{l} 1 \text{ if } \rho = \sigma \\ 0 \text{ if } \rho \neq \sigma \end{array} \right\}$$

They form therefore a system of orthogonal unit vectors that define an "orthogonal coordinate system" with the help of which one can represent any vector ψ whatsoever in the form,

$$\psi(q) = \sum_\rho \psi_\rho v_\rho(q) \tag{1}$$

The "components" ψ_ρ of the vector ψ are defined by the "projection"

- Both equations are numbered (1), presumably an oversight. –Eds.

$$\psi_\rho = (v_\rho, \psi)$$

of ψ in the direction of the unit vector v_ρ.
This decomposition into components is quite analogous to the resolution of a vector in ordinary space into projections. We can consider the set of ψ_ρ as equivalent to the function $\psi(q)$ itself; it is one particular decomposition of the vector ψ into orthogonal components. The coefficients

$$\psi_k = (u_k, \psi)$$

give an analogous decomposition of the same vector with respect to another system of orthogonal axes $i_1, i_2 \ldots i_k, \ldots$.

The representation of ψ by itself, that is, the function $\psi(q)$, may be regarded as a special case of representation in terms of orthogonal components-specifically, the orthogonal system composed of the eigenfunctions of the particular operator $F = q$. The cigenvalue problem for this operator has the form,

$$qv_\alpha(q) = q_\alpha v_\alpha(q)$$

or

$$(q - q_x)\, v_x(q) = 0$$

The solutions are the "limiting" or symbolic functions of Dirac,

$$v_\alpha(q) = \delta\,(q - q_\alpha)$$

Such a function by definition vanishes for $q \neq q_\alpha$ but for $q = q_\alpha$ is so singular that

$$\int \delta\,(q - q_\alpha)\,dq = 1$$

In terms of these special eigenfunctions one obtains for $\psi(q)$ the trivial expansion,

$$\psi(q) = \sum_\alpha \psi\,(q_\alpha)\,\delta\,(q - q_\alpha)$$

where the

$$\psi\,(q_\alpha) = \int \psi(q)\delta\,(q - q_\alpha)$$

are the coefficients in the expansion.
From our general definitions thus follows the particular result,
$|\psi(q)|^2 dq =$ (probability to find q in the interval from q to $q + dq$).

Tensors. In the present picture the typical operator $F(q, -i\hbar\delta/\partial q)$, representing a physical quantity, is a tensor; inat is, a linear transformation of vectors. Applied to a vector ψ, it transforms it into another vector,

$$\psi' = F\psi$$

It is linear because, for every combination of multiplications and differentiations, one always has the distributive relation,

$$F(\psi + \chi) = F\psi + F\chi \tag{2}$$

and because, for every constant c, one has

$$\bar{F}c\dot{\psi} = c\bar{F}\dot{\psi}$$

As it represents a real (noncomplex) physical quantity, it has one more important property,

$$(\phi, F\psi) = (\psi, F\phi)^*. \tag{3}$$

Such an operator is ichmed "Hermitia." Rclation (3) is easily demonstrated by an integration by parts that takes account of the facts that every operation of differentiation contained in F brings in a factor i, and that F, considered as a function of q and $-i\hbar\partial/\partial q$, is a real function.

When we are using for ψ a representation in terms of the ψ_k that is, when we refer the state vector to a system of coordinates $u_1, u_2 \ldots u_k \ldots$, we must also decompose the operator F into components referred to the same coordinates. In this way F evidently finds itself expressed as the linear transformation brought about by the matrix

$$F_{kl} = \int u_k^* F u_l dq = (u_k, F u_l) \tag{4}$$

Thus if one applies this transformation to a vector ψ_l,

$$\sum_l F_{kl}\psi_l = \left(u_k, F\sum_l \psi_l u_l\right) = (u_k, F\psi)$$

one obtains the k th component of the function $F\psi$.
From (3) immediately follows the relation

$$F_{kl} = F^*_{lk} \tag{5}$$

of "Hermitian matrices."
There is a system of coordinates in which the matrix representing the operator
F shows an especially simple form. These are the coordinates defined by the eigenfunctions $v_1 \cdots v_\rho \cdots$ of this operator itseif. in terms of them one finds,

$$\Gamma_{\rho\sigma} = (v_\rho, Fv_\sigma) - f_\sigma (v_\rho, v_\sigma) - f_\sigma \mathcal{E}_{\rho\sigma} = \left\{ \begin{array}{l} f_\sigma \text{ for } \sigma = \rho \\ 0 \text{ for } \sigma \neq \rho \end{array} \right\}.$$

In its "eigen"-basis the matrix F therefore takes a diagonal form and its diagonal elements are the eigenvalues of F,

$$F_{\rho\sigma} = \left\| \begin{array}{ccccc} f_1 & 0 & 0 & 0 & \cdots \\ 0 & f_2 & 0 & 0 & \cdots \\ 0 & 0 & f_3 & 0 & \cdots \\ 0 & 0 & 0 & f_4 & \cdots \\ \cdots & \cdots & \cdots & & \\ \cdots & \cdots & \cdots & & \end{array} \right\| \tag{6}$$

In the system of coordinates ψ_ρ used to cxpand ψ in a series of eigenfunctions $v_1 \cdots v_\rho \cdots$ of an arbitrary operator F, the Hamiltonian operator H takes the form $H_{\rho\sigma} = (v_\rho, Hv_\sigma)$ and the Schrödinger equation becomes

$$\sum_\rho H_{\rho\sigma}\dot{\psi}_\sigma = i\boldsymbol{h}\dot{\psi}_\rho \tag{7}$$

the discontinuous form in which Heiscnberg, Born, and Jordan found the cquations of quantum mechanics in the first place.

Invariants. We use capital letters H, F, etc. for tensors, and Greek letters ψ, ϕ, etc. for vectors. We can then suppress indices (or arguments) associated with any special decomposition into components and write (7) in an invariant form, independent of the system of coordinates, or rather encompassing all possible systems (see §1, equation 2),

$$H\psi = i\hbar\dot{\psi}$$

Two distinct representations of the same vector ψ, for example $\psi_k = (u_k, \psi)$ and $\psi_\rho = (v_\rho, \psi)$, are related by a linear transformation,

$$\psi_k = \sum_\rho S_{k\rho}\psi_\rho \quad \text{with} \quad S_{k\rho} = (u_k, v_\rho) \tag{8}$$

Thus, as $\psi = \sum_\rho v_\rho (v_\rho, \psi)$, one has,

$$\psi_k = (u_k, \psi) = \sum_\rho (u_k, v_\rho)(v_\rho, \psi) = \sum_\rho S_{k\rho}\psi_\rho$$

For the coefficients $S_{k\rho}$ one easily finds the relations,

$$\sum_\rho S_{k\rho}S^*_{l\rho} = \delta_{kl} \quad \text{or} \quad S\tilde{S}^* = 1 \tag{9}$$

where $\tilde{S}_{k\rho} = S_{\rho k}$.
These relations characterize the transformation (8) as a "unitary" transformation. Two different

representations of the same tensor F, for example $F_{kl} = (u_k, Fu_l)$ and $F_{ps} = (u_p, Fu_a)$, are related, as one easily verifies, by the relations,

$$\mathrm{F}_{kl} = \sum_{\rho\sigma} \mathrm{S}_{k\rho}\, \mathrm{F}_{\rho\sigma} \widetilde{\mathrm{S}}^*_{\sigma l}$$

Thus, as $u_\kappa = \sum_\rho v_\rho\,(v_\rho u_\kappa) = \sum_\rho S^*_{\kappa\rho} v_\rho$, one has

$$F_{hi} = (u_h, Fu_l) = \int \sum_\rho S_{h\bar{\mu}} v^*_{\bar{\mu}} F \sum_\sigma S^*_{l\bar{\nu}} v_{\bar{\nu}} dq = \sum_{\rho\sigma} S_{h\bar{\mu}} \int v^*_{\bar{\mu}} F v_{\bar{\nu}} dq S^*_{l\bar{\nu}}$$
$$= \sum_{\rho\sigma} S_{k\rho} F_{\rho\sigma} \tilde{S}^*_{\sigma l}$$

Physically significant numerical values naturally ought to be scalars invariant under these unitary transformations. The unly scalar invaniants that we will meet are the "scalar product" of two vectors ψ and ϕ,

$$(\psi, \phi) = \int \psi^*(q)\phi(q)dq = \sum_k \psi^*_k \phi_k = \sum_\rho \psi^*_\rho \phi_\rho$$

and the "trace" of a tensor F_{kl},

$$\mathrm{Trace}(F) = \sum_k F_{kk} = \sum_\rho F_{\rho\rho}$$

Thus, for example, mean value of a physical quantity F in a state ψ is given in invariant form by the scalar product

$$\mathrm{Mean}_\psi(F) = \sum_k F_{kk} = \sum_\rho F_{\rho\rho}$$

The other results of the theory can also be expressed in invariant form. We will come back to this in §5.

The scalar product can also be considered as the trace of a special matrix ($\psi \times \phi$) defined by

$$(\psi \times \phi)_{k\rho} = \psi^*_k \phi_\rho \tag{10}$$

termed the "direct product" of the vectors ψ and ϕ.

25.1.4 §3. Statistics and Objectivity

Already in the classic memoir (Born, 1926) where he proposed foundations for the statistical interpretation of quantum mechanics, Born remarked that the probabilities which he introduced there must have a strange character, quite different from what one normally understands when one speaks of probability.

This feature he expressed in a form a bit paradoxical: "Although the movements of particles are not determined, except by probabilities, these probabilities themselves evolve according to a causal law." What he understands here by "causal law" is a connection between the "states" at different moments, such that a knowledge of the initial state at an arhitrary instant uniquely implies a knowledge of the state at every subsequent time. A "state," on the other hand, is a well-defined collection of data on the system in question at a given moment.

Naturally, there is no way of predicting a priori whether, in a given domain of science, there exist causal laws as so defined, nor what are the necessary and sufficient conditions for

giving rise to such laws. If one does not end up with unique predictions, if one finds oneself forced to be satisfied with probabilities, that may be either because our knowledge of the "state" is not yet compiete or because causality does not hold. But conversely, when one has succeeded in establishing causal laws, that is evidently a criterion for deciding that one has attained a complete knowledge of the object in question and thus, in some measure, a maximum description.

But the Schrödinger equation has all the features of a causal connection. If the ψ function is known at a given moment, it is determined at every subsequent time. It therefore seems difficult to believe that this function nevertheless contains a statistical collection. At first sight it seems impossible to avoid the following dilemma.

1. One might imagine that the ψ function has the character of the ordinary probability function such as one uses, for example, to describe Brownian motion. A function of this type contains certain statistical predictions that we can test. We then verify which of the possibilities foreseen in the theory is realized in fact in a given case. After this observation we are naturally entitled to use, for the subsequent predictions, the knowledge thus obtained and to replace our original probability function by a function of the same type, but better tuned. Evidently this is only possible by virtue of the enrichment of our knowledge, which is always partial. Of course we do not claim that the object itself has changed its state as a consequence of our observation. All that has changed is the discrepancy between our knowledge and the object. In this case the ψ function will therefore represent the state of our partial knowledge of the object and not the state of the object itself.

2. Imagine, on the contrary, that the ψ function has an "objective" character, as, for example the wave functions of optics. It then claims to represent, in an idealized and simplified form, something complete, a maximum picture of the state
of the object. But if this is the situation, it seems difficult to understand how this ψ function implies a statistic. If one checks experimentally predictions that can be made from it, and if one observes which of the possible outcomes is realized-an outcome predicted by the theory, but only with a certain probability—by what right can we add this new knowledge to the supposedly complete knowledge that we already had?

Heisenberg found the solution to this dilemma. He emphasized that it is the process of measurement itself which introduces the element of indeterminacy in the state of the object.

Thus the statistical feature would not show up except on the occasion of a measurement. If the ψ function gives us probabilities, it does so only in anticipation of un evential measurement. Thus these are only, so to speak, "potential" probabilities which come into force only on the occasion of an actual measurement. They do not affect the precision with which the state of the system is currently known; thus it is already maximal when the ψ function is given.

Of course it may happen that there is an additional uncertainty in the state of the system-that is, in the ψ function itself. In this case it is a question of probabilities in the ordinary sense of the word. They arise from an incomplete knowledge of the state of the object. It is necessary to distinguish clearly between these provabilities and the "potential" probabilitics furnished by ψ functions.

25.1.5 §4. Mixtures and Pure States

That an essential distinction is in question can be seen most clearly by an example.
I. Let us consider first the case where the system is represented by a wave function,

$$\psi = \sum_k \psi_k u_k(q)$$

where $u_1, u_2 \cdots u_k \cdots$ are, for example, eigenfunctions of the energy. We know that the quantity $|\psi_k|^2$ gives us the probability of finding the value E_k of the energy when an energy measurement is made on a system in a state ψ.

II. It has often been considered that this case corresponds straightforwardly to a virtual ensemble of identical systems in different states possessing respectively energies $E_1, E_2 \ldots E_k \ldots$, each one of them being contained in an ensemble with a relative weight $p_k = |\psi_k|^2$.

However, this latter case (II), which will interest us also, is basically different from the pure state (**I**) represented by a single function ψ. It is a mixture of several distinct pure states, each represented by its wave function,*

(1)
$\psi(q) = u_1(q)$
(2)
$\psi(q) = i_2(q)$

(k)
$\psi(q) = u_k(q)$
with the respective fractional abundances

$$\tilde{p}_1 = |\psi_1|^2, \quad p_2 = \left|\dot{\psi}_2\right|^2, \ldots p_k = |\psi_k|^2, \ldots$$

One easily verifies that case I and case II give two completely different statistical distributions. Of course they are identical for energy, because we have arranged that their statistics shouid be the same. But iet us consider another physical quantity, F for example, not having the same eigenfunctions as energy. In case I the mean value of F takes the form (see §1),

$$\overline{\text{Mean}}_{\mathbf{1}}(\bar{F}) = (\dot{\psi}, \bar{F}\dot{\psi}) = \sum_{k,l} \dot{\psi}_k^* \psi_l \bar{F}_{kl} \tag{I}$$

while in case II each component $\psi = u_k$ gives a contribution of this kind:

$$\overset{(k)}{\text{Mean}}\ (F) = (\psi, \overset{(k)}{F}\psi) = (u_k, Fu_k) = F_{kk}$$

When this component appears with the probability p_k in the mixture, one obtains altogether

$$\text{Mean}(F) = \sum_k p_k^{(k)} (\psi, F\psi) = \sum p_k F_{kk}$$

If in particular we consider the case of a mixture where $p_k = |\psi_k|^2$, we find,

$$\text{Mean}_{\text{II}}(F) = \sum_k |\psi_k|^2 F_{kk} \tag{II'}$$

Thus, provided that F_{kl} is not by a chance a diagonal matrix (that is, F does not have the same eigenfunctions as H), the two cases I and II are completely different.

8

- In what follows the upper indices $\begin{pmatrix} (1) & (2) & (n) \\ \psi, & \psi & \ldots \end{pmatrix}$ (w) always designate distinct pure states.

It is evident that in case II our knowledge of the system is much more restricted than in case I. If our knowledge is limited to the statistics of energy-that is, if we have only the equations

$$p_1 = |\psi_1|^2, \quad p_2 = |\psi_2|^2 \cdots p_k = |\psi_k|^2$$

we do not know the coefficients ψ_k themselves, but only their absolute values. Given that the ψ_k are nomally complex quantities, we can write them in the form

$$\psi_k = \sqrt{p_k} \exp(i\alpha_k) \tag{1}$$

where the phases α_k are still indeterminate. One easily verifies that the difference between cases II and I arises from this ignorance about the phases α_n. Thus, in introducing (1) in the expression $\text{Mean}_1(F)$, we find

$$\text{Mean}_{\mathbf{I}}(F) = \sum_{kl} \sqrt{p_k p_l} F_{kl} \exp[i(\alpha_l - \alpha_k)]$$

If we then average over the unknown phases we find that all of the terms with $k \neq l$ drop out and we get precisely $\text{Mean}_{\text{II}}(F)$.

One thus sees that it is necessary to make a careful distinction between:
I. A pure state described by a single wave function ψ that represents, we see, something irreducible, the probabilities that it implies being only "potential" probabilities;
II. A mixture, composed of different pure states

$$\begin{matrix}(1)(2) & (n)\\ \psi, \psi \cdots \psi,\end{matrix}$$

realized with probabilities $p_1, p_2 \cdots p_n \ldots$. These latter probabilities are understood in the ordinary sense of the word. Naturally, they are all non-negative. We suppose them to be normalized:

$$\sum_n p_n = 1$$

25.1.6 §5. the Statistical Operator

It will be useful to introduce here a concise notation to describe statistical ensembles in all generality. We will consider a mixture such as we have just defined ($4, case II). The mean value of a physical quantity G in this mixture is

$$\text{Mean}(G) = \sum_n p_n(\psi, G\psi), (n),$$

or, referred to a concrete coordinate system,

$$\text{Mean}(G) = \sum_n p_n \sum_{\rho\sigma} \frac{(n)(n)}{\psi_\sigma \psi^*_\rho G_{\rho\sigma}}$$

which can be written

$$\begin{aligned}\text{Mean}(G) &= \text{Trace}(PG)\\ &= \text{Trace}(GP),\end{aligned} \tag{I}$$

when one introduces a Hermitian matrix P, the statistical matrix, defined by

$$P = \sum_n p_n \overset{(n)}{(\psi)} \times \overset{(n)}{(\psi)}; \tag{1}$$

that is, in some chosen system of coordinates,

$$P_{\sigma\rho} = \sum_n p_n \dot{\psi}^*_\rho \dot{\psi}_\sigma \tag{1'}$$

The case of a pure state $\psi = \sum_\rho \psi_\rho u_\rho$ is included in these formulas as the special case of a mixture where all the p_n are zero except for the singie one, which is equal to unity. Its statistical matrix takes the form

$$\overset{(\psi)}{P}_{\sigma\rho} = \psi^*_\rho \psi_\sigma, \quad \text{or} \quad \overset{(\psi)}{P} = (\psi \times \psi) \tag{2}$$

Let us call the statistical matiix for pure state an elementury matrix (Linzclmatrix). The matrix P for a general mixture can thus be considered as a linear superposition of "elementary matrices,"

$$P = \sum_n p_n^{(n)} P$$

The elementary matrix for a pure state ψ takes an especially simple form in a system of coordinates $v_1, v_2 \cdots v_\rho$ in which the wave function ψ is identical with one of the axes. For example, let ψ be equal to v_2. Then one has

$$\overset{(\psi)}{P}_{\rho\sigma} = \delta_{2\rho} \cdot \delta_{2\sigma} = \left\| \begin{array}{ccccc} 0 & 0 & 0 & 0 & \cdots \\ 0 & 1 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 0 & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \end{array} \right\| \tag{1'}$$

Let us now calculate the probability of finding the value g_α of G in the ensemble characterized by the statistical matrix P.

Let us take as axes the eigenfunctions v_x of the operator G. For the pure component

$$\overset{(n)}{\psi} = \sum {}_\psi \psi_u v_k$$

with the index n we have (§1, equation 13)

$$\overset{(n)}{\text{Prob}}\,(g_\alpha) = \left|\overset{(n)}{\psi_\alpha}\right|^2 = \overset{(n)}{P}_{\alpha\alpha}$$

When this component occurs in the ensembie with the provability $\bar{p}_n$ one has altogether

$$\text{Proh}\,(g_*) = \sum_n p_* \left|\psi^{(n)}_*\right|^2 = P_{\alpha\gamma}$$

$$(x)$$

If we make use of the elementary matrix P for the pure state in which $G = g_\alpha$ (see 2′),

$$P_{\beta\gamma} = \delta_{\alpha\beta}\delta_{\alpha\gamma}$$

we can express the probability of finding the value g_x in the mixture P in the invariant form,

$$\text{Prob}_P\,(g_x) = P_{xx} = \text{Trace}\left({}^{(x)}P\right) \tag{II}$$

In particular, if $P = P$ designates the case of the pure state where an arbitrary physical quantity F has the eigenvalue f_n, one sees that

$$\overset{(n)(x)}{\text{Trace}}(PP) = \text{Prob}\,(f_n, g_\alpha)$$

is the probability of finding the value $G - g_\alpha$ for the pure state in which $F = f_n$. One notes that this expression is completely symmetric between F and G. The same expression (III) also gives the probability of finding $F = f_n$ for the pure state in which $G = g_\alpha$.

The statistical matrices P therefore present an evident advantage. They permit us to express all our definitions so that the very form (I, II, III) already indicates the invariant character.

25.1.7 §6. Some Mathematical Properties of Statistical Matrices

(a) Let us calculate the trace of an arbitrary statistical matrix P,

$$\text{Trace } P = \sum_\alpha P_{\alpha\alpha} = \sum_n p_n \sum_\alpha \left|\psi_\alpha^{(n)}\right|^2 = \sum_n p_n = 1$$

In this way we obtain the relation

$$\text{I race } P = 1, \tag{1}$$

which expresses in brief form the normalization of probabilities.

(b) In particular, the elementary statistical matrices P for pure states possess the additional property

$$\overset{(\psi)}{P^2} = P, \tag{2}$$

which results immediately from the definition (§5, equation 2) of these matrices,

$$\left(P^2\right)_{\sigma\rho} = \sum_\tau \psi_\rho^* \psi_\tau \psi_\tau^* \psi_\sigma = \psi_\rho^* \psi_\sigma = \overset{(\psi)}{P}_{\sigma\rho}$$

Relation (2) is in any case evident if one recalls the diagonal representation (§5, equation 2′) of elementary matrices.

One perceives immediately that the converse is also true. From $P^2 = P$ and from Trace $P = 1$ it follows that P is an elementary matrix. Thus when P is written in its diagonal form, P^2 is likewise diagonal, and $P = P^2$ implies $p_i = p_i^2$. The eigenvalues are therefore zero or unity. From the equation Trace $P = \sum_i p_i = 1$
it follows, finally, that a single one of p_i is equal to unity, and that all the others vanish. The relation $P^2 - P = 0$ is therefore necessary and sufficient for the statistical matrix $\bar{P}$ to be the matrix for a pure state.

(c) We have not yet placed any restrictions on the choice of the pure states which constitute the mixture. In particular, we have not assumed that they were represented by orthogonal wave functions ψ (later to be distinguished from one another by an index (n) written directly above the ψ). But one can show very easily that an arbitrary mixture composed of arbitrary pure states can always be written in the form of a mixture of orthogonal pure states with non-negative relative probabilities p_i.

Let us first verify that a matrix $\bar{P}$ is a semi-definite matrix; that is, that for our arbitrary vector ξ one always has

$$(\xi, P\xi) \geq 0 \tag{3}$$

Thus the definition (§5, equation $1'$) of P gives

$$(\xi, P\xi) = \sum_{n\alpha\beta} p_n \xi^*_\alpha \psi_\alpha \cdot \xi_\beta \psi^*_\beta = \sum_n p_n |(\xi, \psi)|^2$$

an expression which cannot be negative because

$$p_n \geq 0 \quad \text{and} \quad |(\xi, \psi)|^2 \geq 0$$

But P is a Hermitian matrix. Therefore, there exists an orthogonal coordinate system $v_1, v_2 \ldots v_p$ in which P takes its diagonal form,

$$P_{\rho\sigma} = \left\| \begin{array}{ccccc} p'_1 & 0 & 0 & 0 & \cdots \\ 0 & \bar{p}'_2 & 0 & 0 & \cdots \\ 0 & 0 & \bar{p}'_3 & 0 & \cdots \\ 0 & 0 & 0 & \bar{p}'_4 & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \end{array} \right\|. \tag{4}$$

The values of the diagonal elements $p'_1, p'_2 \ldots p'_\rho$ cannot be negative. Thus, again one has in these coordinates

$$(\xi, P\xi) = \sum_\rho p'_\rho \, |\xi_\rho|^2 \geq 0$$

which is not possible for an arbitrary vector ξ unless $p'_\rho \geq 0$ for every ρ. The matrix P therefore can always be written in the form

$$P = \sum_\rho p'_\rho \overset{(\rho)}{P}, \tag{$\prime$}$$

(ρ)
where the P are the elementary matrices for a certain system of orthogonal pure states $v_1, v_2 \ldots v_\rho$. The $p'_1, p'_2 \ldots p'_\rho \geq 0$ are the relative probabilities for these states.

As Trace $P = 1$, we also have

$$\sum p'_\rho = \mathbf{i},$$

and $p'_\rho \geq 0$ implies

$$0 \leq p'_\rho \leq 1$$

(d) From this inequality follows another,

$$p'_\rho - p'^2_\rho \geq 0.$$

From this equation we conclude that for an arbitrary vector ξ,

$$\left(\xi, \left(P - P^2\right)\xi\right) = \sum_\rho |\xi_\rho|^2 \left(p'_\rho - p'^2_\rho\right) \geq 0. \tag{5}$$

The matrix $P - P^2$ is therefore likewise semidefinite.
In particular for a purc state the quantity $P - P^2$ vanishes (see equation 2). Elementary statistical operators like $P = (\psi \times \psi)$ can be considered as "projectors" or "projection operators." Applied to an arbitrary state vector ξ, P singles out the projection of this vector in the direction of the vector ψ,

$$\sum_{\sigma} P_{\sigma\rho}\breve{\zeta}_{\sigma} = \sum_{\sigma} \psi_{\rho}\psi^{*}_{\sigma}\xi_{\sigma} = \psi_{\rho}(\psi, \xi)$$

The magnitude of this vector is (ψ, ξ) and its direction is that of the unit vector ψ. The iteration of the projection produces no further change: $P^2 = P$.

25.1.8 §7. the Statistical Operator and Thermodynamics

The operator P describes an ensemble of identical systems which are distributed in an arbitrary way among the different states. It plays the role analogous to that
of a distribution function in ordinary statistical mechanics. Therefore there ought to exist a connection between operator P and the macroscopic thermodynamic quantiiies. It will be enough for us to point out briefly the main features of this connection without stopping for proofs (see von Neumann, 1927, p. 273). Everything is summarized in the definition of entropy, S :

$$S = -kN \,\mathrm{Trace}(P \ln P), \tag{1}$$

where
and
k = Boltzmann's constant
N = the total number of systems.

This relation becomes quite plausible when one recalls that in statistical mechanics one has

$$S = -k \sum_{\alpha} (n_{\alpha} \ln n_{\alpha} - N \ln N)$$

where n_{α} is the number of systems in the state α. Therefore if $p_{\alpha} = n_{\alpha}/N$ represents the probability for a system to be in the state α, one has again

$$S = -kN \left[\sum_{\alpha} p_{\alpha} (\ln p_{\alpha} + \ln N) - \ln N \right],$$

which is identical with (1) in a system of coordinates in which P is diagonal (§6, equation 4). Our definition of entropy is therefore the entirely straightforward generalization of the usual definition. One sees immediately that for a pure state the entropy thus defined is zero. Thus, if one represents P in diagonal form, the entropy becomes

$$S = -kN \sum_{\dot{a}} p_{\alpha} \ln p_{\alpha}$$

Every term $p_{\alpha} \ln p_{\alpha}$ of the sum vanishes, because in a pure state the p_{α} are all zero except for a single one which is unity. One also sees immediately that the entropy of a mixture is always positive.

To maximize the entropy for a given total energy E is to impose on P the following conditions:

```
-kN Trace(P ln P) -> Max;
        Trace P = 1;
    N Trace (PH) = E.
```

The solution of this extremum problem is represented by the matrix,

$$P - e^{-\beta H} / \text{ Trueve } \left(e^{-\beta H}\right) = e^{-\beta H} / \boldsymbol{Z}(\beta), \tag{2}$$

where

$$Z(\beta) = \text{Trace}\left(e^{-\beta H}\right).$$

The Lagrange factor β is determined, as always, by equilibrium with a perfect gas; thus, $\beta = 1/kT$, where T is the absolute temperature.

One thus obtains for the entropy of the most probable distribution,

$$\begin{aligned} S &= kN \,\text{Trace}\left[e^{-\beta H}(\beta H + \ln Z)/Z(\beta)\right] \\ &= -kN[\beta\partial \ln Z/\partial\beta - \ln Z] \end{aligned}$$

and for the energy,

$$E = -N\hat{C} \ln Z/\partial\beta$$

from which one easily gets all the other thermodynamic quantities, for example the free energy

$$F = E - TS = -kNT \ln Z,$$

et cetera.

25.1.9 §8. the Irreducibility of the Pure Case

Our definitions would be worthless if pure cases were not characterized by some kind of irreducibility. We have to show that it is not possible to represent a pure case in the form of a mixture. For this purpose we will show that a statistical matrix P, obtained as a mixture of two statistical matrices Q and R,

$$P = \alpha Q + \beta R \tag{1}$$

with

$$\alpha + \beta = 1, \quad \alpha \geq 0, \quad \beta \geq 0,$$

cannot be an elementary statistical matrix (such that $P = P^2$) except if $Q = R = P$. Let us calculate

$$\begin{aligned} P^2 &= \alpha^2 Q^2 + \beta^2 R^2 + \alpha\beta(QR + RQ) \\ &= \alpha^2 Q^2 + \beta^2 R^2 + \alpha\beta\left[Q^2 + R^2 - (Q - R)^2\right] \\ &= \alpha Q^2 + \beta R^2 - \alpha\beta(Q - R)^2 \end{aligned}$$

where we used the condition $\alpha + \beta = 1$. Thus

$$P - P^2 = \alpha\left(Q - Q^2\right) + \beta\left(R - R^2\right) + \alpha\beta(Q - R)^2$$

We now recall that the matrices $\bar{Q} - \bar{Q}^2$ and $K - R^2$, as welli as $(\bar{Q} - R)^2$, are always semidefinite (§6, equation 5). Therefore it is necessary that all these quantities should vanish

for P to be an elementary matrix ($P = P^2$). In particular, we have $(Q - R)^2 = 0$, from which we conclude

$$Q = R$$

because the square of a Hermitian matrix cannot vanish unless the original matrix vanishes,

$$\left(\frac{\sum_k}{k} A_{ik} A_{ki} = \sum_k A_{ik} A_{ik}^* = \sum_k |A_{ik}|^2 = 0 \text{ implies } A_{ik} = 0 \right)$$

From $Q = R$ and from (1) it follows that $Q = R = P$.
Statistical operators thus form an ensemble of a characteristic structure, called convex ensemble. Its boundary is formed by the operators for pure cases. No pure case can be constructed by linear superposition with positive coefficients-that is, by mixture-of two nonidentical pure cases.

Although the statistical operator P of a pure case cannot be decomposed, one might imagine that there perhaps exists some other means to reduce directly the corresponding statistics.

In actuality this problem does not differ from the problem that we have just discussed. However, it would perhaps be useful to consider it explicitly.

Of course we always take as our foundation the statistical distributions as predicted by the formalism of the theory and verified by so many experiments. Therefore we will not discuss the validity of these statistical predictions. We will ask ourselves rather if, once assumed, they might not be represented by mixtures of aibitrary form, but belonging to systems that are well defined in the ordinary sense of classical mechanics.

Let us take a concrete example that is as simple as possible, that of the statistical description associated with a "spin." Let us consider an atom of angular momentum $\hbar/2$ and let us focus attention on the component of this angular momentum in an arbitrary direction. For any given direction there are only two values possible for this component of the spin: $+\hbar/2$ and $-\hbar/2$. Let us fix in space the axis of a system of spherical polar coordinates. Let $u_+$and u_-be the eigenfunctions associated with the two possible values for the component along this axis. To be concrete, suppose that

$$\psi = u_+$$

is the wave function of the state in question-that this state is a "pure case." Let us now consider, for the same state ψ, the component of the spin in another direction, oblique to the polar axis and characterized, for example, by the polar coordinates θ, ϕ. The only possible values for the component of the spin in this direction are again $+\hbar/2$ and $-\hbar/2$. To evaluate the probabilities for finding each of these two values it is necessary to represent ψ in terms of the two eigenfunctions associated with those two possibilities. We will call them u'_+ and u'_-. A calculation gives

$$u_1 = c_+ u'_+ + c_- u'_-$$

with

$$c_+ = e^{i\phi/2} \cos \theta/2$$
$$c_- = e^{-i\phi/2} \sin \theta/2$$

The squares of the absolute values of the coefficients u'_+ and u'_- represent the probabilities for finding the one or the other of the two possible components in the direction θ, ϕ; thus,

$$p'_+ = |c_+|^2 = \cos^2 \theta/2$$
$$p'_- = |c_-|^2 = \sin^2 \theta/2$$

But, in the same state, the probabilities of the two values for the component along the original polar axis are, respectively,

$$p_+ = 1$$

and

$$p_- = 0$$

Evidently it is impossible to decompose these statistics into a mixture of definitely oriented spins. In such a mixture it would be necessary that a fraction $\cos^2\theta/2$ of the atoms should have a component $\mathbf{h}/2$ in the direction θ, ϕ and that a fraction $\sin^2\theta/2$ should have the opposite orientation. This, by itself, would be possible. But we ought, in addition, to have 100% of the atoms with the same component $\hbar/2$ along the direction of the polar axis, and yet a fraction $\cos^2\theta'/2$ along any other direction θ'. That would be a juggling trick rather difficult to bring off!

Evidently it is impossible to arrange a virtual ensemble of oriented atoms that meets simultaneously all of these statistical requirements. The mathematics of the probability calculations alrcady precludes this possibility.

We will use the same simple example in section §12 to study in detail how, by his own intervention, the observer succeeds in doing the juggling trick. However, to keep the discussion clear, it is first necessary for us to bring out an aspect of quantum mechanics which we have not yet mentioned, but which contains the very essence of the theory, the feature responsible for the appearance of probabilities.

25.1.10 §9. Statistics of a System Composed of Two Subsystems

At first sight the mathematical formalism of quantum mechanics seems entirely analogous to that of the theories of "classical" physics: a differential equation uniquely prescribes the evolution of the wave function ψ that describes the state of the system. Therefore it seems as though our task, faced with Schrödinger's equation, is no different from that of Laplace faced with the equations of Newton. The state of a closed system, perhaps the entire universe, is completely determined for all time if it is known at a given instant. According to the Schrodinger equation, a pure case represented by a ψ function remains always a pure case. One does not immediately see any occasion for the introduction of probabilities, and our statistical definitions might appear in the theory as a foreign structure.

We will see that that is not the case. It is true that the state of a closed system, once given pure, always remains pure. But let us study what happens when one puts into contact two systems, both originally in pure states, and afterwards separates them.

Let us therefore consider two systems, I and II, originally separated. Let x be the conscmble of the coordinates of I and y the coordinates of II. Each of the two systems is assumed to be in a pure state given by its wave function:

$$\psi(x) = \sum_k \psi_k u_k(x) \quad (\text{ system } I)$$

$$\phi(y) = \sum_\rho \phi_\rho v_\rho(y) \quad (\text{ system II })$$

We have expressed the functions ψ and ϕ as series built on the orthogonal functions $u_k(x)$ and $v_\rho(y)$. The coefficients ψ_k and ϕ_ρ depend only on time.

Although the two systems are originally taken to be separated, we can nevertheless describe them by a combined wave function $\Psi(x, y)$, whose evolution is governed by a combined Hamiltonian. The fact that the two systems are isolated from each other is expressed in the form of the Hamiltonian. It is the sum of two terms, each depending only upon the coordinates of one of the two systems; thus,

$$H\left(x, p_x, y, p_y\right) = H_I\left(x, p_x\right) + H_{II}\left(y, p_y\right)$$

It is easily verified that the combined wave function $\Psi(x, y)$, which unites the statistics contained in $\psi(x)$ and $\phi(y)$, is the simple product of the two separate
wave functions. It obeys the wave equation with Hamiltonian $H_I + H_{II}$. One has therefore before contact

$$\Psi(x, y) = \psi(x)\phi(y) = \sum_{k,\rho} \psi_k \phi_\rho u_k(x) v_\rho(y) \tag{1}$$

Let us now bring the two systems into contact. That makes it necessary to add to H an interaction term, $H_i\left(x, p_x, y, p_y\right)$, containing the two sets of variables x, p_x and y, p_y in a form that is not simply additive. It is evident that the combined function Ψ for the pair of systems will no longer in general keep the form of a product of two functions each depending on a single set of variables. However, it naturally can be expanded at each instant as a series of products $u_k(x)v_\rho(y)$ with coefficients that will depend on the instant chosen. Thus, if $u_k(x)$ and $v_\rho(y)$ form complete systems of orthogonal functions in their own domains, x and y, the products $u_k(x)v_\rho(y)$ also form an orthogonal system that is complete in the space of functions on the domain (x, y) of the ensemble. During or after the contact the wave function will be written in every casc in the general form,

$$\Psi(x, y) = \sum_{k,\rho} \Psi_{k\rho} u_k(x) v_\rho(y) \tag{2}$$

where the coefficients $\Psi_{L\rho}$ in the generic case will not have the special form of a product, $\psi_k \phi_\rho$. As we are always dealing with a unique wave function evolving in accord with a Schrödinger equation, we have for the combined system a constantly pure case. Its statistical matrix is an clementary matrix,

$$P_{k\rho, l\sigma} = \Psi_{k\rho} \Psi^*_{l\sigma}$$

As one pair of indices, k, ρ, is needed here to characterize a state of the total system, the elements of the statistical matrix of this system will evidently depend on two pairs of indices, k, ρ and l, σ.

Let us now focus attention on the system I. What is its statistical matrix?
Let F be a function solely of the variables of system I and F_{kl} its representation in the coordinates $u_k(x)$. The mean or expectation value of F in the state Ψ will be given by

$$(\Psi, F\Psi) = \sum_{kl,\rho} \Psi^*_{k\rho} \Psi_{l\rho} F_{kl} = \text{Trace}\left(P^I F\right)$$

Therefore the matrix

$$P^I_{lk} = \sum_{\rho} \Psi_{l\rho} \Psi^*_{k\rho} \tag{3a}$$

plays the role of statistical matrix for system I. Similarly one obtains for system II the statistical matrix

$$P^{II}_{\sigma\rho} = \sum_k \Psi_{k\sigma}\Psi^*_{k\rho} \tag{3b}$$

P^I and P^{II} are evidently no longer elementary matrices. We are dealing with mixtures. What are their components? And what are the relative probabilities or concentrations of these components?

We note that the $\Psi_{k\rho}$ are normalized in the space of the indices k, ρ; thus,

$$\sum_{k,o} |\Psi_{k\rho}|^2 = 1$$

(ρ)
Therefore the magnitude ψ with the components

$$(\rho)$$
$$\psi_k = \Psi_{k\rho} / \left[\sum_I |\Psi_{l\rho}|^2\right]^{1/2}$$

is a normaiized state vector for system **i** and represents a pure case. We can therefore give to P^I the following form,

$$P' = \sum_\rho p_\rho (\dot{\psi} \times \overset{(\rho)}{\psi}) \tag{3}$$

where

$$p_\rho = \sum_l |\Psi_{l\rho}|^2 \tag{4a}$$

(ρ)
is the concentration with which the pure case ψ is contained in the mixture I. In the same way one has

$$P^{II} - \sum_k p^{(k)}_k (\phi \times \overset{(k)}{\phi}), \tag{/}$$

where

$$\phi^{(k)}_\rho = \Psi_{k\rho} / \left[\sum_\sigma |\Psi_{k\sigma}|^2\right]^{1/2}$$

is a unit vector, representing a pure case in II; and

$$p_k = \sum_\sigma |\Psi_{k\sigma}|^2 \tag{4b}$$

$$(k)$$

is the concentration with which ϕ is contained in the mixture II.
While the combined system I + II, which we suppose isolated from the rest of the world, is and remains in a pure state, we see that during the interaction systems I and II individually transform themselves from pure cases into mixtures.

This is a rather strange result. In classical mechanics we are not astonished by the fact that a maximul knowledge of a composite system implies a maximal knowledge of all its parts.

We see that this equivalence, which might have been considered trivial, does not take place in quantum mechanics. There a maximal knowledge of a composite system ordinarily implies only mixtures for the component partsinat is, a knowledge that is not maximal.

The mixtures represented by P^I and P^{II} naturally cannot express all that it is possible to know about the combined system I + II. It is evident that the elementary combination of statistical mixtures for two individual systems cannot by itseif reproduce a pure case for the combined system. Thus the function $\Psi(x, y)$ for the combined system contains still other relations, to wit, statistical correlations between the components of the two mixtures I and II.

The fact that the description we obtain for each of the two individual systems does not have the character of a pure case warns us that we are renouncing part of the knowledge contained in $\Psi(x, y)$ when we calculate probabilities for each of the two individual systems separately. This renunciation expresses itself by the summation over the index ρ in the definition of P^I, where we abstract away from what might be known about the state ρ of system II and about its connection with system I. This loss of knowledge expresses itself by the appearance of probabilities, now understood in the ordinary sense of the word, as expression of the fact that our knowledge about the combined system is not maximal.

25.1.11 §10. Reversible and Irreversible Evolution

It is evidently necessary to make a characteristic distinction between two essentially different modes of evolution of an individual system, a distinction which has no analog in classical mechanics.

I. Reversible or "causal" transformations. These take place when the system is isolated. They can be described by the change with time of a ψ function (or of a certain number of distinct ψ functions when one deals with a mixture). If $\psi(t_0)$ represents a pure case at the instant t_0, its evolution can be written in the form

$$\psi(t) = T\psi(t_0) \tag{1}$$

with the operator

$$T = \exp\left[-iH(t - t_0)/\hbar\right] = \sum_n (1/n!)\left[-iH(t - t_0)/\hbar\right]^n$$

In the case of a mixture, the time dependence of the statistical operator

$$P(t) = \sum_\rho p_\rho \begin{pmatrix} & \overset{(\rho)}{\psi}(t) \times \overset{\rightarrow}{\psi}(t) \\ (\rho) & \end{pmatrix} = \sum_\rho p_\rho \begin{pmatrix} & \overset{(\rho)}{T\psi}(t_0) \quad \overset{(\rho)}{T\psi}(t_0) \\ & \end{pmatrix}$$

is thus given by the equation

$$P(t) = I\bar{P}(t_0)\tilde{I}^*$$

where $\tilde{T}_{li}$ is the abbreviation for the matrix T_{lk}. One verifies that

$$\tilde{T}^* = \sum_n (1/n!)\left[iH(t - t_0)/\hbar\right]^n$$

and that

$$T\tilde{T}^* = 1$$

It is therefore a unitary transformation that characterizes a causal evolution. It transforms a pure case into a pure case.

A unitary transformation, keeping invariant-as it does-the trace of a tensor, does not change the value of the entropy; the quantity $\mathrm{Trace}(P, \ln P)$ stays constant.
II. Irreversible transformations, which one might also call "acausal." These take place only when the system in question (I) makes physical contact with another system (II). The total system, comprising the two systems (I + II), again in this case undergoes a reversible transformation so long as the combined system I + II is isolated. But if we fix our attention on system I, this system will undergo an irreversible transformation. If it was in a pure state before the contact, it will ordinarily be transformed into a mixture. If it was already a mixture, it will be transformed into another mixture, the entropy of which (§7, equation 1) will be increased. Once thus degraded, the system has no chance in and by itself ever to regain its initial degree of determination.

We shall see specifically that measurement processes bring about an irreversible transformation of the state of the measured object, such that the initial statistical operator for a pure case

$$\left[\psi(q) = \sum_n \psi_n u_n(q)\right],$$
$$P = (\psi \times \psi),$$

is transformed, by interaction with the measuring apparatus, into the mixture,

$$P' = \sum |\psi_n|^2 (u_n \times u_n)$$

the u_n being the eigenfunctions of the quantity measured. The transition from P to P' clearly cannot be represented by a unitary transformation. It is associated with an increase of the entropy from 0 to $-k \sum_n |\psi_n|^2 \ln |\psi_n|^2$, which cannot come about by a unitary transformation.

The distinction between these two modes of evolution has no analog in classical mechanics, where it is always possible to give a maximal description of the state of an object by its $2f$ coordinates and momenta $q_1, q_2 \cdots p_f$, whatever the interactions between systems.

25.1.12 §11. Measurement and Observation. the Act of Objectification

We are now ready to analyze what happens in the act of measurement. We will first outline a protocol for this process and then verify in the following section that it describes properly the typical course of a measurement.

Suppose that we want to measure the quantity $F(x, p_x)$ of a system ("the object") given to be in the state $\psi - \sum_k \psi_k u_k(x)$ where u_k is an eigenfunction corresponding to the value f_k of F. We couple it with an apparatus capable of measuring F.

Let $G(y, p_y)$ be the coordinate specifying the position of the "needle" of the measuring device, and $g_0, g_1 \ldots g_\rho$ its eigenvalues, with eigenfunctions $v_0(y)$, $v_1(y) \ldots v_\rho(y)$. The state $v_0(y)$ corresponds to the zero of this apparatus.

Before the coupling we will attribute to the combined system a collective wave function of the form,

$$\Psi(x, y) = v_0(y) \sum_k \psi_k u_k(x) \tag{1}$$

This is a pure case for each of the two individual systems. After the interaction the wave function will be of a more general character,

$$\mathbf{\Psi}(x,y)=\sum_{k,\rho}\mathbf{\Psi}_{k\rho}u_k(x)v_\rho(y) \tag{2}$$

But an arbitrary interaction does not provide a measurement. In order for it to do so, it is necessary that it disturb the state of the object as little as possible and in addition that it should let one deduce from a g_ρ the corresponding f_k. Thus the values of the measurement scale g_ρ should be coordinated one-to-one with the values f_k of the quantity under consideration, so that one can inscribe directly onto the g_ρ scale the corresponding values of F. That occurs by replacing the index $\rho_{(k)}$ by k. Thus $g_k=g_{\rho_{(k)}}$ will correspond to f_k.

We will see (§12) that after a measurement of the quantity the wave function takes the special form,

$$\Psi(x,y)=\sum\psi_k u_k(x)v_k(y) \tag{1'}$$

According to the preceding section, this function represents a state of the combined system that has for each separate system, object, and apparatus, the character of a mixture. According to §9, equation (4), the quantity $p_k=|\psi_k|^2$ gives the probability of finding the object in the pure state u_k with $F=f_k$; and the same quantity $p_k=|\psi_k|^2$ also gives the probability of finding the apparatus indication $G=g_k$. Moreover, we have a correlation between the two mixtures: specifically, we know with certainty that if $G=g_k$, then $F=f_k$. But of course quantum mechanics does not allow us to predict which value will actually be found in the measurement. The interaction with the apparatus dues not put the object into a new pure state. Alone, it does not confer on the ohject a new wave function. On the contrary, it actually gives nothing but a statistical mixture: It leads to one mixture for the object and one mixture for the apparatus. For either system regarded individually there resuits uncertainty, incompiete knowiedge. Yet nothing prevents oi teducing this uncertainty by further observation. And this is our opportunity.

So far we have only coupled one apparatus with one object. But a coupling, even with a measuring device, is not yet a measurement. A measurement is achieved only when the position of the pointer has been observed. Ii is precisely this increase of knowledge, acquired by observation, that gives the observer the right to choose among the different components of the mixture predicted by theory, to reject those which are not observed, and to attribute thenceforth to the object a new wave function, that of the pure case which he has found.

We note the essential role played by the consciousness of the observer in this transition from the mixture to the pure case. Without his effective intervention, one would never obtain a new ψ function. In order to see this point clearly, let us consider the ensemble of three systems, (object x) + (apparatus y) + (observer z), as a combined and unique system. We will describe it by a global wave function with a form analogous to (2),

$$\Psi(x,y,z)=\sum_k\psi_k u_k(x)v_k(y)w_k(z)$$

where the w_k represent the different states of the observer.

"Objectively"-that is, for us who consider as "object" the combined system x,y,z-the situation seems little changed compared to what we just met when we were considering only apparatus and object. We now have three mixtures, one for each system, with those statistical correlations between them that are tied to a pure case for the combined system. Thus the function $\Psi(x,y,z)$ represents a maximal description of the combined "object," consisting of the actual object x, the apparatus y, and the observer z; and nevertheless we do not know in what state the object x is.

The observer has a completely different impression. For him it is only the object x and the apparatus y that belong to the external world, to what he calls "objcctivity." By contrast

he has with himself relations of a very special character. He possesses a characteristic and quite familiar faculty which we can call the "faculty of introspection." He can keep track from moment to moment of his own state. By virtue of this "immanent knowledge" he attributes to himself the right to create his own objectivity-that is, to cut the chain of statistical correlations summarized in $\sum_k \psi_k u_k(x) v_k(y) w_k(z)$ by declaring, "I am in the state w_k " or more simply, "I see $G = g_k$," or even directly, " $F = f_k$."

Accordingly, we will label this creative action as "making objective." By it the observer establishes his own framework of objectivity and acquires a new piece of information about the object in question.*

Thus it is not a mysterious interaction between the apparatus and the object that produces a new ψ for the system during the measurement. It is only the consciousness of an " 1 " who can separate himself from the former function $\Psi(x, y, z)$ and, by virtue of his observation, set up a new objectivity in attributing to the object henceforward a new function $\psi(x) = u_k(x)$.

Neither is it some ignorance as to the state of the observer that creates quantum indeterminacy. On the contrary, in assuming a pure case for the combined system, we have implicitly presupposed an equally perfect knowledge of the initial state $w_0(z)$ of the observer and of the apparatus $v_0(y)$, that is, maximal information. Moreover, we have assumed that the observer can keep track perfectly of his own state.

Of course there might also be restrictions on the immanent knowledge of the observer. But these, if they existed, would in any case have nothing to do with quantum indeterminism; they would be additional restrictions of a completely different character. Moreover, it is not ordinarily required for a discussion of the mcasuring process that one should have an all-encompassing knowledge of the state of the observer; for example, there is little chance of making a big mistake if one does not know his age.

25.1.13 §12. an Example of Measurement

It only remains for us now to verify the protocol for measurement that we have just discussed. Let us take as a typical example the determination of the value of

- This paragraph is new. We have translated it from a typed addition inserted by Professor Fritz London in his own copy of the printed book, kindly sent to us October 24, 1980, by Mrs. Fritz London.-Eds.
  one component of the magnetic moment of an atom by the method of Stern and Gerlach. The formulas that we will get can be generalized without difficulty to an arbitrary measurement.

This measurement is made, as is well known by observing the motion of an atom through a nonuniform magnetic field. The field points in the direction along which one wants to determine the component of the magnetic moment of the atom. The coordinates, y; of the center of gravity of the atom play the role of the pointer reading $G(y, \beta_y)$. The internal coordinates of the atom, relative to the center of gravity, serve as object coordinates x. Specifically, we are concerned with the component, $M = M(x, p_x)$, of the magnetic moment in the direction of the field.

Let us write the wave equation for this problem in the form

$$\left\{-\left(\hbar^2/2m\right)\Delta_y + H_0(x, \partial/\partial x) + \left[M(x, p_x), F(y)\right]\right\}\Psi(x, y) = i\hbar\dot{\Psi}(x, y) \tag{1}$$

Here H_0 is the Hamiltonian operator for the field-free atom after one has separated off the center-of-gravity variables, $-(\hbar^2/2m)\Delta_y$ is the operator of the "apparatus" corresponding to the kinetic energy of the center of gravity, (M, F) is the contribution arising from the magnetic field F, and M is the operator for the magnetic moment of the atom in the direction of the field.

So long as the field F is constant-that is, so long as it does not depend on the coordinates y-the variables x and y can be separated in equation (1). For the different states of the "object" we must deal with the eigenvalue problem,

$$(H_0 + MF)\, u_k(x) = E_k u_k(x) \tag{2}$$

Let us limit ourselves to the lowest state of the atom, a state which we assume to be degenerate, with its components splitting in the ficld in proportion to the field strength F,

$$E_\kappa = E_0 + (k\mu/j)F \tag{3}$$

Here μ is the magnetic moment of the atom and k is the magnetic quantum number, $k = j, j-1, j-2, j-3 \ldots -j$, where j h represents the total magnetic moment of the atom. When the ficld is no longer constant, $F = F(y)$, equation (2) contains the coordinates y as parameters. Consequently the eigenvalues of (2),

$$E_k(y) = E_0 + (k\mu/j)F(y) \tag{3a}$$

will also depend on these parameters y; likewise the eigenfunctions $u_k(x)$, which will be written more appropriately as $u_k(x, y)$. In practical terms the perturbation
of the u_k by the nonuniformity of the field is so slight that we can forget this dependence of the u_k on the parameter y.

Let us now deveiop $\Psi(x, y)$ in a series in terms of the functions $u_k(x)$,*

$$\Psi(x, y) = \sum_k v_k(t, y) u_k(x),$$

and let us introduce this development into the Schrödinger equation (1). After multiplication by u_k and integration over x we find for the coefficients $v_k(t, y)$ the following equations:

$$\left\{ -\left(\hbar^2/2m\right) \Delta_y + E_k(y) \right\} v_k(y) = i\hbar \dot{v}_k(y). \tag{4}$$

They are still of the Schrödinger type but now refer solely to the motion of the center of gravity. In a typical such equation, the cigenvalue (3 a) of (2), $E_k(y)$, plays the role of the potential. Let us now consider an atomic beam and let us develop $E_k(y)$ in the neighborhood of this beam,

$$E_k = E_0 + (k\mu/j)\left[F_0 + (y, \operatorname{grad} F) + \cdots\right].$$

In first approximation the "potential" $E_k(y)$ varies linearly; thus it behaves like the potential of gravity near the earth's surface. Consequently equation (4) is nothing other than the equation of free fall. But in it the acceleration is proportional to the quantum number k. Thus the acceleration depends on the value of the component of the magnetic moment in the direction of the field, and can be positive or negative. Therefore it is easy to foresee in general terms and without detailed calculation the shape of the various trajectories which come from a well-collimated and initially monokinetic source and then travel through the nonuniform magnetic field. A single beam v_{00} splits into separate beams belonging to different values of k. The cross-hatched regions in Figure 1 show where the functions v_k are appreciably different from zero.

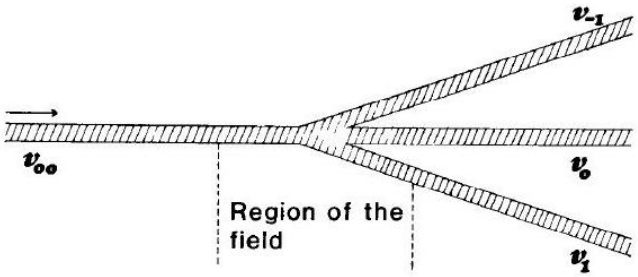


FIGURE 1. Splitting of the atomic beam in a non-uniform field.

- This is certainly permissible. The $v_k(y,t)$ show up in this development, not as given eigenfunctions, but as the still unknown coefficients of the functions $u_k(x)$.

So far we have been discussing the not-yet-normalized solutions of the auxiliary equations (4). A complete solution of the Schrödinger equation (1) will have the form

$$\Psi(x,y) = \sum_k c_k v_k(y) u_k(x) \tag{5}$$

Let

$$\dot{\psi} = \sum_k \dot{\psi}_k u_k(x)$$

with

$$\sum_k |\psi_k|^2 = 1$$

be the state of the atom before the measurement in the region at the left of the figure, where we can still separate off the motion of the center of gravity and where all the functions $v_k(y)$ are identical [$= v_{00}(y)$].

The total wave function of object-plus-apparatus before entry into the region of the field is

$$\Psi(x,y) = v_{00}(y) \sum_k \psi_k u_k(x)$$

On the other side of the field region, according to (5) and the principle of continuity, it is

$$\Psi'(x,y) = \sum_k \psi_k u_k(x) v_k(y)$$

A measurement of the y coordinate of the center of gravity of an atom that has crossed the field is equivalent to a determination of k because each $v_k(y)$ differs from zero oniy in a limited region, fixed by k, and because a determination of k is equivalent to a knowledge of the component of the magnetic moment parallel to F. This is exactly the type of statistical link that we presumed in §11.

Let us take, for example, an atom of total angular momentum 1 , for which k is restricted to the values $1, 0, -1$. The effect of the measurement shows up in the transition of the coefficients $\Psi_{k\rho}$ of the wave function of the combined system from

$$\Psi_{k\rho} = \psi_k \delta_{0\rho} = \begin{Vmatrix} 0 & 0 & 0 \\ \psi_{-1} & \psi_0 & \psi_1 \\ 0 & 0 & 0 \end{Vmatrix} \quad \text{(before the measurement)}$$

to

$$\Psi'_{k\rho} = \psi_k \delta_{k\rho} = \left\| \begin{array}{ccc} \psi_{-1} & 0 & 0 \\ 0 & \psi_0 & 0 \\ 0 & 0 & \psi_1 \end{array} \right\| \text{ (after the measurement).}$$

Before the measurement the statistical matrices P^I and P^{II} have the form of two pure cases,

$$P^I_{kl} = \left\| \begin{array}{ccc} \psi_{-1}\psi^*_{-1} & \psi_{-1}\psi^*_0 & \psi_{-1}\psi^*_1 \\ \psi_0\psi^*_{-1} & \psi_0\psi^*_0 & \psi_0\psi^*_1 \\ \psi_1\psi^*_{-1} & \psi_1\psi^*_0 & \psi_1\psi^*_1 \end{array} \right\|$$

and

$$P^{II}_{\rho\sigma} = \left\| \begin{array}{ccc} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{array} \right\|.$$

The action of the magnetic field transforms them into mixtures,

$$\left(P^{\tilde{i}}_{kl}\right)' = \left\| \begin{array}{ccc} \| \psi_{-1}|^2 & 0 & 0 \\ 0 & |\psi_0|^2 & 0 \\ 0 & 0 & |\psi_1|^2 \end{array} \right\|$$

and

$$\left(P^{II}_{\rho\sigma}\right)' = \left\| \begin{array}{ccc} |\psi_{-1}|^2 & 0 & 0 \\ 0 & |\psi_0|^2 & 0 \\ 0 & 0 & |\psi_1|^2 \end{array} \right\|$$

Here the components have a one-to-one correspondence, implying the associated correlations. For the combined system the transition $\Psi \to \Psi'$ is a unitary transformation,

$$\Psi'_{k\rho} = \sum_{l.\sigma} T_{k\rho.l\sigma} \Psi_{l\sigma},$$

where

$$T_{k\rho.l\sigma} = \delta_{kl} \delta_{\rho,l+\sigma},$$

it being understood that

$$\rho = \pm 2 \text{ is equivalent to } \rho = \mp 1.$$

25.1.14 §13. Individuality and Pure Case

A measuring arrangement, such as we have just finished describing in the previous section, can be used to "filter" through objects possessing a prescribed value of a certain physical quantity. It is enough to make a suitable slit through the screen on which the atoms fall to transform the Stern-Gerlach apparatus into a source of identically oriented atoms. It thus becomes a good set-up for producing pure cases.

Does not this conclusion contradict what we just learned (§11), to the effect that a pure case is brought about only by an "act of objectifying," accomplished by the appropriate intervention of an observer? It is necessary, however, to be more precise: the filter never puts any individual object whatsoever into a new pure state. It can only put it into a mixed state. This is what always happens when one coupies one system with another. By contrast, we can cvidently say

that the states of atoms which have gone through the slit have the desired property. We can attribute to them the wave function of the pure case in question. But this attribution only works out, so to speak, at the expense of the individuality of the object, as one does not know in advance which are the atoms that have the property in question. We can easily attribute to the objects that get through the slit the ψ function of the pure case, but we cannot say which object, that is, which variable is the argument of this ψ function. Without a supplementary check by an observer, it is not possible to guaranter wheluce a given atom has gonc through the filter or been caught in it. The filter alone thus truly produces pure cases, but in an absolutely anonymous form. Of course we can attribute to these cases afresh some names of their own, for example by numbering in sequence the atoms that really get through the slit. But that is no different from a true measurement, and we would be led back in that way to what we have already discussed.

Moreover, anonymous objects are precisely the focus of one's interest in many experiments. The majority of the measurements in atomic physics really do not deal with an individual system; rather, they seek to find out the general properties of an entire species of atoms-or of molecules, or of elementary particles. Thus for example the Stern-Gerlach set-up just discussed is ordinarily used, not to measure a component of the spin of an individual atom, but rather to determine the spin of the silver atom.

Quantum mechanics, truly a "theory of species," is perfectly adapted to this experimental task. But given that every measurement contains a macroscopic process, unique and separate, we can hardly escape asking ourselves to what extent and within what limits the everyday concept of an individual object is still recognizable in quantum mechanics.

25.1.15 §14. Scientific Community and Obiectivity

At firsi sight ii would appear that in quantum mechanics the concept of scientific objectivity has been strongly shaken. Since the classic period, the idea has become familiar that a physical object is something real, existing outside of the observer, independent of him, and in particular independent of whether or not the object has been subjected to measurement. The situation is not the same in quantum mechanics. Far from it being possible to attribute to a system at every instant its measurable properties, one cannot even claim that to attribute to it so much as a wave function has a well-defined meaning, unless referring explicitly to a definite measurement. Moreover, it looks as if the result of a measurement is intimately linked to the consciousness of the person making it, and as if quantum mechanics thus drives us toward complete solipsism.

Actually, however, we know that the relations between physicists have undergone practically no change since the discovery of quantum mechanics. No physicist has retired into a solipsistic isolation. Physicists use the same means of scientific exchange as in the past and are capable of cooperation in studying the same object. Thus there really exists something like a community of scientific perception, an agreement on what constitutes the object of the investigation, and it is this that still has to be looked into.

First of all, it is easy to recognize that the act of observation, that is, the counling between the measuring apparatus and the observer (see our example in §11), is truly a macroscopic action and not basically quantal. Consequently one always has the right to neglect the effect on the apparatus of the "scruiny" of the observer. Tracing things back in time, one will obtain definite conclusions about the state of the apparatus (or the photographic plate) and consequently the state of the object before the observation (but of course after the coupling is turned off). Morcover, nothing prevents another observer from looking at the same apparatus; and one can predict that, barring errors, his observations will be the same. The possibility of abstracting away from the individuality of the observer and of creating a collective scientific perception therefore in no way comes seriously into question.

It might appear that the scientific community thus created is a kind of spiritualistic society which studies imaginary phenomena-that the objects of physics are phantoms produced by the observer himself. In classical physics, one can picture a system at every instant in a unique and continuous way by the set of all of its measurable properties, even when it is not subjected to observation. It is exactly the possibility of this continuity of connection between properties and object that has ordinarily been considered as proof that physics deals with something "real," that is, having in principle an existence "independent of all observers." In quantum mechanics an object is the carrier, not of a definite set of measurable properties, but only of a set of "potential" probability distributions or statistics
(§3) referring to measurable properties, statistics which only come into force on the occasion of an effective, well-defined measurement. If one abstracts away from all acts of measurement, it is meaningless to claim these measurable properties as realized; the very mathematical form of the statistics does not allow it (see §8).

But that does not keep us from predicting or interpreting experimental results. Theory fixes the rules. It teaches us first of all how to filter an object to get a pure case-that is, reproducible conditions; then it suggests how to make measurements, either to check theoretical predictions or to discover new empirical regularities. The theory adapts itself truly marvelously to the realities of experiment. it gives answers on aii desired detaiis and is silent on hypothetical questions without experimental meaning.

In present physics the concept of "objectivity" is a little more abstract than the classical idea of a material object. Is it not a guarantee of "the objectivity" of an object that one can at least formaily attribute measurabie properties to it in a continuous manner even at times when it is not under observation? The answer is No, as this new theory shows by its internal consistency and by its impressive applications. It is enough, evidently, that the properties of the object should be present at the moment they are measured and that they should be predicted by theory in agreement with experiment.

In the limiting case of macroscopic phenomena, quantum theory rejoins classical theory. Thus it justifies the use of the "naive" concept of "objectivity" and at the same time specifies the limitations of this concept.

What has just been said relates to an important philosophical problem that we cannot enter into here: the determination of the necessary and sufficient conditions for an object of thought to possess objectivity and to be an object of science. This problem was perhaps posed for the first time in any general way by such mathematicians as Malebranche, Leibniz, and especially by B. Bolzano. More recently Husserl (1901, 1913; see also the rather similar ideas in Cassirer, 1910, 1936) has systematically studied such questions and has thus created a new method of investigation called "Phenomenology."

Physics insofar as it is an empirical science cannot enter into such problems in all their generality. It is satisfied to use philosophical concepts sufficient for its needs; but on occasion it can recognize that some of the concepts that once served it have become quite unnecessary, that they contain elements that are useless and even incorrect, actual obstacles to progress. One can doubt the possibility of establishing philosophical truths by the methods of physics, but it is surely not outside the competence of physicists to demonstrate that certain statements which pretend to have a philosophical validity do not. And sometimes these "negative" philosophical discoveries by physicists are no less important, no less revolutionary for philosophy than the discoveries of recognized philosophers.

25.2 II. 2 Interpretation of Quantum Mechanics by Wigner

25.2.1 §1. Problems Raised by Quantum Theory Before the Advent of Quantum Mechanics

The conceptual problems generated by the generally accepted interpretation of quantum mechanics overshadow in philosophical depth those generated by the older quantum theory (see for example the collections of basic papers edited by ter Haar, 1967, and Kangro, 1972) to such an extent that one is likely to forget the latter. Nevertheless, these were very real also, though more concrete and lying more within physics proper than those generated by quantum mechanics.

The idea of the quantum emission and absorption of radiation was conceived by M. Planck (1900a, b) in order to explain the finite energy density of the black body radiation. Classical electrodynamic theory gave an infinite density for this radiation. The energy density per unit frequency, as calculated on the basis of this theory, was

$$8\pi v^2 kT/c^3$$

and the integral of this over the frequency v is clearly infinite. Partly on the basis of experimental information, partly on intuition, and partly to maintain conformance with Wien's displacement law, Planck replaced this by

$$\frac{8\pi h v^3/c^3}{e^{hv/kT}-1},$$

Lectures originally given in the Physics Department of Princeton University during 1976, as revised for publication, 1981. Copyright 1983, Princeton University Press.
and in order to "explain" it, postulated that both emission and absorption of radiation occur instantaneously and in finite quanta. It may be worth mentioning that, somewhat latcr, rcalizing how drastic this assumption was, he modified it somewhat, postulating that the absorption is a continuous process. [An account of the history of Planck's black body theory and of its influence on the development of quantum mechanics can be found in a book by Kuhn(19/8) which contains aiso an extensive list of references. -Eds.]

Bohr's postulate of the quantum condition for the electronic orbits was the second building block of pre-quantum-mechanical quantum theory. This also was highly successful, explaining the spectrum of atomic hydrogen clearly and also, in a qualitaiive, but only qualitative way, the periodic system and hence some basic pronerties of all atoms (Bohr, 1913a.b.c; 1914; 1915a,b). The latter considerations were qualitative and it remains true that, in spite of many efforts, no mathematically consistent rules could be formulated specifying the orbits of eiectrons in systems with more than a single clectron. In spite of this, the picture, analogous to the present Hartree-Fock picture, was quite successful. Nevertheless, the absence of mathematically consistent rules on the basis of which the electronic orbits, and hence the energy levels, could be determined was greatly disturbing. In addition, it was, of course, a mystery how the electron jumps from one precisely defined orbit to another. The problems which were most deeply felt were, however, different, and were concerned principally with the flow of the conserved quantities, such as energy.

The large cross section of atoms for the absorption of light, which, for instance, for the Na resonance radiation is around 10^{-9} cm^2, was in agreement with classical electromagnetic theory but difficult to understand if light consisted of quanta with a point-like structure, since the radii of atoms are around 3×10^{-8} cm. On the other hand, the uniform spread of the radiation energy over the area of the light beam, as postulated by classical theory, was in apparent contradiction with the fact that the emission of the photoelectrons was not delayed

by a decrease of the intensity of the light beam-not even if the average energy incident on an atom on the surface of the electron emitter was less inan a thousandth of the energy needed to liberate the electron. This did indicate a concentration of the energy in point-like quanta, so that the striking of an atom by a quantum could furnish the energy needed to liberate the electron. In order to reconcile the two phenomena, Bohr, Kramers, and Slater (1924) postulated that the conservation law of energy is valid only statistically. However, the experiments of Bothe and Geiger (1924), and of Compton and Simon (1952a,b,c), refuted this assumption.

Another phenomenon which was difficult to explain was the Stern-Gerlach effect (Gerlach and Stern, 1921; 1922). A beam of silver atoms is split, by an inhomogeneous magnetic field, into two beams, such that the angular momentum of the atoms in one of the beams has a definite direction, and that of the atoms in the other beam has the opposite direction. Originally, evidently, the angular momenta
were randomly oriented. How could they all assume one of two definite directions? Surcly the final state must depend continuousiy on ine intial state. It was aiso perturbing that the classical picture, developed by Fhrenfest, could not account for the transfer of the angular momentum to those atoms whose angular momentum included, originally, a considerable angle with both of the two final momentum directions (Einstein and Elrenfesi, 1922).

As the last example of the difficulties, chemical association reactions may be mentioned. An illustration is $2NO_2 \rightarrow N_2O_4$. For such a reaction to take place, the two associating molecules must collide with an energy which corresponds to one of the energy levels of the compound molecule, N_2O_4 in the example cited. This has a small probability but since the levels of the compound molecule have a certain width-this was already recognized before the advent of quantum mechanics-it is not entirely impossible. However, the angular momentum of the compound is strictily quantized and the probability of a collision with a sharply defined angular momentum surely has zero probability. In spite of this, association reactions do take place. How this happens was at least as much of a mystery as how the electron from one orbit of the hydrogen atom jumps into another, equally sharpiy defined, orbit. n explanation was proposed by Polanyi and Wigner (1925): that the angular momentum (as considered from the coordinate system in which the total center of mass is at rest) is increased, as a result of the collision, to the nearest integer multiple of $\hbar$-an assumption leading to very nearly correct results but surely in contradiction to a basic conservation theorem.

All the phenomena mentioned were very puzzling so puzzling indecd that many physicists doubted that a rational explanation of quantum phenomena would ever be found. It may be worthwhile, therefore, to mention Einstein's suggestion for overcoming the paradox mentioned in connection with the photoelectric effect. He believed in the concentration of the energy in quanta and that these quanta have structures similar to particles. However, their motion is governed by what he called Fhrungsfeld-that is, "guiding field"—and this obeys the equations of electrodynamics. In this way the existence of interference phenomena could be reconciled with the concentration of cncrgy in very small-perhaps infinitesimally small-volumes. However, the picture could not be reconciled with the conservation laws for energy and momentum, and Einstein firmly believed in these. As a result Einstein never published the Fhrungsfeld idea. Schrödinger's theory (1926) reconciled the two postulatcs: his Fhrungsfeld the Schrödinger wave, moved not in ordinary space, but in configuration space and referred not to single particles, but to the change of the configuration of the whole system, i.e., the motion of all particles. However, his theory was not a pre-quantum-mechanical theory but a fascinating reformulation and even reinterpretation of the original Heisenberg-Born-Jordan (Heisenberg, 1925; Born and Jordan, 1925; Born, Heisenberg, and Jordan, 1926) quantum mechanics which, originally, attempted only the calculation of energy levels and transition probabilities.

It may be useful, at this point, to recall a few dates:

1900-(Dec. 14) M. Planck announces his quantum theory (Planck, 1900a, b).

1905-Einstein proposes his law of the photoelectric effect (actually, the Nobel prize was awarded to Einstein for this, not for his theory of relativity) (Einstein, 1905).
1913 – N. Bohr's theory of the **H** atom ($\bar{B}0hr, 1913\mathrm{a}, \mathrm{b}, \mathrm{c}$).
1914 The experiment of Franck and Hertz (1914).
1916-Einstein's derivation of Planck's black-body-radiation formula (Einstein, 1916a,b; 1917a).
1921 -Stern-Gerlach experiment (Gerlach and Stern, 1921).
1923-L. de Broglie suggests that matter also has a wave nature (de Broglie, 1923a.b.c; 1924a.b.c.d.e; 1925; 1926).
1925-W. Heisenberg's article which was to form the basis of matrix mechanics (Heisenberg, 1925).
1925-M. Born and P. Jordan cstablish matrix mechanics (Born and Jordan, 1925).
1926-E. Schrödinger proposes his equations of wave mechanics (Schrödinger, 1926, 1930).
1927-Davisson and Germer verify the wave nature of matter by their interference experiment (Davisson and Germer, 1927).
1927 -W. Heisenberg's article "Uber den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik"-the uncertainty principle (Heisenberg, 1927).

At first, it was difficult for the community of physicists to accept Planck's quantum idea of absorption and emission of radiation. In fact he himself proposed a modification of it which, he expected, would make it more palatable: hc suggested that only the emission process is instantaneous, while the absorption of light is a continuous process (Kuhn, 1978). Einstein was the first to accept Planck's original idea at face value and his proposal of the law of photoelectric emission was a result of this. As to the interpretation of the Schrödinger waves as Fhriangsfeld, this became generally accepted as a result of Heisenberg's 1927 paper. This paper also convinced most physicists that it is not meaningful to attribute a definite orbit, or a definite path, to particles - that the concepts in terms of which classical mechanics characterizes the states of a particle are not applicable in the microscopic domain.

Actually, Heisenberg's argument was not entirely rigorous - it was based on the analysis of measurements by means of a %-ray microscope, but the analysis was not complete in all details. Nevertheless, the article had a profound influence. One can substitute for Heisenberg's γ-ray microscope the measurement of position by means of a light quantum sent out toward the object at time t_1, reflected by it, and received at the position of the emission at time t_2 (Figure 1). The collision of the light quantum with the object occurred at time

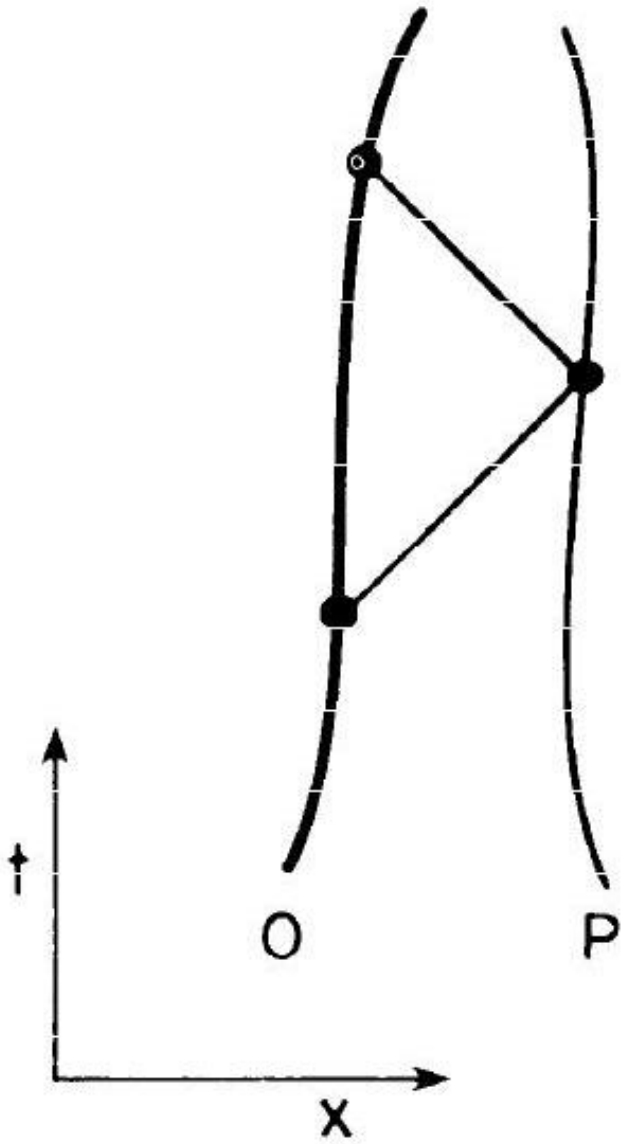


figure 1. The uncertainty principle, illustrated for the paticie, P. The observer, O, sends out a pulse of light at t_1 and receives this pulse, reflected, at t_2. The distance of the particle is determined to be $(t_2 - t_1)/2$, but only with the accuracy of the length of the pulse. The momentum of the particles is uncertain to the extent of the kick the photon has given to it-i.e., at least $\sim h/[$ the length of the pulse].

$$t_{\text{collision}} = \frac{1}{2}(t_1 + t_2) \tag{1}$$

and the object's position at that time was

$$x_{\text{collision}} = \frac{1}{2}c(t_2 - t_1). \tag{1a}$$

However, the times t_1 and t_2 cannot be measured exactly because the light quantum's ficld had to have a finite extension, to be denoted by Δx. Its frequency, hence, was indeterminate to the extent $c/\Delta x$, its energy had an uncertainty $hc/\Delta x$, and its momentum $h/\Delta x$. It imparted twice its momentum to the particle; thus even if the momentum of this was accurately known before the measurement, after the measurement it was uncertain to about $\Delta p = 2h/\Delta x$. Hence the measurement described permitted the determination of the position only with an accuracy of the order $\Delta x \approx h/\Delta p-$ the conclusion arrived at by Heisenberg. The point is that the measurement described could be made accurate only if one had a light wave of sharply defined

frequency which was at the same time accurately localized in space. The two requirements cannot be met simultaneously.

Let us now give a mathematical proof of the uncertainty relation. We will give two different proofs, the second one of which is due to H. P. Robertson (1929).

We consider a system of units in which $\hbar(\equiv h/2\pi) = 1$. Then we have

$$\bar{x} = \int |\psi(x)|^2 x dx, \quad \bar{p} = \int |\phi(p)|^2 p dp \tag{2a}$$

with

$$\phi(p) = \frac{1}{\sqrt{2\pi}} \int \psi(x) e^{-ipx} dx \tag{2b}$$

Now it will simplify the calculation a bit to set $\bar{x} = 0$ and $\bar{p} = 0$. This represents no loss of generality as it merely amounts to a change of the integration variable as far as x is concerned and a multiplication of ψ by $\exp(-i\bar{p}x)$ to annul the new $\bar{p}$. The uncertainties $\Delta x, \Delta p$ are then defined by

$$(\Delta x)^2 = \int |\psi(x)|^2 x^2 dx \tag{3a}$$

and

$$(\Delta p)^2 = \int |\phi(p)|^2 p^2 dp = \int |\partial\psi/\partial x|^2 dx \tag{3b}$$

We want to prove that for every state

$$(\Delta x)^2 (\Delta p)^2 \geq \frac{1}{4}.$$

We can restrict ourselves without loss of generaiity to the case where the two uncertainties are equal. This is so because the substitution of $\psi_{\text{new}}(x) = \sqrt{\alpha}\psi(\alpha x)$ (the $\sqrt{\alpha}$ is inserted to keep ψ_{new} normalized) decreases Δx by α and increases Δp by α. It does not change $\Delta x \Delta p$, but makes it possible to adjust them so that Δx and Δp become equal. Hence, we can assume that this is the case and we can set

$$\begin{aligned} \Delta x \Delta p &= \frac{1}{2}\left[(\Delta x)^2 + (\Delta p)^2\right] \\ &= \frac{1}{2}\int \left[x^2|\psi(x)|^2 + |\partial\psi/\partial x|^2\right] dx \end{aligned} \tag{4}$$

This is the functional that gives the energy of the harmonic oscillator. It is minimized by $\psi = c\exp(-x^2/2)$ (c is the normalization constant, $\pi^{-1/4}$). The two terms inside the integral of (4) are then indeed equal, and equal to $\frac{1}{2}$, and add to unity. Hence we find, in this case,

$$\Delta x \Delta p \geq \frac{1}{2} \tag{5}$$

and, by virtue of the remark before (4), this holds also generally, as we wanted to show.

The second proof goes as follows. One writes

$$\int \psi^* \left(-x\frac{\dot{C}}{\dot{C}x}\right)\psi dx = a, \quad \int \psi^* \left(\frac{\dot{C}}{\dot{C}x}x\right)\psi dx = b \tag{'6}$$

the star denoting transition to the conjugate complex. Then, because of the normalization of ψ, we know that

$$\int \psi^* \left(-x\frac{\partial}{\partial x} + \frac{\partial}{\partial x}x\right)\psi dx = \int \psi^*\psi dx = \int |\psi|^2 dx = 1$$

or

$$a + b = 1 \tag{6a}$$

Now, by Schwartz's inequality, we have

$$|a|^2 = \left|\int \psi^* x \frac{\partial\psi}{\partial x} dx\right|^2 \leq \int |x\psi(x)|^2 dx \int \left|\frac{\partial\psi}{\partial x}\right|^2 dx \tag{7}$$

so (again assuming for simplicity $\bar{x} = \bar{p} = 0$)

$$|a|^2 \leq (\Delta x)^2(\Delta p)^2 \tag{8}$$

Next one recognizes by partial integration that

$$\dot{b} = a^* \tag{9}$$

This means that if we set

$$a = u + iv \tag{9a}$$

we must have, by (6a),

$$2u = 1 \tag{9b}$$

This result in turn implies

$$|a|^2 = u^2 + v^2 \geq \frac{1}{4} \tag{10}$$

and this together with (7) again proves (5).

It is worthwhile to remark here that the above "proof" for the uncertainty relation is fundamentally different from Heisenberg's. Like equations (3a) and (3b), it is based on the statistical interpretation of (nonrelativistic) quantum mechanics. Those equations do not refer to the actual ways x and p could be measured - the subjects of Heisenberg's article. Thus, they avoid the basic question: how is a measurement to be carried out, how do we prepare the object on which the measurement is taking place? They assume that the probabilities of the various out- of the measurement of x and p are correctly given by the present quantum comes of the measunclusion we obtained is of a statistical nature: There is no state of any system such that the results of the measurements of x and p would be predictable with greater accuracies Δx and Δp inan are indicated by (5). Evidentiy, the verification of this statement requires, first, the repeated production of the same state many times so that the statistical distribution of the outcomes of the measurements of x and of p can be ascertained. This is in itself a difficult problem; one can never be absolutely sure that one has produced the same state of the system. At the first preparation somebody may have looked on-can we be sure that this did not affect the state of the system produced? Similar remarks apply to the measurements. There is also the question: When is the measurement completed? We will see that, if we adhere strictiy to the principies of quantum mechanics, the measurement is completed only when we have observed its outcome, i.e., have read the recording of the measuring apparatus. Apparently, this is not a precisely repeatable process. Could the fluctuations of the outcome of the measurements of

x and p come from these sources? Evidently we believe that this is not the case; but it would be difficult to explain this belief convincingly to a fully detached person. In spite of this, we are all fully convinced of all this and do not believe that any refinement of the preparation of the system the x and p of which is to be measured, or any improvement of the measuring technique, would lead to a violation of (5).

Before going into a more detailed discussion of these questions, we will review the mathematical structure of quantum mechanics, its description of states, and its calculation of the probabilities of the outcomes of measurements. The equations used to derive (5) will naturally appear as special cases of the general theory.

25.2.2 §2. the Mathematical Formalism of Quantum Mechanics

Hilbert Space

In quantum mechanics, as in classical physics, we postulate the existence of isolated systems. In both theories, if a complete description of an isolated system is given at one time, a complete description for any other time is uniquely determined as long as the system remains isolated-i.e., is not influenced by any other system. In this sense, both theories are deterministic. The means of description of the state of the system have, however, undergone drastic changes over the course of the history of physics. In the original Newtonian mechanics, the state of the system was described by the positions and velocities of its constituents. In the later field theories, it was described by the field strengths at all points of space-that is, by one or more-in the case of electrodynamics six-functions of three real variables, the latter characterizing the points of ordinary space. The usual quantum-mechanical description of the state of a system is much more
abstract: it is given by a vector (or, more accurately, by a ray) in an abstract complex Hilbert space. This vector is usually called the state vector. Since the Hilbert space has infinitely many dimensions, this amounts to the specification of the state by an infinite set of complex numbers, $a_1, a_2, a_3, \ldots$, the components of the state vector in Hilbert space, which however, satisfy the condition that the sum

$$\sum |a_i|^2 < \infty \tag{1}$$

is finite. This means that the length of the vectors in Hilbert space is finite. Furthermore, it is postulated that two state vectors which have the same direction, i.e., the components of which differ only by a common factor, characterize the same state. The set of vectors the components of which differ only by a common factor, e.g., the vectors with the components $a_1, a_2, a_3 \ldots$ and the vectors $ca_1, ca_2, ca_3 \ldots$ for any $c \neq 0$, arc said to form a ray. We can choose, therefore, one of these vectors to describe the state, and we usually choose one that is normalized, i.e., one for which

$$\sum |a_i|^2 = 1 \tag{1a}$$

The different normalized vectors describing the same state differ only by a factor ω of modiulus 1 .

Schrödinger's original formulation of his "wave mechanics" was, of course, not in terms of the Hilbert space. Wave mechanics characterized the states of systems in terms of complex valued functions, actually functions in configuration space. However, if one introduces an orthonormal set of functions $u_n(x_1, x_2 \ldots)$ in any space,

$$\int \cdots \int u_n(x_1, x_2 \ldots)^* u_m(x_1, x_2 \ldots) dx_1 dx_2 \cdots = \delta_{nm} \tag{2}$$

one can expand the wave function ψ of any state in terms of this set. Thus,

$$\psi(x_1, x_2 \ldots) = \sum a_n u_n(x_1, x_2 \ldots) \tag{2a}$$

$$a_n = \iint u_n(x_1, x_2 \ldots)^* \psi(x_1, x_2 \ldots) dx_1 dx_2 \ldots \tag{2b}$$

and the numbers a_n can be considered to be the components of a vector in Hilbert space as long as

$$\int \cdots \int |\psi(x_1, x_2 \cdots)|^2 dx_1 dx_2 \cdots = \sum |a_n|^2 \tag{2c}$$

is finite - which we assume to be the case for Schrödinger's wave functions.

It may be worthwhile to observe at this point that the correspondence between functions ψ and the corresponding vector a in Hilbert space is not one to one. Two functions ψ and ψ which differ oniy on a set of measure 0 (for instance only on a denumerable set of points) correspond to the same vector in Hilbert space. However, this observation rarely plays an important role in actual calculations.

The most important derivative concept in Hilbert space is that of the scalar product. The scalar product of two vectors a and b is defined as

$$(a, b) = \sum a_n^* b_n \tag{3}$$

In terms of the wave functions this is

$$\begin{aligned}(\psi, \phi) &= \int \cdots \int \psi(x_1, x_2 \ldots)^* \phi(x_1, x_2 \ldots) dx_1 dx_2 \cdots \\ &= \sum a_n^* b_n \end{aligned} \tag{3a}$$

the last part of the equation being valid if the a are, according to (2a), the expansion coefficients of ψ and the b are, similarly, the expansion coefficients of ϕ. That the sum in (3) is finite follows from (1), and the similar restriction follows for b. by means of Schwartz's inequality. It follows from (3) or (3a) also that

$$(a, b) = (b, a)^* \tag{3b}$$

the star denoting, as before, the conjugate complex.

If a and b are normalized according to (1a), the absolute square $|(a, b)|^2$ of the scalar product (a, b) is called, for reasons which will appear soon, the transition probability from the state a into the state b-or conversely, because of (3b). Otherwise, the transition probability is

$$\frac{|(a, b)|^2}{(a, a)(b, b)} \tag{4}$$

It may be worth remarking that (a, a) is real and also positive unless $a = 0$, and that the scalar product is linear in the second factor,

$$(a, \beta b + \beta' b') = \beta(a, b) + \beta'(ab') \tag{5}$$

and antilinear in the first factor,

$$(\alpha a + \alpha' a', b) = \alpha^*(a, b) + \alpha'^*(a', b) \tag{5a}$$

where α, α', β, and β' are arbitrary complex numbers. These equations are immediate consequences of the definition (3) of the scalar product.

Linear Operators in Hilbert Space

An operator in Hilbert space transforms a vector in Hilbert space into another (or the same) vector in the same space. One should really write $A(\phi)$ for the vector into which the operator A transforms the vector ϕ, but, at least for linear operators A, one writes $A\phi$ instead. An operator A is called linear if for any two vectors ϕ, ψ and any two numbers α, β

$$A(\alpha\phi + \beta\psi) = \alpha A\phi + \beta A\psi \tag{6}$$

holds. More generally, one can write

$$A\left(\sum a_n\psi_n\right) = \sum a_n A\psi_n \tag{6a}$$

Hence if we assume that the ψ_n in (6a) form a complete orthonormal set of vectors, and if we expand the $A\psi_n$ in terms of these vectors, we can write

$$A\dot{\psi}_n = \sum_m A_{mn}\psi_m \tag{7}$$

Then (6a) gives for the transformation properties of the coefficients a_n,

$$a_n \to \sum_m A_{nm}a_m \tag{7a}$$

The operation A acts on the expansion coefficients as the matrix (A_{nm}), the matrix elements of which are, because of (7)

$$A_{mn} = (\psi_m, A\psi_n) \tag{7h}$$

The last two equations are valid if the ψ_m form a complete orthonormal set; but (6a) is valid as a consequence of (6) for any set of vectors ψ_m.

Two special kinds of linear operators play particularly important roles in quantum mechanics. The invariance transformations, such as the time-displacement transformation, are mediated by unitary transformations U which leave the scalar products, and hence the transition probabilities (4), between any two vectors unchanged:

$$(U\phi, U\psi) = (\phi, \psi) \tag{8}$$

They will play a lesser role in the considerations which follows. The other special kind of linear operators of basic significance for what follows are the self-adjoint
operators. In order to define them, one first defines the adjoint $A^\dagger$ to an operator A. This is so defined that for any two vectors ϕ and ψ,

$$(\phi, A\psi) = \left(A^\dagger\phi, \psi\right) \tag{9}$$

is valid. One concludes from (9) and (3b) that

$$(A\psi, \phi) = \left(\psi, A^\dagger\phi\right) \tag{9a}$$

so that A is the adjoint of $A^\dagger$ if $A^\dagger$ is the adjoint of A. The matrix elements of $A^\dagger$ are, as one can infer from (7b),

$$\left(A^\dagger\right)_{nm} = A^*_{mn} \tag{9b}$$

i.e., the matrices of A and $A^\dagger$ are what we call hermitian adjoints. The second type of operators of basic significance can now be defined. They are those which are equal to their adjoints.

$$A = A^{\dagger} \tag{10}$$

In the corresponding matrices the matrix elements which lie symmetrically with respect to the main diagonal are the conjugate compiexes of each viture.

For the sake of accuracy it should be pointed out that the existence of the adjoint $A^{\dagger}$ to an arbitrary linear operator is by no means obvious, and requires, if all the questions of convergence are to be treated rigorously, a reasonably elaborate proof (von Neumann, 1932). Once its existence is established, i.e., once it is shown that there is a ϕ' independent of ψ satisfying the equation

$$(\phi, A\psi) = (\phi', \psi) \tag{11}$$

(ϕ' depending only on $\boldsymbol{A}$ and ϕ), the linear dependence of this $\phi' = A^{+}\psi$ on ψ is easily proved. We have on the one hand,

$$(\alpha\phi_1 + \beta\phi_2, A\psi) = \left[A^{\dagger}\left(\alpha\phi_1 + \beta\phi_2\right), \psi\right] \tag{12}$$

and on the other,

$$\begin{aligned}(\alpha\phi_1 + \beta\phi_2, A\psi) &= \alpha^{*}\left(\phi_1, A\psi\right) + \beta^{*}\left(\phi_2, A\psi\right) \\ &= \alpha^{*}\left(A^{\dagger}\phi_1, \psi\right) + \beta^{*}\left(A^{\dagger}\phi_2, \psi\right) \\ &= \left(\alpha A^{\dagger}\phi_1 + \beta A^{\dagger}\phi_2, \psi\right)\end{aligned} \tag{12a}$$

Hence the right sides of (12) and (12a) are equal and, since this is true for every ψ,

$$A^{\dagger}\left(\alpha\phi_1 + \beta\phi_2\right) = \alpha A^{\dagger}\phi_1 + \beta A^{\dagger}\phi_2, \tag{12b}$$

i.e., $A^{+}$is linear.

Normal Form of Self-Adjoint Operators

Except for the proof of the existence of the hermitian adjoint $A^{\dagger}$, the preceding discussion is straightforward and easy. This is not the case for the following discussion, particularly not if the concept of the operator is extended so that it encompasses also unbounded operators. The following discussion gives only the results. The detailed proofs can be found, for instance, in the book of J. von Neumann (1932) or in the book of G. R. Mackey (1963).

Let us consider first bounded self-adjoint operators, i.e., operators such that $(A\psi, A\psi)$ has an upper limit. The usual procedure to obtain the normal form is to look for the characteristic vectors ψ_v of A

$$A\psi_v = \lambda_v\psi_v. \tag{13}$$

One casily sees that the chatacteristic values λ_v have to be real and the characteristic vectors ψ_v, which are solutions for different λ_v, are orthogonal. We assume that they are also normalized, i.e., that $(\psi_v, \psi_v) = 1$. If the characteristic vectors ψ_v form a complete orthonormal set, we say that A has only a point spectrum, this consisting of the λ_v. The effect of A on an arbitrary vector ϕ

$$\phi = \sum\left(\psi_v, \phi\right)\psi_v \tag{14}$$

is then, because of its linear character,

$$A\phi = A\sum(\psi_v, \phi)\,\psi_v = \sum(\psi_v, \phi)\,A\psi_v$$
$$= \sum(\psi_v, \phi)\,\lambda_v\psi_v. \tag{14a}$$

The measurement theory then posituates that the measurement of A on a system in the state ϕ gives one of the values λ and that it gives the value λ_v with the probability

$$p_v = |(\psi_v, \phi)|^2. \tag{15}$$

It is assumed here that ϕ and the ψ_v are normalized,

$$(\phi, \phi) = (\psi_v, \psi_v) = 1. \tag{15a}$$

It is also reasonable to assume that the system which was originally in the state ϕ is, after the measurement-if the result of that is λ_v-in the state ψ_v. Naturally it would be good to justify this postulate of measurement theory by means of
the equations of motion of quantum mechanics-that is, to decribe the measurement process. Such an analysis would have to treat in quantum-mechanical language the apparatus used for the measurement of A. We will discuss later the extent to which this has so far proved to he possible, and the examples which show that for certain A it is impossible.

The preceding remarks apply to a self-adjoint operator which has a point spectrum only. One can well say that most operators do not have such a spectrum. A self-adjoint operator may have a continuous spectrum also-or only a continuous spectrum. In other words the solutions ψ_v of (13)-with a finite length so that (15a) can be made valid-may not form a complete set. In fact, there may be no such soiution at ali; that is, there may be no vector ψ_v in Hiibert space which satisfies (13) for some λ_v. In the general case the preceding equations have to be replaced by much more complicated ones. In order to illustrate this point, it is helpful to rewrite (14) and (15) somewhat by decomposing A into projection operators $\bar{P}_v$. A projection operator is defined by

$$P_v\phi = (\psi_v, \phi)\,\psi_v. \tag{16}$$

It then follows from (14) that

$$\sum P_v = 1, \tag{17}$$

and from (14a).

$$\sum \lambda_v P_v = A. \tag{17a}$$

One easily verifies that the P_v are self-adjoint, identical with their squares, and more generally satisfy the equations,

$$P_v P_\mu = \delta_{v\mu} P_v \tag{17b}$$

In fact,

$$P_v P_\mu \phi = P_v\,(P_\mu\phi) = P_v\,(\psi_\mu, \phi)\,\psi_\mu = (\psi_\mu, \phi)\,P_v\psi_\mu$$
$$= (\psi_\mu, \phi)\,(\psi_v, \psi_\mu)\,\psi_v = \delta_{v\mu}\,(\psi_\mu, \phi)\,\psi_v = \delta_{v\mu}P_v\phi. \tag{17c}$$

The expression for the transition probability into ψ_v - which is also the probability that the outcome of the measurement of A on ϕ will be λ_v-becomes, in terms of P_v,

$$p_v = (\phi, P_v \phi)\,. \tag{18}$$

One can also write this in the form

$$p_v = (P_v \phi, P_v \phi) \tag{18a}$$

as, because of the self-adjoint nature of P_v and (17),

$$(\boldsymbol{P}_v \phi, \boldsymbol{P}_v \phi) = \left(\phi, \boldsymbol{P}_v^2 \phi\right) = (\phi, \boldsymbol{P}_v \phi) \tag{18b}$$

The derivation so far has supposed that A has only a discrete spectrum, a condition for the validity of equations (17).

We now proceed to the more general case that A may also have a continuous spectrum. In this case one has to admit that the measurement will not yield a mathematically precise value - no one asks whether the outcome of this measurement is a rational or irrational number. It is more reasonable to ask, for instance, whether the outcome is smaller than a number λ. The probability for a "yes" answer to this question can be written, in the case of a discrete spectrum, as

$$p(\lambda) = [\phi, P(\lambda)\phi]. \tag{19}$$

Here

$$P(\lambda) = \sum_{\lambda v < \lambda} P_v \tag{19a}$$

It then follows from (18) that the probability for an outcome of the measurement between λ and $\lambda > \lambda'$ is

$$p(\hat{\lambda}) - p\left(\hat{\lambda}'\right) = \{\phi, [P(\lambda) - P\,(\lambda')]\,\phi\} \tag{20}$$

it foilows from the theory of self-adjoint operators in Hilbert space that the operators $P(\lambda)$ can also be defined if the spectrum is not exclusively discrete. In other words, the $P(\lambda)$ can be defined for every self-adjoint operator, for any real λ. One clearly has

$$P(\lambda) \to 0 \text{ for } \lambda \to -\infty \tag{21a}$$

and the analogs of (17) and (176) are

$$P(\lambda) \to 1 \text{ for } \lambda \to \infty \tag{21b}$$

and

$$P(\lambda) P\,(\lambda') = P\,(\lambda')\,P(\lambda) = P\,(\lambda') \text{ for } \lambda' \leq \lambda \tag{21c}$$

These equations, of course, do not determine the $P(\hat{\lambda})$ since they do not involve A. In order fully to define the $P(\hat{\lambda})$, one has to write the analog of (17a). This becomes, in the general case, a somewhat complicated expression-a limit of a sum with increasingly many terms. One has to form series of increasingly many λ values which cover the real line with increasing density. If the density is $1/N$, one has the series

$$A = \sum_{n=-\infty}^{\infty} \sum_{m=1}^{N} (n + m/N)[P(n + m/N) - P(n + (m-1)/N)] \tag{22}$$

and this is valid in the limit $N = \infty$. Naturally, this is a special form for A in which the distance between successive λ values is uniformly $1/N$. There are infinitely many other ways to increase the density of the λ. The mathematician writes a Sticltjcs integral for (22) and, in fact, (22) is the definition of the Stieltjes integral. The expression for A is written in the elementary form (22) because it does not presuppose familiarity with that integral. The point is that (22), together with the equations (21), fully defines the λ and hence determines the mathematical expression (20) for the probability of the outcome of the measurement of A lying between λ' and λ.

A few remarks are needed to complete the discussion. First, the possibility of finding a mathematical expression for the outcome of the measurement of an operator obviousiy dues not guarantee the possibility of such a measurement. Second, the theory postulates measurements corresponding to operators, not to classical quantities. Originally, the attempt was made to define operators to correspond to classical quantities. The present theory does not strive for such a coordination. Thus, one does not try to choose, for instance, between $\left(px^2 + x^2p\right)/2$ and xpx as operators to correspond to the classical quantity, "product of the square of the coordinate and first power of the momentum." Instead, one asks if an experimental device can be constructed that will realize a measurement of the operator $\left(px^2 + x^2p\right)/2$ and whether another can be built that will measure xpx.

On the mathematical side if A is bounded, $P(\lambda)$ remains 0 up to the lower bound of A and becomes 1 at the upper bound. Hence that part of the sum in (22) vanishes for which $n+m/N$ is below the lower bound; and so does that which is above the upper bound. However, and this theorem is due to von Neumann (1932), the preceding equations as written are valid also for general self-adjoint operators, not only for bounded ones. It is worthwhile, nevertheless, to add a few words relating to the former, since most common operators are not bounded. There are vectors in Hilbert space to which an unbounded operator cannot be applied. Both multiplication by x and $i\partial/\partial x$ are unbounded operators. For instance, multiplication of the state vector $1/(i+x)$ by x does not produce a state vector, since $\psi(x) = x/(i+x)$ is not square integrable; for it the expression (2c) is infinite. For an unbounded operator it is postulated only that there be an everywhere dense set of vectors to which it can be applied-i.e., that in the neighborhood of any chosen vector there be vectors arbitrarily close to it to which the operator can be applied. In the case of $1/(i+x)$ such vectors are, for instance $e^{-\varepsilon x^2}/(i+x)$ with decreasing values of ε. In fact, the square of the difference vector,

$$\int \left| \frac{1}{i+x} - \frac{e^{-\varepsilon x^2}}{i+x} \right|^2 dx \tag{23}$$

goes to zero as ε goes to zero. Moreover, multiplication with x leaves $e^{-\varepsilon x^2}/(i+x)$ within the Hilbert space no matter how small ε is, as long as it remains positive.

It is remaikable that the probability of the outcome of measurements, given by (20), is well defined even for unbounded operators, even in the case of state vectors ϕ to which the unbounded operator cannot be applied. The intrinsic reason for this is that the measurement hardly refers to the operator and its spectrum - what it really purports to define is the transition probability into the state $\left[P(\lambda) - P\left(\lambda'\right)\right]\phi$ if the original state was ϕ. The projection operators $P(\lambda)$ could be given other labels, such as $\lambda/\left(\lambda^2+1\right)^{1/2}$, and the measurement would still be the same, only its outcome would be called differently. To repeat, however, all this is theory, and there is no mathematical guarantee that even a transition probability into an arbitrary state can be measured. In order to guarantee the possibility of such a measurement one would have to describe a way to do it. The mathematical theory of the measurement, as formulated first by von Neumann but now generally accepted, ingenious as ii is, does noi do that.

It may be worthwhile to observe, nevertheless, that the self-adjoint nature of an unbounded

operator imposes rather rigorous criteria. First, the operator and its adjoint must give the same vector if applied to a vector which lies in the intersection of the domains of definition of the two operators. Second, the two domains of definition must be identical (von Neumann called them hypermaximal). Fortunately, this criterion apparently plays no practical role in the theory.

25.2.3 §3. Direct Product and Quantum Mechanical Description of the Measuring Process

The Direct Product of Hilbert Spaces

Starting from two Hilbert spaces, one can construct a single larger Hilbert space, a sort of union of the two. If the axes of the first Hilbert space are specified by Greek indices v. and of the second by Latin indices such as n, then the axes of the direct product are specified by a double index, such as vn. Thus vn specifies a single axis of the Hilbert space which is the direct product of the original two Hilbert spaces. The number of axes vn is still denumerable even though it appears to be greater than the number of axes of the factors: one can order pairs of ordered numbers into a single series such as $11; 12.21; 13, 22, 31; 14, 23$, and so on. The components Ψ_{vn} of a vector Ψ in the space of the direct product have two indices, and the scalar product of two vectors Ψ and Φ in that space is

$$(\Psi, \Phi) = \sum_{vn} \Psi^*_{vn} \Phi_{vn} \tag{24}$$

The Hilbert space which is the direct product of two Hilbert spaces H_1 and H_2 is usually denoted by $H_1 \otimes H_2$

One also defines the direct product of two vectors, one of which, ϕ, is in H_1, and the other, ψ, in H_2. This direct product, denoted by $\phi \otimes \psi$, is in the space $H_1 \otimes H_2$. Its vn component is

$$(\phi \otimes \psi)_{vn} = \phi_v \psi_n \tag{25}$$

The direct product is linear in its two factors. Thus

$$(\alpha\phi + \alpha'\phi' \otimes \psi) = \alpha(\phi \otimes \psi) + \alpha' (\phi' \otimes \psi) \tag{25a}$$

and a similar equation appiies if ψ is replaced by $\hat{p}\dot{\psi} + \hat{p}\dot{\psi}'$. Th order to verify (25a), one compares the vn components of the two sides. These are $(\alpha\phi + \alpha'\phi')\,\psi_u$ and $\alpha\phi_v\psi_n + \alpha'\phi'_v\psi_n$ and the two are equal.

The square length of $\phi \otimes \psi$ is

$$\begin{aligned}(\phi \otimes \psi, \phi \otimes \psi) - \sum_{vn} |(\phi \otimes \psi)_{vn}|^2 &= \sum_{vn} |\phi_v \psi_n|^2 \\ &= \sum_v |\phi_v|^2 \sum_n |\psi_n|^2\end{aligned} \tag{25a}$$

and is the product of the squares of the lengths of the two factors ϕ and ψ. The scalar product of two direct product vectors $\phi \otimes \psi$ and $\phi' \otimes \psi'$ in the new Hilbert space becomes, similarly,

$$\begin{aligned}(\phi \otimes \psi, \phi' \otimes \psi') = \sum_{vn} (\phi \otimes \psi)^*_{vn} (\phi' \otimes \psi')_{vn} &= \sum_{vn} (\phi_v \psi_n)^* \phi'_v \psi'_n \\ = \sum_v \phi^*_v \phi'_v \sum_n \psi^*_n \psi'_n &= (\phi, \phi')\,(\psi, \psi')\end{aligned} \tag{25b}$$

that is, the product of the scalar products of the two factors.
It is important to remark, finally, that the direct product of two factors ϕ and ψ is the same vector in the new Hilbert space no matter which coordinate systems are used for its definition in (25). If the unit vectors in the direction of the coordinate axes used in (25) for the two Hilbert spaces H_1 and H_2 are denoted by e_v and f_n, the vn component of $\phi \otimes \psi$ is, by (25),

$$(\phi \otimes \psi)_{vn} = \phi_v \psi_n = (e_v, \phi)\,(f_n, \psi) = (e_v \otimes f_n, \phi \otimes \psi) \tag{26}$$

This equation remains valid for any other choice of the coordinate axes in the original Hilbert spaces. One can verify this statement by explicit calculation. It follows from (26) that

$$\phi \otimes \psi = \sum_{vn} (e_v, \phi)\,(f_n, \psi)\, e_v \otimes f_n \tag{26a}$$

Hence, the component of the state vector in the new $e'_\mu \otimes f'_m$ direction becomes

$$\begin{aligned} \left(e'_\mu \otimes f'_m, \phi \otimes \psi\right) &= \sum_{vn} (e_v, \phi)\,(f_n, \psi)\left(e'_\mu \otimes f'_m, e_v \otimes f_n\right) \\ &= \sum_{vn} (e_v, \phi)\,(f_n, \psi)\left(e'_\mu, e_v\right)(f'_m, f_n) \end{aligned} \tag{26b}$$

But we have the equality,

$$\sum_v \left(e'_\mu, e_v\right)(e_v, \phi) = \sum_v \left(\left(e_v, e'_\mu\right) e_v, \phi\right) = \left(e'_\mu, \phi\right); \tag{26c}$$

and a similar equation applies for the f. Therefore, we have verified explicitly that

$$\left(e'_\mu \otimes f'_m, \phi \otimes \psi\right) = \left(e'_\mu, \phi\right)(f'_m, \psi) \tag{26d}$$

This result proves that the equation (25) defining the direct product of the two vectors is independent of the coordinate systems used in the original Hilbert spaces.

The direct product of two Hilbert spaces, and the direct product of vectors in them, is introduced in order to describe the joining of two systems into a single system. This is important if one wants to describe the interaction of two systems which were originally separated-in our case the interaction between the measuring apparatus and the system on which the measurement is undertaken. If it is possible to describe the two systems in separate Hilbert spaces, their union can indeed be most easily characterized in the direct product of these Hilbert spaces. In this "product space" the state vector of the union is the direct product of the state vectors of the components. Indeed, if one wants to calculate the probability that the first system is in state ϕ' and the sccond is in state ψ' when their actual state vectors are ϕ and ψ, one obtains by (25b),

$$|(\phi' \otimes \psi', \phi \otimes \psi)|^2 = |(\phi', \phi)|^2\, |(\psi', \psi)|^2 \tag{27}$$

which is the product of the transition probabilities from ϕ into ϕ' and from ψ into ψ'. Since the two system are assumed to be independent, this is the expected result.

Direct Products of Operators

In order to obtain the more general expressions corresponding to (18), etc. for the joint system, it is useful to introduce the concept of the direct product of two operators A and B, acting in the two original Hilbert spaces H_1 and H_2. The action of A is described by the equation

$$(A\phi)_v = \sum_{v'} A_{v'v}\phi_{v'} \tag{28a}$$

that of B by

$$(\bar{B}\psi)_n = \sum_{n'} \left(\bar{B}_{n'n}\dot{\psi}_{n'} \right. \tag{28b}$$

Their direct product, to be denoted by $A \otimes B$, will then transform Ψ with the components Ψ_{vn} into $A \otimes B\Psi$, the components of which are

$$((A \otimes B)\Psi)_{vn} = \sum_{v'n'} A_{v'v}B_{n'n}\Psi_{v'n} \tag{28}$$

This is the definition of $A \otimes B$. Clearly, if Ψ is a direct product, $\Psi = \phi \otimes \psi$. The action of $A \otimes B$ on this will give

$$(A \otimes B)\phi \otimes \psi = A\phi \otimes B\psi \tag{29}$$

the direct product of the results of the actions of A and of B in their respective Hilbert spaces.

The concept of the direct product of two operators enables us to generalize the expression for the transition probability (27) as the similar expression (15) for a single system was generalized, first in (18) for the case of a discrete spectrum, and then in (19) and (20) to the case where a continuous spectrum may also be present. First, if both operators A and B, to be measured on the two systems, have only a discrete spectrum, then let us denote the projection operators which correspond to the characteristic values α_v of A and b_n of B with P_v and Q_n, respectively. The probability that the outcome is a_v for the measurement of A on ϕ is then $(\phi, P_v\phi)$. The probability that the outcome is b_n for the measurement of B on ψ is $(\psi, Q_n\psi)$. The probability that the two outcomes on the joint system be a_v and b_n is then given by

$$P_{vn} = (\phi \otimes \psi, (P_v \otimes Q_n)(\phi \otimes \psi)) = (\phi, P_v\phi)\left(\psi, \bar{Q}_n\psi\right) \tag{30}$$

as follows from (29). We conclude that $P_v \otimes Q_n$ is the projection operator for the outcome a_v of A and b_n of B. Similarly, we can generalize (19): the probability for A giving a result smaller than $\hat{\lambda}$ and B giving a result smaller than l is

$$p(\lambda, l) = \{\phi \otimes \psi, [P(\lambda) \otimes Q(l)]\phi \otimes \psi\} = [\phi, P(\lambda)\phi][\psi, Q(l)\psi] \tag{31}$$

Here $P(i)$ is defined for operator A as in (19a) and $Q(l)$ is defined similarly for B. Equation (31) is valid even when there is a continuous spectrum. The formula for the probability that the outcomes will fall in the intervals λ_1, λ' and l, l', respectively, is obtained equally easily as

$$\begin{aligned}&[p(\lambda'.l') - p(\lambda.l')] - [p(\lambda'.l) - p(\lambda.l)] \\ &\quad = (\phi \otimes \psi, [P(\lambda') - P(\lambda)][Q(l') - Q(l)]\phi \otimes \psi)\end{aligned} \tag{32}$$

in generalization of (20). The first two terms provide the probability that B will fall below l' and A between λ and λ'. The square bracket gives the probability for the same interval of A and that B will fall below l. Hence (32), the difference between the two, gives the probability that A will fall between $\hat{\lambda}$ and λ' and B between l and l'. The right side is a symmetric expression for this probability. Actually, these formulae are given only for the sake of completeness; they will not bc used. The same applies to the general formula.

$$(A \otimes B)(A' \otimes B') = (AA' \otimes BB') \tag{33}$$

It is worth remembering, though, that the projection operator in the direct product space for the probability of the outcome a_v for A without specification of the outcome for any measurement on the second system is $P_v \otimes 1$; and conversely, it is $1 \otimes Q_n$ for the outcome b_n of B as measured on the second system if no measurement on the first system is undertaken. This concludes our mathematical discussion of the direct product concept.

It should be admitted, however, that the exclusion principle's requirement of the antisymmetrization of the state vector puts a certain restriction on the posiulate that the states of the two noninteracting systems be described in separate Hilbert spaces. As a result of the antisymmetrization, this separation is not actually directly possible. A similar remark applies for particles obeying Bose statistics and demanding a symmetrized state vector. It does not seem, though, that this restriction is truly relevant in the case to be considered: the two Hilbert spaces may describe not the two different objects but the conditions in two distinct parts of space, in our case that of the object and that of the apparatus. It seems that field theories might not encounter this difficulty, but since actually no one seems to believe that a more precise discussion, taking the symmetric or antisymmetric nature of the Schrödinger wave functions into account, would alter any of the conclusions, such a precise discussion of this point does not appear in the literature. It may be true that it would be good to provide such a discussion for the sake of accuracy.

The Quantum Mechanical Description of Measurement

The concept of the direct product greatly facilitates the quantum mechanical description of the measurement process. This consists of a temporary interaction between the object on which the measurement is undertaken and the apparatus which performs the measurement. Let us consider, first, a measurement on an object which is in a state for which the outcome is surely determined-i.e., a state, the state vector σ_κ of which is a characteristic vector of the quantity to be measured.

If we denote the initial state vector of the apparatus by a_0, then the initial state of apparatus plus object is $a_0 \otimes \sigma_\kappa$. After the measurement, the apparatus has assumed a state which shows the outcome of the measurement; we denote its state vector by a_k. Hence, if the object did not change its state as a result of the measurement-this assumption will be discussed further later-the interaction between apparatus and object transforms $a_0 \otimes \sigma_\kappa$ into

$$a_0 \otimes \sigma_\kappa \to a_\kappa \otimes \sigma_\kappa \tag{34}$$

and this is assumed to be valid for all κ. Thus, the art of measuring the quantity with the characteristic vectors σ_κ consists in producing an apparatus the interaction of which with the object has the result indicated by (34).

It now follows from the linear nature of the quantum-mechanical equations of motion that if the initial state of the object is a linear combination of the σ_κ, say $\sum \alpha_\kappa \sigma_\kappa$, the final state of object plus apparatus will be given by

$$a_0 \otimes \sum \alpha_k \sigma_k = \sum \alpha_k (a_0 \otimes \sigma_k) \to \sum \alpha_k (a_k \otimes \sigma_k) \tag{35}$$

The second member of (35) follows from the linearity of the direct product in terms of its factors, an immediate consequence of (25); the last member, from the linear nature of the time-development operator.

Do the processes postulated in (34) and (35) fully describe the measurement? In the case of (34) this is true: the apparatus assumes a definite state which indicates the state of the object. In the general case, described by (35), this is not the case: the apparatus is not. with the desired probability $|\alpha_\kappa|^2$, in the state a_κ. In fact, the joint state of object and apparatus appears

quite complicated. This could not have been expected to be otherwise: the transformation indicated by the arrow is a consequence of the quantum-mechanical equation of motion and this is deterministic. The outcome of the measurement in the general case of (35) has a probabilistic nature. What the final state of (35) does show is that a statistical correlation between the state of the apparatus and that of the object has been established: the probability of finding both in the state ν is, according to the standard postulate of quantum mechanics,

$$\left|a_v \otimes \sigma_v, \sum \alpha_\kappa \left(a_\kappa \otimes \sigma_\kappa\right)\right|^2 = \left|\sum_\kappa \alpha_\kappa \left(a_v, a_\kappa\right)\left(\sigma_v, \sigma_\kappa\right)\right|^2$$
$$= \left|\sum_\kappa \alpha_\kappa \delta_{v\kappa}\right|^2 = \left|\alpha_v\right|^2 . \tag{36}$$

Both (a_v, a_κ) and (σ_v, σ_κ) have been set equal to $\delta_{\kappa\bar{\nu}}$ the former because the states a_v and a_κ are supposed to be distinguishable even at the macroscopic level, the latter because the σ are normalized characteristic vectors of the self-adjoint
operator which is being measured. A calculation entirely similar to (36) then shows also that the probability is zero of finding the apparatus in state a_λ and the object on the state σ_κ with $\kappa \neq \lambda$-i.e., that indeed the right side of (35) represents a joint state of object and apparatus with the statistical correlation between the states as indicated.

It is evident, therefore, that interesting and suggestive as (35) may be (it is due, essentially, to von Neumann, 1932) it does not completely describe the quantummechanical measurement. In order to give (35) the meaning just outlined, we must assume that a measurement on the state of the right side of (35) is possible and that it gives the different possible values with the probabilities postulated by the usual interpretation. Actually, in order to obtain the state of the object, it is necessary only to measure the state of the apparatus. However, the quantummechanical description of this measurement suffices no more than before to pick out one definite value of κ from many. The equations, being deterministic, lead always from a superposition to a superposition. Nevertheless, if (1) one measures the state of the apparatus a by a second apparatus b, and if (2) the states a_κ of a definitely put the apparatus b into the state b_i; in other words if

$$b_0 \otimes a_\kappa \rightarrow b_\kappa \otimes a_\kappa, \tag{37}$$

then (3) the interaction of this apparatus with the state (34) resulting from the measurement on σ_κ by a, will give

$$b_0 \otimes \left(a_\kappa \otimes \sigma_\kappa\right) \rightarrow b_\kappa \otimes a_\kappa \otimes \sigma_\kappa \tag{37a}$$

This is true, at least, if b interacts only with a, not with the object. Hence, in this case, the interaction of b_0 with the result of the measurement on the general state (cf. [35]) will give

$$b_0 \otimes \sum_\kappa \alpha_\kappa \left(a_\kappa \otimes \sigma_\kappa\right) \rightarrow \sum_\kappa \alpha_\kappa \left(b_\kappa \otimes a_\kappa \otimes \sigma_\kappa\right) \tag{37b}$$

Thus, a correlation between the states of all three systems-object, apparatus a, and apparatus $b-$ is established; but, naturally, no choice between the different states σ_κ is made. A similar statement applies if a fourth apparatus is used to "measure" the state of b, and so on. The measurement process, as far as it can be described by standard quantum mechanics, only establishes statistical correlations between the states of the apparata and those of the object. No choice for a definite state emerges, except if the object was, to begin with, in a state in which the outcome of the measurement is unique, as it is in the case considered in (34).

Before discussing some further problems arising from the assumption embodied in (34) and (35), and before proposing a possible resolution of the problem here encountered, it may be worth pointing out the obvious fact that while it may be
possible to envisage an interaction of the form (34) between apparatus and object, this in no way guarantees that an apparatus with this interaction with the object can be found. This also will be discussed further later.

25.2.4 §4. the Physics of the Measurement Description (35)

The description of the measurement indicated by (34) and (35) has one very happy consequence: it shows that only self-adjoint operators are measurable. This follows from the unitary nature of the transformation indicated by the arrow. If one writes (34) for two different indices, say κ and λ, the final states of the contesponding transformations are orthogonal
We have

$$(a_\kappa \otimes \sigma_\kappa, a_\lambda \otimes \sigma_\lambda) = (a_\kappa, a_\lambda)\,(\sigma_\kappa, \sigma_\lambda) \tag{38}$$

Moreover, a_κ and a_λ are two clearly distinguishable states-distinguishable, as a rule, even macroscopically. Therefore $(\ a_k, a_k\ ) = 0$. Hence, it follows from the unitary nature of the transformation indicated by the arrow that the initial states were also orthogonal:

$$(a_0 \otimes \sigma_\kappa)\,(a_0 \otimes \sigma_\lambda) = (a_0, a_0)\,(\sigma_\kappa, \sigma_\lambda) = 0 \tag{38a}$$

In addition we know that $(a_0, a_0) = 1$. We conclude that $(\sigma_\kappa, \sigma_\lambda) = 0$ if a_κ and a_λ indicate two different outcomes of the measurement. If we further postulate that the outcomes are described by real numbers, i.e., that the characteristic values of the operator Q of which the a_κ are characteristic vectors are real,

$$Qa_\kappa = q_\kappa a_\kappa, \qquad \text{with} \qquad q_\kappa = q_\kappa^* \tag{38b}$$

then the operator Q is necessarily self-adjoint. This means that for any two functions $\sum \alpha_\kappa a_\kappa$ and $\sum \beta_\lambda a_\lambda$ we have

$$\begin{aligned}\Big(\sum \alpha_\kappa a_\kappa, Q \sum \beta_\lambda a_\lambda\Big) &= \sum_\kappa \alpha_\kappa^* \Big(a_\kappa, \sum \beta_\lambda Q a_\lambda\Big) = \sum_{\kappa\lambda} \alpha_\kappa^* \beta_\lambda\,(a_\kappa, q_\lambda a_\lambda) \\ &= \sum_{\kappa\lambda} \alpha_\kappa^* \beta_\lambda q_{j'\kappa\lambda} = \sum_\kappa \alpha_\kappa^* \beta_\kappa q_\kappa\end{aligned} \tag{38c}$$

and one obtains the same expression for $(Q \sum \alpha_\kappa a_\kappa, \sum \beta_\lambda a_\lambda)$. This is satisfactory. It may be worth observing that all the preceding calculations seem to imply a discrete set of outcomes of the measurement-the last proof implies that the measured quantity Q has a discrete spectrum. This is both realistic and essentially unavoidable: the outcome of a measurement is restricted to a discrete set; in the case of the measurement of a continuous quantity, such as the momentum, the
finite accuracy of the measuring device still guarantees that the different outcomes realized form only a discrete set, which in practice is even finite. If one does not want to accept this argument, it is ncessary to rewrite the preceding discussion, essentially in terms of Stieltjes integrals, and this is quite possible, though, in the opinion of this writer, unnecessary.

This is on the favorable side. One has to admit, on the other hand, that (35) is a highly idealized description of the measurement. It does not specify the duration of the measuring process. In fact, most writers, including von Neumann, at least imply that the transition indicated by the arrow in (35) is instantaneous. Of course, even if one accepts this idealization,

unless the quantity to be measured commutes with the Hamiltonian of the system, its value will change after the measurement, and this applics also for the microscopic, that is, quantum-mechanical, description of the apparatus. However, these changes in the system and in the apparatus do not introduce basic problems. Thus, if the σ_κ are orthogonal to each other immediately after the measurement, orthogonality will continue also after the measurement as long as the system remains isolated.

The fact that the measurement is of finite duration introduces a more serious problem. If the operator of the quantity which is being measured does not commute with the Hamiltonian of the system, as is the case, for instance, when position is measured, it will change in the counse of the measurement. To which position at which time does the measurement then refer? This issue is unclear and is rarely discussed. The existence of this issue reemphasizes that the quantum-mechanical description of the measurement, embodied in (34) and (35), is a highly idealized descripion-unless, as was mentioned before, the quantity to be measured is stationary.

In view of all these reservations, it is worthwhile to give a practical example of a measurement (Wigner, 1963). The example most often given is the measurement of the operator s_z-that is, the component of the spin of a particle in a fixed direction. This is a quantity which, for the free particle, is stationary; it commutes with the Hamiltonian. The measurement is called the Stern-Gerlach experiment and was discussed above in a cursory fashion. A particle with spin is passed through an inhomogeneous magnetic field. It is easiest to discuss the case of total spin $\frac{1}{2}$. When the magnetic moment of the particle points in the direction of increase of the field, the particle experiences a force-and is deflected-in the direction of decrease of the field, and conversely. The incoming beam is split into two beams. In one, the spin variable in the field direction has one value, and in the other beam, the other value. Hence, a statistical correlation is established between the position of the particle and its spin direction. The " a " of (34) or (35) is, in this case, the position of the particle. The two σ_κ are the two states of the spin, one parallel, the other antiparallel to the magnetic field. The right side of (35) resembles an expression such as

$$\alpha_+ e^{-x^2-y^2-(z-c)^2}\delta\left(s_z, \frac{1}{2}\right) + \alpha_- e^{-x^2-y^2-(z+c)^2}\delta\left(s_z, -\frac{1}{2}\right) \tag{39}$$

Of course, even if the beam is spiii, one does not yet know what the spin of the particle is; (39) is still a consequence of the quantum-mechanical equation of motion. In order to have a particle with a definite spin direction one must make an additional measurement, determining whether it is in one beam or the otherwhether its z coordinate is positive or negative. This is the process indicated in equations (37a) and (37b)–and it is much more difficult to describe quantum mechanically because the quantum-mechanical description of the position measurement is not at all unique. Nevertheless, this example is instructive, and the expression for the state vector after the original measurements, indicated in (39), is a relatively easy consequence of the quantum-mechanical equations of motion. This is not the case for the measurements of most quantities-including the position of a particle.

Conceptual Problems of the Measurement Description

It was pointed out at the end of §3-and also sometime ago, particularly by von Neumann—that the description given is incomplete. Even if we accept the validity of the equations postulated, (34) and (35), we can account only for the establishment of a statistical correlation between the states of the object and those of the apparatus, not for the fact that the measurement gives one result once, another result another time-i.e., not for the statistical nature of the outcome of the measurement process. As was also pointed out earlier, this is hardly surprising because the deterministic nature of the equations of motion prevents them from accounting

for a probabilistic result. The present section will deal with the problem resulting from this circumstance.

Naturally, one way out of this difficulty would be to postulate that the equations are not fully correct, or, at lcast, that they do not fully describe the actual situation. This has often been suggested, by various writers, and this possibility will be discussed in some detail later-on the whole with a rather negative, but not completely negative result. A more natural explanation would be that the statistical nature of the measurcment outcome arises because the initial state of the apparatus-of a macroscopic apparatus-is not unique. Some initial states of the apparatus give one, others another result, and the statistical nature of the measurement outcome is due to the statistical nature of the initial state of the apparatus. Of course this proposed explanation would not apply to all processes of measurement. It does not apply to the Stern-Gerlach experiment insofar as it leads to a state like that given by (39). However, the final process of observation always involves some macroscopic apparatus, and the statistical explantion could be imagined to apply to that phase of the measurement. We shall see, however, that this proposed way out is also unacceptable. If the outcome of the measurement
obeys the statistics postulated by quantum-mechanical theory, this correctness of prediction cannot be explained by the statistical nature of the initial state of the apparatus if we continue to believe in the uniimited validity of the present quantummechanical equations.

Let us consider, for the sake of simplicity, a measurement which can have, as in the Stern-Gerlach experiment discussed before, only two outcomes. For σ_+it will have the outcome 1, for $\sigma_-$the outcome - 1 , for $\alpha\sigma_+ + \beta\sigma_-$(with $|\alpha|^2 + |\beta|^2 = 1$) the outcome 1 with probability $|\alpha|^2$, the outcome -1 with probability $|\beta|^2$. The possible initial states of the apparatus will be denoted by a_0', a_0'', a_0''', and so on. If the object's initial state is, for instance, $(\sigma_+ + \sigma_-)/\sqrt{2}$, we would expect on this view that half of the states $a_0', a_0'', a_0''' \cdots$ will give the result 1 , half of them -1 .

This expectation, however, is at odds with the linear nature of the cquations. We are supposing that each of the apparatus states a_0 gives, with σ_+, the result 1 , with $\sigma_-$the result -1 . This supposition means that

$$a_0 \otimes \sigma_+ \to a_+ \otimes \sigma_+ \quad \text{and} \quad a_0 \otimes \sigma_- \to a_- \otimes \sigma_- \tag{40}$$

or, in other words, that a_+shows a result $+1$, and $a_-$the result -1 . It now follows from the linear nature of the interaction operator that

$$a_0 \otimes (\sigma_+ + \sigma_-)/\sqrt{2} \to a_+ \otimes \sigma_+/\sqrt{2} + a_- \otimes \sigma_-/\sqrt{2} \tag{40a}$$

that is, that none of the $a_0', a_0'', a_0''' \ldots$ can give definitely $a = +1$ or definitely $a = 1$ as a result. We believe that each apparatus will give the correct result whenever the state of the object is definitely σ_1, and also whenever the state of the object is definitely σ_-. But we see from (40a) that as long as we maintain this belief, we cannot blame the statistical nature of the outcome of the measurement for the state $(\sigma_+ + \sigma_-)/\sqrt{2}$ on the uncertain initial state of the apparatus. Thus, if (40) holds, none of the states a_0 can give either purely $a_+ \otimes \sigma_+$or purely $a_- \otimes \sigma_-$. All give the linear combination (40a) of these two states.

This situation suggests a drastic reformulation of the basic concepts of quantum mechanics. It appears that the statistical nature of the outcome of a measurement is a basic postulate, that the function of quantum mechanics is not to describe some "reality," whatever this term means, but only to furnish statistical correlations between subsequent observations. This assessment reduces the state vector to a calculational tool, an important and useful tool, but not a representation of "reality." The statistical correlations can be calculated with the aid of the state vector. If the first observation tells us that the state vector is σ_κ, we can calculate the probability of the outcome λ of an experiment the characteristic functions of the operator of

which are $b_1, b_2 \ldots$ This probability is $|(a_\kappa, b_\lambda)|^2$. The probability that the next measurement of the quantity the characteristic functions of which are
$c_1, c_2 \ldots$ will give the result μ is then $|(b_\lambda, c_u)|^2$ and the probability of both outcomes b_λ and c_μ is

$$|(a_\kappa, b_\lambda)(b_\lambda, c_\mu)|^2 = (a_\kappa, b_\lambda)(b_\lambda, c_\mu)(c_\mu, b_\lambda)(b_\lambda, a_\kappa) \tag{41}$$

The generalization to more measurements is obvious (Iloutappch, Van Dam, and Wigner, 1963).

It is of some interest that (41) can be given a more concise form. If the state vectors in (41) can be written as functions of a variable x, then (41) can be given the form,

$$\int \cdots \int a_*(x)^* b_2(x) b_2(x')^* c_\mu(x') c_\mu(x'')^* \cdot b_2(x'') b_2(x''')^* a_*(x''') dx \cdots dx'''$$

However, $b_\lambda(x) b_\lambda(x'')^*$ is the kernel of the projection operator P defined in (16) and equations (i7) for the operator A. Hence, if we make $a_\kappa(x''')$ of (41a) the first factor, the factors $a_\kappa(x''') a_\kappa(x)^*, b_\lambda(x) b_\lambda(x'')^*$, and so on, are the kernels of the projection operators P_κ for the first quantity measured, P'_λ for the second one, P''_μ for the third, and again P'_λ for the second. The integrations over x, x', x'' give the product of these projection operators, and the integration over x''' the trace of the product. Hence, the first measurement having given the outcome κ, the probability that the second one gives λ, the third one μ etc. becomes

$$\frac{\text{Trace } P_\kappa P'_\lambda P''_\mu P'''_v \cdots P''_v P''_\mu P'_\lambda}{\text{Trace } P_\kappa} \tag{42}$$

where $P, P', P'' \ldots$ are the proper projection operators for the first, second, third, etc. measurement, respectively. The Trace P_κ in the denominator appears because the characteristic value κ of the operator of the first measurement may not be simple-in which case one has to divide with the multiplicity of this characteristic value. It may be worth remarking that one can add a last factor P_κ in the numerator of (42) to make it more symmetric. This does not change its value because, with $P_\kappa^2 = P_\kappa$, one can insert another factor P_κ on the left side of the expression the trace of which appears in the numerator. This extra factor P_κ can then be shifted to the right end of the numerator since, quite generally, Trace AB = Trace BA or, in our case, Trace $P_\kappa Q$ = Trace $Q P_\kappa$ where Q is the expression in the numerator of (42). The insertion of the P_κ factor on the right therefore does not change the value of (42); it only makes it appear more symmetric.

The preceding derivation of(42) is incomplete, because the possibility of multiple characteristic values of the measured operators is not explicitly taken into account. This has little significance for (35)-it does not matter whether or not the same "pointer position" corresponds to several a_κ. As far as the primed P are concerned
(that is, as far as the measurements after the initial one are concerned), the possibility of multiple characteristic values can easily be taken into account and the resuit is correctly represented by (42). However, (42) also contains the assumption that, if P_κ corresponds to a multiple characteristic value, that is, if Trace $P_\kappa \geq 2$, the state produced by this initial measurement contains the different states of this characteristic value with equal probabilities. This is an assumption which cannot be fully justified.

It should be observed also that if the later measurements, those to which the primed P correspond, take place at later times, the corresponding P must be modified so that they are in the "Heisenberg picture." This means that if the measurement to which $P_v^{(n)}$ corresponds takes place at time t_n after the first measurement, the $P_v^{(n)}$ in (42) can be obtained from the $P_v^{(n)}$ applicable if the measurement n had taken place immediately after the tirst one by the formula,

$$P_v^{(n)}(t_n) = \exp(-iHt_n/\hbar)\, P_v^{(n)}(0) \exp(iHt_n/\hbar)\,. \tag{43}$$

(Naturally $t_1 \leq t_2 \leq t_3 \ldots$.)

The preceding interpretation of the quantum-mechanical formalism reflects its concern with observations, and with giving probabilities for the outcomes of these observations. It does not eliminate the difficuliy which the finite length of the measurement time creates, the difficulty mentioned at the end of the preceding section. Nor does it alter the fact that we have not specified how the measurements are to be carried out. A discussion of limitations on the possibility of measuring certain operators will be given in the next chapter. In spite of aii these reservations, it remains essentially correct to say that the basic statement of quantum mechanics can be given in a formula as simple as (42).

25.2.5 §5. Other Proposed Resolutions of the Measurement Paradox

The measurement paradox referred to in the title of this section is the contradiction between the deterministic nature of the quantum-mechanical equations of motion and the probabilistic outcome of the measurements - processes which should be describable by the quantum-mechanical equations of motion. Section 4 above proposed a resolution of the paradox: the quantum-mechanical equations of motion do not describe the measurement process; they only help in the calculation of the probabilities of the different outcomes. These probabilities form the real content of quantum-mechanical theory. The formalism of state vectors, equations of motion, etc., are only means to calculate these probabilities. The observation results are the true "reality" which underlie quantum mechanics. The state vector does not represent "reality." It is a calculational tool. It should be mentioned that von Neumann's idea was not truly different from this. He postulated that the state vector varies in two different ways. As long as the system is isolated, its
state vector is subject to the quantum-mechanical equation of motion and its behavior is deterministic. When an observation takes place, there is a second type of change of the state vector. Its change then has a probabilistic nature. It jumps discontinuously. It becomes one of the characteristic vectors of the operator which is being measured. If the initial state vector (normalized) was ϕ, it jumps with the probability $|(\psi_v, \phi)|^2$ into the state ψ_v which is one of the (normalized) characteristic vectors of the operator which is being measured. Naturally, the sum of these probabilities must be 1 and this is the consequence of the normalized nature of ϕ. The second type of change of the state vector, the jump from ϕ into one of the ψ_v, according to von Neumann's picture, is not described by the quantummechanical equations of motion.

The other resolutions of the measurement paradox propose more "physical" pictures. The most popular of these is the picture of hidden parameters - embraced particularly by D. Bohm (1952a,b), Y. Aharonov (Bohm and Aharonov, 1957), J. Bub (1969), (see also Bohm and Bub, 1966a,b), J. P. Vigier (1951; 1956), and Bohm and Vigier (1954), but also by many others. The story of this picture is given in some detail by F. Belinfante (1973) as well as by M. Jammer in his book, The Philosophy of Quantum Mechanics (Jammer, 1974) which is worth reading for other reasons-it encompasses an amazing amount of information on the history of our general subject. The other attempt at the resolution of the parador is due to H. Everett (1957), B. S. DeWitt (1970), and J. A. Wheeler (1957) (see also DeWitt and Graham, 1973). This is the "relative state" theory, postulating that, as a result of an observation, the world splits into several new worlds, existing independentiy of each other. Both these pictures will be discussed in more detail, and arguments against them will be presented. It should perhaps be added now that J. A. Wheeler (1977) no longer supports this view.

Theory of "Hidden Variables"

The idea of "hidden variables" postulates that the description of states, by the quantum-mechanical state vector, is incomplete; that there is a more detailed description, by means of variables now "hidden," which would be complete and the knowledge of which would permit one to foresee the actual outcomes of observations - observations about whose outcomes present-day quantum mechanics makes only probabilistic statements. The relation of the postulated theory of hidden variables to present quantum mechanics would be similar to the relation of classical microscopic physics to macroscopic physics. The former uses the positions and velocities of the atoms as variables, while macroscopic physics, such as, for instance, hydrodynamics, describes only the average velocities of the atoms situated in volumes which are large on the microscopic scale and contain many atoms.

There is no clear specification of the nature of the "hidden variables"-they are hidden. The best known replacement for Schrödinger's equation is Bohm's
(1952a,b), in which he reverses Schrödinger's analysis. Schrödinger derived the wave equation named after him by viewing the classical Hamilton-Jacobi equation as giving an incomplete and approximate description of this wave: incomplete, in the sense that it deals only with the phase, $S(x,y,z,t)/\hbar$, of this wave, $\psi(xy,z,t)$; approximate, in the sense that the equation for the Hamilton-Jacobi function S is nonlinear, whereas by demanding linearity Schrödinger got the right equation for ψ. Bohm turns this reasoning around. He assumes that Schrödinger's equation for

$$\psi = Re^{-iS/\hbar} \tag{44}$$

is valid (R and S being real and functions of the position coordinates) and obtains equations for R and S. The equation for S,

$$\frac{\partial S}{\partial t} = \sum_j \frac{1}{2m_j}\left[\left(\frac{\partial S}{\partial x_j}\right)^2 + \left(\frac{\partial S}{\partial y_j}\right)^2 + \left(\frac{\partial S}{\partial z_j}\right)^2\right] + V + Q \tag{44a}$$

differs from the classical Hamilton-Jacobi equation by containing an extra "quantum term" Q. All the other terms are obtained from the Hamilton equation for the energy, $E - H(x,p)$, by replacing E by $-\partial S/\partial t$ and p_{x_j} by $\partial S/\partial x_j$, etc. The additional term, Q, is the "quantum potential,"

$$Q = -\sum_j \frac{\hbar^2}{2m_j R}\left(\frac{\partial^2}{\partial x_j^2} + \frac{\hat{C}^2}{\partial y_j^2} + \frac{\partial^2}{\partial z_j^2}\right) R \tag{44b}$$

in the equation for S. The equation for R is the classical one:

$$\frac{\partial R}{\partial t} = \sum_j \frac{1}{m_j}\left(\frac{\partial R}{\partial x_j}\frac{\partial S}{\partial x_j} + \frac{\partial R}{\partial y_j}\frac{\partial S}{\partial y_j} + \frac{\partial R}{\partial z_j}\frac{\partial S}{\partial z_j}\right) + \frac{R}{2m_j}\left(\frac{\partial^2 S}{\partial x_j^2} + \frac{\partial^2 S}{\partial y_j^2} + \frac{\partial^2 S}{\partial z_j^2}\right). \tag{44c}$$

One can obtain these equations by introducing (44) into Schrödinger's timedependent equation for ψ and separating real and imaginary parts.

The interpretation of these equations from the point of view of hidden variables theory is not so simple. It seems to be agreed that R^2 gives, as in the quantum interpretation, the probability of the configuration indicated by its variables, i.e., that it refers to an ensemble. For S, the classical interpretation is postulated, but it is difficult to understand then how the properties of the ensemble, described by R^2, can influence the motion of an individual system, the system which S is supposed to describe. Yet Q depends on R and R describes the ensemble

containing the system the motion of which should be described by S. Is it that a system's behavior is different depending on the set of systems of which it may be a part?

This dependence of the individual on the ensemble is an objection against a specific theory of hidden variables, not a general objection against all such theories; i.e., it is not an argument against the existence of a deterministic theory of the motion of atomic objects and constituents. Von Neumann was convinced that no such deterministic theory is compatible with quantum mechanics. The reason is easily illustrated by the Stern-Gerlach experiment, or rather, by an indefinite number of repetitions of that experiment. One may consider the measurement of the spin component first in the z direction, then in the x direction, then again in the z direction, then again in the x direction, and so on. If the total spin of the particle on which the measurements are undertaken is $\frac{1}{2}$, all measurements succeeding the first one give the two possible results with a probability $\frac{1}{2}$. If these resuits are, fundamentally, all detemined by the initial values of the hidden narameters, the outcome of each measurement should give some information on the initial values of these parameters. Eventually, it would seem, the values of the "hidden parameters" which determine the outcomes of the first N measurements would be in such a narrow range that they would determine, if N is large enough, the outcomes of all later measurements. Yet this is in contradiction to the quantum-mechanical prediction.

The preceding argument can be made more convincing by substituting other measurements, such as a position and momentum measurements, for the measurements of spin direction. Yet this argument apparently cannot be made mathematically rigorous and it was not published by von Neumann. The proof he published (see p. 173 of von Neumann, 1932; pp. 326-28 in English translation), though it was made much more convincing later on by Kochen and Specker (1967), still uses assumptions which, in my opinion, can quite reasonably be questioned.

Bell's Argument

In my opinion, the most convincing argument against the theory of hidden variables was presented by J. S. Bell (1964). His argument, in its simplest form, starts with a system of two particles with spins $\frac{1}{2}$, these spins being antiparallel, i.e., forming a singlet state. I he spin part of the state vector is

$$\sigma_+(1)\sigma_-(2) - \sigma_-(1)\sigma_+(2) \tag{45}$$

Here $\sigma_+(1)$ is the state vector of particle 1 , with positive component in the z direction. The meaning of the other symbols should then be obvious. Actually, the state (45) is spherically symmetric. It is the only antisymmetric combination possible for the two spin functions. Thus the z direction mentioned above can be replaced by any other direction without changing the value of (45) (as can be verified, of course, by actual calculation). The state (45) is called the spin singlet state. The spin parts of the state vectors of the two electrons of the He atom, or of the H_2 molecule, are actually in that state. In fact, the spin state remains essentially unchanged even if the electrons are torn away from the atom or molecule by dipole radiation, so that their spins remain, to a very good approximation, in the state (45) even when they are widely separated from each other, as is demanded for some applications of Bell's argument. Even for that case, (45) represents a state of the two spins which is not only theoretically possible but also, to a good approximation, experimentally realizable.

For the state (45), there is, according to quantum mechanics, a statistical correlation for the measurement of the spin components in two directions, $\mathbf{e}_1$ and $\mathbf{e}_2$, which enclose an angle θ_{12}. The probability that both components are positive is

$$P_{++} = \left(\frac{1}{2}\right)\sin^2(\theta_{12}/2) = P_{--} \tag{46}$$

and this is aiso the probability that the measurement of the spin components of the two particles, in the $\mathbf{e}_1$ and $\mathbf{e}_2$ directions respectively, will have a negative outcome for both. The probability that one component will be positive the other negative, or for the converse, is

$$P_{+-} = P_{-+} = \left(\frac{1}{2}\right) \cos^2 (\theta_{12}/2) \tag{46a}$$

If $\theta_{12} = 0$, i.e., if the two directions are parallel, the probability (46) of both having the same component is zero. This vanishing of $P_{++}$is what makes the aggregate spin 0 , i.e., makes the total state a singlet. The expressions (46) and (46a) for the probabilities will not be proved explicitly. They are contained, at least implicitly, in the usual textbooks on quantum mechanics.

Bell's inequality, based on the assumption that the "hidden variables" of the two particles uniquely determine the outcomes of the measurements of spin components in all directions, will be shown to be in conflict with equations (46) and (46a). Actually, it suffices to consider three directions, $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$, and measurements of the spin components in these directions. Let us denote $(+-+; --+)$ the probability weighted integral over the values of the hidden variables, an integral taken over that domain of these variables which ensures that the first particle's spin has a positive component in the $\mathbf{e}_1$ and $\mathbf{e}_3$ directions, and a negative component in the $\mathbf{e}_2$ direction, while the second particle's spin has a negative component in the $\mathbf{c}_1$ and $\mathbf{e}_2$ directions, and a positive component in the $\mathbf{e}_3$ direction. The meaning of the other combinations of six + and - signs is similar; thus $(+++; ---)$ gives the probability that the spin component of the first particle is positive in all three directions, that of the second negative. Since the hidden variables are supposed to determine completely the properties of the objects to which they refer, all these quantities are fully defined and are, surely, non-negative. It appears that there are $2^6 = 64$ of them.

It can be noted, next, that most of the 64 symbols are 0 . Thus $(++-;+-+)$ must vanish because it corresponds to such values of the hidden variables as
give, for both particles, a positive component of the spin as measured in the $\mathbf{e}_1$ direction. Because of (46), the probability for this spin configuration vanishes. That is, no value of the hidden variables produces a positive spin component for both particles in the $\mathbf{e}_1$ direction, at least not if quantum mechanics, and hence (46), properly gives the probabilities of the outcomes of measurements. Similarly, if quantum mechanics is correct, all symbols vanish in which the same sign appears at the same position both before and after the semicolon. This then leaves 8 symbols such as $(+--:-++)$ which can have non-zero values.

Next, we write down the probabilities for those outcomes of the measurements which indicate a positive spin component for both particles if these are measured in two different directions, and equate these with the corresponding quantummechanical expressions. First, if the spin components are measured in the $\mathbf{e}_1$ and $\mathbf{e}_2$ directions, respectively, the probability of finding positive components is, according to the theory of hidden variables (the first sign before, and the second sign after the semicolon must be +),

$$(+-+;-+-) + (+--;-++) = \left(\frac{1}{2}\right) \sin^2 (\theta_{12}/2) \tag{47}$$

All other bracket symbols vanish in which the first sign before the semicolon and the second sign after the semicolon are + Similarly, if the measurements are made in the $\mathbf{e}_2$ and $\mathbf{e}_3$ directions, respectively, we have

$$(++-;--+) + (-+-;+-+) = \left(\frac{1}{2}\right) \sin^2 (\theta_{23}/2) \tag{47a}$$

Likewise we have

$$(++-;--+)+(+--;-++)=\left(\frac{1}{2}\right)\sin^2(\theta_{13}/2) \tag{47b}$$

It follows from equations (47) that

$$\begin{aligned}\sin^2(\theta_{12}/2)+\sin^2(\theta_{23}/2) &= \sin^2(\theta_{13}/2)+2(+-+;-+-)+2(-+-;+-+)\\ &\geq \sin^2(\theta_{13}/2)\end{aligned} \tag{48}$$

This is the Bell inequality. It should be fulfilled if the theory of hidden variables is correct, and if, in addition, quantum mechanics correctly predicts-as it apparently does-the probabilities of all conceivable outcomes of a measurement.

It is easy to find directions $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$, however, for which (48) is not valid. It is not valid, in particular, if the three directions are in the same plane and $\mathbf{e}_2$ is between $\mathbf{e}_1$ and $\mathbf{e}_3$. Specifically, if $\theta_{12}=\theta_{23}=\pi/3, \theta_{13}=2\pi/3$, then the left side of (48) is $\frac{1}{4}+\frac{1}{4}=\frac{1}{2}$, the right side $\frac{3}{4}$. Hence, the hidden variable theory, as applied here, leads to a contradiction.

There are then two questions. First, is (46) correct, i.e., can it be confirmed experimentally? This will he discussed later. Second, can one modify the theory of hidden variables in such a way that Bell's inequality (48) does not follow? The answer to this second question is "yes"; but the modified theory implies the use of hidden variables which specify not only the state of the two particles but also the states of the measuring devices, and postulates correlations between the state of the particles and the directions in which the spin is going to be measured. The theory that assumes that there are no such correlations is often called "local" hidden variable theory. The preceding argument shows that any theory of hiddent variables conforming with the postulate of locality is in conflict with quantum mechanics. On the other hand, if one admits hidden variables which establish correlations between the measuring devices and the objects, i.e., describe the states of both together, one cannot see the limit of the complex that has to be described jointly. It sccms highly questionable whether a theory which does not nermit the specification of the states of isolated objects can be in any way useful.

Of course, if future experiments were to demonstrate that Bell's inequalities, in particular (48), are correct and the quantum-mechanical equations, in particular (46) and (400), incomect, this finding would constitute strong evidence in favor of some theory of hidden variables. As was mentioned before, the present status of the experimental research will be discussed later. As of 1981 it appears to be definitely established that what is called "Bell's inequality" is strongly violated, whereas the quantum-mechancal predictions appear to be well supported.

Many-World Theories

"Many-world" theories are much more difficult to discuss than theories of hidden variables. They postulate-as mentioned earlier-that if a measurement with a probabilistic outcome is undertaken, the world splits into several worlds, and each possible outcome of the observations appears in the fraction of the new worlds given by the quantum-mechanical probability of that outcome. This reestablishes the determinism which the laws of nature are expected to exhibit.

It is, of course, difficult to see the meaning of the statement that there are other worlds with which we never will have any contact, which have no influence on us, and which we cannot influence or perceive in any way. From a positivistic point of view, the statement that there are such worlds, and that they are constantly created in large numbers, is entirely meaningless. It can be neither confirmed nor refuted.

Let us admit, however, in conclusion, that the weakness of the theories which have been proposed to replace the standard interpretation of quantum mechanics, and which form the subject of most of these notes, does not establish the full validity of quantum theory. The weaknesses of quantum theory, though not as marked as the deficiencies of the theories discussed in the present chapter, are real nevertheless. They will be discussed subsequently.

25.2.6 §6. Experimental Tests of Bell's Inequality

The conflict between quantum theory and the theory of hidden variables, as manifested by Bell's inequality, was discussed in the last section. The original version of the present section was kindly provided by S. J. Freedman, then at Princeton University. It dealt, principally, with the experimental work then available and aimed at deciding which of the two formulations-Bell's inequality or the conclusions of quantum mechanics was correct. Since that time (1976) the experimental information has been greatly extended, and also some errors in the earlier work have been detected. As a result, it would not be reasonable to repeat Freedman's analysis fully. Instead we refer the reader to Pipkn's (1978) summary of the experimental findings. These findings disagree with Bell's inequality and seem to agree with the consequences of quantum theory. This is a very important point.

In spite of the fact that the more recent experimental results are of great relevance and are, naturally, not contained in Frecdman's original analysis, his discussion will be presented below, though in much abbreviated form, as being of some historical interest. It is also good to realize that experimental results can be in error. It is even better to realize that these errors can be corrected.

Freedman also presented some remaiks on three general, largely theorctical, questions on our subject. (1) He characterized the structure of a general hidden variable model. One of his "hidden variables" was the wave function (and, in many cases, this also is hidden). But he introduced a set of other variables which aiways remain hidden and which are supposed to give a complete description of the state of the system. (2) He presented a special model in order to prove that it is conceivable that hidden variables could be found which would determine the future of the system completely. He admitted, though, at this point, that in order to eliminate the difficulty (for hidden variables!) of the invalidity of Bell's inequality one has to abandon the postulate of the local character of the hidden variables. These must be so constituted, he said, that they establish statistical correlations between the state of the object on which the measurement will be undertaken, and the state of the apparatus which will carry out the measurement. These corrclations, he supposed, exist before the measurement takes place. (3) Freedman also presented a modification of Bell's inequality which is more easily and more directly subject to an experimental test than is the original inequality.

Perhaps the present writer will be permitted to voice his opinion on theories of hidden variables of the type which were crudely described under (2) and which are often proposed. In my opinion, it is not very meaningful to introduce variables, the magnitude of which cannot be determined. These variables could be defined as giving the state of the system for the entire future. Such a description would require the introduction of one additional variable, most naturally denoted by t,
to describe the system. However, it is the purpose of physics to give information on the future based on facts ascertainable at present. The unqualified existence of "hidden variables" would nullify this purpose.

Let us go over to a short description of the experimental information available at the time Freedman made his remarks. Actually, the first two experiments were not carried out with spin- $\frac{1}{2}$ particles in the singlet state of (45) but with two photons emitted in succession by an atom. Their polarizations then give correlations similar to those of the two spin- $\frac{1}{2}$ particles discussed in the preceding chapter.

The first set of experiments was carried out on Ca by Freedman in collaboration with Clauser (1972). The result was a correlation factor of 0.300 ± 0.009. This agrees with the quantum-mechanical value of 0.301 but contradicts Bell's inequality which postulates a value smaiier than 0.25 .

The next set of experiments was done by Holt and Pipkin (1974) with isotopically pure Hg^{198} (zero nuclear spin). Their result was 0.216 ± 0.013. This agrees with Bell's inequality

but differs grossly from the quantum-mechanical value of 0.301 . Perhaps fortunately, it was demonstrated not long after this section was otiginally written that an experimental error had crept into the original value (see Clauser, 1976).

Still other experiments deal with the decay of positronium, in a ground state of spin zero, into two photons. Experiments on the correlation of the poiarization of these two photons were originally suggested by Wheeler (1946). The early experiments, carried out before 1970, gave excellent agreement with quantum mechanics (Wu and Shaknov, 1950; Kasday, Ullman, and Wu, 1970). Their results did not really contradict Bell's inequality, but it is hard to believe that the laws of quantum mechanics are violated in any area under consideration if they are so well obeyed in the region investigated. But more recent work disagrees with these results, referring to conditions in which quantum mechanics and Bell's inequality are in contradiction (Faraci, Gutkowski, Notarrigo, and Pennisi, 1974). This creates a confusing situation.

The last experiment referred to by Freedman related to the spin-spin correlation when a low energy proton is scattered by a proton at rest. Low energy scattering is dominated by proton pairs of zero orbital momentum. The space part of the wave function is therefore symmetric on interchange of the two particles. Consequently the spin part must be antisymmetric, of the form (45), corresponding to zero total spin. The original experiments did not seem to confirm quantum mechanics, but the later, improved ones, did, and were in contradiction with Bell's inequality (Lamehi-Rachti and Mittig, 1976).

This will conclude the somewhat abbreviated review of the experimental material available in 1975 on the validity of Bell's inequality and hence on the possibility of explaining the statistical nature of the outcomes of measurements with hidden variables of a local and reasonable nature. As was mentioned before, the subject was treated in more detail in the original version of these lecture notes
as given by Freedman. As was also mentioned, more recent experimental data definitely deny the possibility that Bell's inequality is generally valid, and hence ruie out any possibility of eliminating the statistical nature of the measurement process by the introduction of local hidden variables.

The next section, the last one, will deal with problems of the standard interpretation. That interpretation assumes that the principle of determinism does not apply to the measurement process. It also shows weaknesses. Nevertheless, no current experimental information contradicts it. Its principal weakness is that it gives no clear and simple rule for the way the measurement can be carried out nor for the limits of the accuracy of the measurement process. The preceding discussion was confined to measuring the spin component or the state of polar ization, both of which clearly appear to be determinable with high accuracy.

25.2.7 §7. Probifms of the Standard Interpretation: Unmeasurable Quantities

Most physicists working on or with quantum mechanics were quite surprised that the experimental confirmation of some of its simple consequences, such as the violation of Bell's inequality, was as ambiguous as described in the preceding sections. Most of us are convinced, nevertheless, that the consequences of quantum theory, which were tested in the experiments described, will be unambiguously confirmed by further and perhaps more precise experiments.

The present section will be devoted to a discussion of internal problems of the standard interpretation as discussed in §3. Let us admit that these problems do mar the mathematical beauty of the theory by demonstrating the difficulty of making measurements and the unavoidable limitations on the accuracy of most of them. These difficulties and limitations indicate, as do the remarks of §4, that quantum mechanics shares a degree of incompleteness with all other theories of physics.

It is a reassuring feature of quantum theory, however, that the earliest problem of measurement-a problem which generated a great deal of discussion-was not really a problem. The apparent problem was to construct the proper quantummechanical opcrator to correspond to a given classical expression. For example, what is the operator which corresponds to the classical expression xp ? Surely xp, where p stands for $(\mathbf{h}/i)c/\partial x$, has to be rejected because it is not self-adjoint. It is natural to choose, instead,

$$xp \to \frac{1}{2}(xp+px) = \frac{1}{2}\frac{\hbar}{i}\left(x\frac{\partial}{\partial x}+\frac{\partial}{\partial x}x\right) = \frac{\hbar}{i}\left(x\frac{\partial}{\partial x}+\frac{1}{2}\right). \tag{49}$$

However, in somewhat more complicated cases, such as x^2p^2, the choice is not unique. Two possible choices are $\frac{1}{2}\left(x^2p^2+p^2x^2\right)$ and xp^2x (p here stands again for $(\mathbf{h}/i)\partial/\partial x$), both of which are self-adjoint but not equal to each other. It should
perhaps be mentioned that Weyl (1927) has proposed a definite operator to correspond to any classical function of position and momentum. But as long as no experimental prescription is provided for the measurement of that operator, the meaning of the Weyl prescription is not clear.

The quandary just described has been resolved by considering the operator to be defined by the quantity which is measured. Thus one does not ask for the operator which corresponds to the classical expression x^2p^2 but asks for ways in which either $\frac{1}{2}\left(x^2\bar{p}^2+\bar{p}^2x^2\right)$ or $x\bar{p}^2x\left(-\bar{p}x^2\bar{p}\right)$ can be measured. We will be concerned henceforth with questions of this nature. Unfortunately, as we shall see, there are serious limitations on the measurability of an arbitrary quantity. They blur the mathematical elegance of von Neumann's original postulate that dil self-adjoint operats are measurable. Von Neumann does produce a expression for the interaction between object and apparatus which would lead to equation (34) of our §3. However, the ensuing considerations show that for many if not most operators, this expression-or any other expression which might lead to that equation-contradicts some of the basic principles of quantum theory. What then are the limitations of measurability?

Only Quantities Which Commute with All Additive Conserved Quantities Are Precisely Measurable

This theorem, dating back to 1952 (Wigner, 1952); see also Araki and Yanase, 1960; Yanase, 1961), will not be proved generally. Only a characteristic example will be given. The quantity to be measured is the component of the spin in the x direction. The "additive conserved quantity" wiil be the angular momentum in the z direction. By "additive" we mean that the magnitude of the quantity for object-plus-apparatus is the sum of this quantity for object and for apparatus, both before and after the measurement.

In the case considered, the argument is very simple. Let us denote the spin states with positive and negative z-component by α and β respectively. The state vector associated with the positive x-component spin is then $2^{-1/2}(\alpha+\beta)$, and that of the negative one, $2^{-1/2}(\alpha-\beta)$. Hence equation (34) of §3 reads in this case

$$a\otimes(\alpha+\beta)\to a^+\otimes(\alpha+\beta), \tag{50a}$$
$$a\otimes(\alpha-\beta)\to a^-\otimes(\alpha-\beta). \tag{50b}$$

Let us decompose the apparatus states a, a^+, and a^-into state vectors each having a definite angular momentum in the z direction,

$$a=\sum a_m;\quad a^+=\sum a_m^+;\quad a^-=\sum a_m^- \tag{51}$$

It then follows from the addition and subtraction of equations (51) that

$$2\sum a_m \otimes \alpha \to \sum a_m^+ \otimes (\alpha+\beta) + \sum a_m^- \otimes (\alpha-\beta) \tag{51a}$$

$$2\sum a_m \otimes \beta \to \sum a_m^+ \otimes (\alpha+\beta) - \sum a_m^- \otimes (\alpha-\beta) \tag{51b}$$

it simplifies these equations to iniroduce the symbols

$$2b_m = a_m^+ + a_m^- \quad \text{and} \quad 2c_m = a_m^+ - a_m^- \tag{52}$$

Hence (5ia) and (5ib) become

$$\sum a_m \otimes \alpha \to \sum (b_m \otimes \alpha + c_m \otimes \beta) \tag{52a}$$

$$\sum a_m \otimes \beta \to \sum (b_m \otimes \beta + c_m \otimes \alpha) \tag{52b}$$

The angular momentum of $a_m \otimes \alpha$ in the z direction is $m+\frac{1}{2}$, that of $a_m \otimes \beta$ is $m-\frac{1}{2}$. Since the anguar monentum in the z direction (or any other direction) does not change as a result of the interaction, it follows that the interaction of the state a_m alone with α will yield

$$a_m \otimes \alpha \to b_m \otimes \alpha + c_{m+1} \otimes \beta \tag{53a}$$

and of a_m alone with β will give

$$a_m \otimes \beta \to b_m \otimes \beta + c_{m-1} \otimes \alpha \tag{53b}$$

Now the lengths of the vectors on the left and right sides of (53a) must be equal. Moreover, the two terms on the right side are orthogonal. Therefore we have

$$(a_m, a_m) = (b_m, b_m) + (c_{m+1}, c_{m+1}) \tag{54a}$$

and similarly, from (53b)

$$(a_m, a_m) = (b_m, b_m) + (c_{m-1}, c_{m-1}) \tag{54b}$$

Hence, we have

$$(c_{m+1}, c_{m+1}) = (c_{m-1}, c_{m-1}) \tag{54}$$

which is a contradiction. Thus (54) means either (1) that the c_m are all 0 -in which case the $a_m^+ = a_m^-$so that $a^+ = a^-$whereas they should be orthogonal-or (2) that

$$(c, c) = \sum (c_m, c_m) \tag{55}$$

is infinite unless all (c_m, c_m) vanish. But this is impossible. Thus from (52) $(c, c) = \frac{1}{2}$ because $a^+$and $a^-$are of the same unit length and are orthogonal. However, (55) already indicates how this difficulty will be overcome. We will recognize that (52a) and (52b) can be oniy approximateiy vaiid (see equations 560 and 560 b). In other words, all (c_m, c_m) will be very small and they will not be absolutely equal (Gaussian dependence on m, with a very large spread in m-values). This means that the measurement is not absolutely accurate, as (52a) and (52b) would imply. However, the magnitude of the inaccuracy, i.e., the magnitude of the terms η in (56a) and (56b), will be minimized.

The conclusion thus arrived at seems to deny the possibility of measuring the spin component precisely in an arbitrary direction, as described in §3. However, two points have to be remembered. First, the measuring equipment uses an external magnetic field. If that field is

considered to be "external," it invalidates the law of conservation of angular momentum. The only way to remedy this difficulty is to consider the magnet as part of the apparatus - as it is. The thus enlarged apparatus becomes quite macroscopic. Second, as equation (39) indicates, the measurement is not perfect. The two beams, with positive and negative s_z, overlap to a certain extent. These two points suggest first, that the measurement of a quantity not commuting with additive conserved quantities requires a large apparatus and, second, that the limitations on the possible accuracy of the measurement can decrease with increasing "size" of the apparatus. "Size," we shall sec, means the amount of the additive conserved quantity that is contained in the apparatus. Instead of (50a) and (50b) we now write

$$a \otimes (\alpha + \beta) \to a^+ \otimes (\alpha + \beta) + \eta^+ \otimes (\alpha - \beta), \tag{56a}$$
$$a \otimes (\alpha - \beta) \to a^- \otimes (\alpha - \beta) + \eta^- \otimes (\alpha + \beta). \tag{56b}$$

Here the terms $\eta^+$and η^-express the error in the measurement. We will try to make $\eta^+$and η^-as small as possible. We write, similar to (51),

$$\eta^+ = \sum \eta_m^+, \quad \eta^- = \sum \eta_m^- \tag{57}$$

and, in analogy to (52), we set

$$\eta_m^+ + \eta_m^- = 2\sigma_m \quad \text{and} \quad \eta_m^+ - \eta_m^- = 2\delta_m \tag{58}$$

Hence, (56a) and (56b) give as a result of the conservation of the z angular momentum the relations

$$a_m \otimes \alpha \to (b_m + \sigma_m) \otimes \alpha + (c_{m+1} - \delta_{m+1}) \otimes \beta \tag{58a}$$
$$a_m \otimes \beta \to (b_m - \sigma_m) \otimes \beta + (c_{m-1} + \delta_{m-1}) \otimes \alpha \tag{58b}$$

These are the analogs of (52a) and (52b). The arrow here, as there, denotes a unitary transformation. Can this requirement be satisfied? Previously, using only part of the unitary restrictions, we arrived at the contradiction (54). Now we have to take into account all the consequences of unitarity.

The left sides of (58a) and (58b) are orthogonal to each other and orthogonal to all similar expressions with other m-values. Their unitary transforms must likewise be orthogonal. This they are automatically when they have different values of the conserved quantity, "total z angular momentum." When the left sides, say $a_m \otimes \alpha$ and $a_{m+1} \otimes \beta$, have the same value for this quantity, orthogonality of the right sides gives

$$(b_m + \sigma_m, c_m + \delta_m) + (c_{m+1} - \delta_{m+1}, b_{m+1} - \sigma_{m+1}) = 0 \tag{59}$$

Since the lengths of the $\bar{u}_m$ vectors are free, the only further relation imposed by the unitarity condition is that the lengths of the vectors on the right sides of (58a) and (58b) be equal. This gives, again for all m,

$$(a_m, a_m) = (b_m + \sigma_m, b_m + \sigma_m) + (c_{m+1} - \delta_{m+1}, c_{m+1} - \delta_{m+1}) \tag{60a}$$
$$(a_m, a_m) = (b_m - \sigma_m, b_m - \sigma_m) + (c_{m-1} + \delta_{m-1}, c_{m-1} + \delta_{m-1}) \tag{60b}$$

As when (54) was derived, so here we take the difference of these two equations. The (b_m, b_m) term drops out to give

$$
\begin{aligned}
&(c_{m+1},\ c_{m+1}) - (c_{m-1}, c_{m-1}) \\
&\quad = 2\,\mathrm{Re}\left[(c_{m+1}, \delta_{m+1}) + (c_{m-1}, \delta_{m-1}) - 2\,(b_m, \sigma_m)\right. \\
&\quad\quad \left. + (\delta_{m-1}, \delta_{m-1}) - (\delta_{m+1}, \delta_{m+1})\right]
\end{aligned} \tag{60}
$$

In the case of an ideal measurement, the left side vanished; we had $\sigma = \delta = 0$; and we encountered a contradiction. The sums of (60a) and (60b) for definite m-values need not be considered; they only give the probabilities $(\ a_m, a_m\ )$ of the specified angular momenta of the measuring device in terms of the other quantities that appear in the state vector of the system after the measurement has taken place. The sum of these probabilities for all m-values, however, does give the normalization condition for the apparatus. Because $(\alpha, \alpha) = (\beta, \beta) = 1$, this condition becomes

$$
\begin{aligned}
\sum (a_m, a_m) = \sum \Bigg\{ &(b_m, b_m) + (\sigma_m, \sigma_m) + \frac{1}{2}\,(\delta_{m-1}, \delta_{m-1}) + \frac{1}{2}\,(\delta_{m+1}, \delta_{m+1}) \\
&+ \frac{1}{2}\,(c_{m+1}, c_{m+1}) + \frac{1}{2}\,(c_{m-1}, c_{m-1}) + \mathrm{Re}\left[(c_{m-1}, \delta_{m-1}) - (c_{m+1}, \delta_{m+1})\right] \Bigg\} = 1
\end{aligned} \tag{61}
$$

The second member of (61) gives $(\ a_m, a_m\ )$ as the average of the two expressions given by (60). We have a final condition. We require that at least the first terms on the right sides of (50a) and (50b) should represent different states-i.e., that $(a^+, a^-) = 0$. In terms of the b_m and c_m this condition says,

$$
\sum_m (b_m + c_m, b_m - c_m) = 0. \tag{62}
$$

Equations (59), (60) and (61), (62) represent the conditions which b, c, σ, and δ must satisfy in order to guarantee the unitary nature of the transformation indicated by (56a) and (56b). In equations (61) and (62) there is summation over m. They give the normalization condition and the requirement that the transformations (56a) and (56b) represent a measurement at least in the approximate sense.

Next, we define the error ε implicit in the measurement process indicated by these expressions,

$$
\varepsilon = \sum \left[\left(\eta_m^+, \eta_m^+\right) + \left(\eta_m^-, \eta_m^-\right)\right] = 2 \sum \left[(\sigma_m, \sigma_m) + (\delta_m, \delta_m)\right]. \tag{63}
$$

The "size," M, of the apparatus which permits an crror so small will be defined by

$$
\begin{aligned}
M^2 =& \sum m^2\,(a_m, a_m) \\
=& \frac{1}{2} \sum m^2 \left[2\,(b_m, b_m) + (c_{m+1}, c_{m+1}) + (c_{m-1}, c_{m-1})\right. \\
&\left. + 2\,\mathrm{Re}\,(c_{m-1}, \delta_{m-1}) - 2\,\mathrm{Re}\,(c_{m+1}, \delta_{m+1}) + (\delta_{m+1}, \delta_{m+1}) + (\delta_{m-1}, \delta_{m-1})\right]
\end{aligned}
$$

Again, the average of the right sides of (60a) and (60b) was substituted for $(\ a_m, a_m\ )$. The problem then is to find expressions for b_m, c_m, σ_m, and δ_m satisfying equations (59) to (62) which, for a given error ε, make M as small as possible; or, equivalently, for a given "size" of the apparatus, M, make the error ε as small as possible.

This minimum problem will not be solved exactly but only under the assumption that the error ε is small as compared with 1 -i.e., that the σ_m and δ_m are small as compared with b_m and c_m. This means that $(\ b_m, b_m\ )$ and $(\ c_m, c_m\ )$ are appreciable for a rather wide range of

m-values. Therefore they will be assumed to depend continuously on m. Even though this idealization is not mathematically rigorous, we adopt it. We rewrite in terms of this continuum approximation all of the equations from (59) to (64) except for (60), which only gives (a_m, a_m) in terms of the other quantities:

$$(b_m, c_m) = 0 \tag{59a}$$

$$2\frac{d}{dm}(c_m, c_m) = 2\,\mathrm{Re}\,[(c_m, \delta_m) - (b_m, \sigma_m)] \tag{60c}$$

$$\sum [(b_m, b_m) + (c_m, c_m)] = 1; \tag{61a}$$

$$\sum (b_m, b_m) = \sum (c_m, c_m)\,, \quad \mathrm{Im} \sum (b_m, c_m) = 0; \tag{62a}$$

$$\varepsilon = 2 \sum [(\sigma_m, \sigma_m) + (\delta_m, \delta_m)]\,; \tag{63a}$$

$$M^2 = \sum m^2\,[(b_m, b_m) + (c_m, c_m)]\,. \tag{64a}$$

It now follows that the Hilbert space vectors δ_m and σ_m are best assumed to be parallel to c_m and b_m, respectively, and indeed the proportionality constant between them is real. A part of δ_m which would be orthogonal to c_m would not change any of the equations, except by adding to the error ε. The same applies to σ_m with respect to b_m. The same argument shows that the proportionality factor between δ_m and c_m, and between σ_m and b_m, has to be real. Next, we assume that the iengths of b_m and c_m, and of δ_m and σ_m, arc equal, but of course, wherever (c_m, δ_m) is positive, (b_m, σ_m) is negative, and conversely. Otherwise the derivative of (c_m, c_m) would become 0 and we would face the same difficulty as in the case of the idealized measurement (cf. equation 54). The equalities assumed can be justified, but this will not be done here. Capitalizing on these observations, and writing $c(m)$ for the length of c_m and $c(m)\delta(m)$ for (c_m, δ_m), we can restate the preceding set of equations:

$$4c(m)\frac{dc(m)}{dm} - 4c(m)\delta(m) \tag{60d}$$

$$\int c(m)^2 dm = \frac{1}{2} \tag{61b}$$

$$\varepsilon = 4\int \sigma(m) dm \tag{63b}$$

$$M^2 = 2\int m^2 c(m)^2 dm \tag{64b}$$

The other equations are automatically satisfied-except that the vectors b_m and c_m must be assumed to be orthogonal.

It follows from (60a) that $\delta(m)$ is the derivative of $c(m)$, so that the error becomes

$$\varepsilon = 4\int \left(\frac{dc(m)}{dm}\right)^2 dm \tag{63c}$$

The problem, therefore, reduces either to minimizing the size M (or its square) given by (64b) while fixing the error ε of (63c) and the normalization (61b)-or to minimizing the error but fixing the size and taking the normalization into account. The Lagrange equation of the minimum problem reduces in both cases to a linear relation between $c(m), m^2c(m)$, and $d^2c(m)/dm^2$-i.e., the quantummechanical equation of the oscillator. The solution is, therefore, that $c(m)$ is a Gauss error curve

$$c(m) = \alpha e^{-(\beta/2)m^2} \tag{65}$$

the constants of which are determined by (61b) and either (63c) or (64b). The relation between error ε and size naturatiy is the same no matter which proceciure is used:

$$\varepsilon = 1/\left(2M^2\right) \tag{66}$$

This is an interesting result, due in this form to Araki and Yanase (1960). It shows that most measurements cannot be made mathematically precise. Moreover, the more accuracy we demand, the greater must be the "size" (equation 64b) of the measuring apparatus.

Are there any quantities where the preceding size-accuracy correlation does not apply, quantities which, as far as this argument goes, may be measured precisely with a small apparatus? For elementary particles, only the mass and the magnitude of the spin are such precisely measurable quantities; none of the quantitics specifying the actual state is measurable with arbitrary precision. If one has a more complex system, the preceding quantities do depend on the state because the degree of excitation is determined by the Minkowski length of the four-dimensional monentum vector (the rest mass). In addition, if the system contains several particles, the scalar product of the momentum vectors and many other similar quantities do commute with all additive conserved quantities. Nevertheless, it is clear that the limitation on the measurability of many quantities with a small apparatus is very severe (Yanase, 1961).

The preceding discussion, leading to equation (66), is incomplete-and this not only from the point of view of mathematical rigor. We considered only a system of spin $\frac{1}{2}$ and only one conservation law, conservation of the angular momentum in one of the directions perpendicular to that in which the spin component is to be measured. It is true that the components of the linear momentum do commute with the spin components; but the other components of the angular momentum do not. It would be interesting to generalize the result (66) both as to the system considered, and as to the inclusion of all additive conservation laws. It should also be repeated that (66) represents only a necessary condition for the apparatus to measure the spin component, and even such a generalization as is suggested above would only give a necessary condition. To demonstrate the actual measurability, one would have to describe the measuring apparatus and its functioningas was done to some degree in §3 with respect to the measurement here considered, but not generally. In fact we shall derive in what follows several other constraints on measurability.

It has been observed that, in order to define a position coordinate, one has to have a coordinate system with a definite position in space and equipped with a clock with well-defined zero of time. The former requires that the apparatus which defines the coordinate system have a spread in momentum which corresponds to
the position-momentum uncertainty relation, and a similar remark, to be discussed later, applies to the clock. Hence, in the case of the measurement of the position coordinate, the need to have an apparatus with a large momentum uncertainty, that is, momentum spread, is obvious. The same applies for many other measurements, but not with the generality established in the preceding discussion. In particular, the argument in this section also applies to the conservation laws for electric charge, for baryon number, etc., and already shows the difficulty of measuring any operator not commuting with these quantities. This last point will be taken up again when the superselection rules are discussed.

The Boson-Fermion Superselection Rule

The preceding section dealt with difficulties inherent in the measurement of a great many, if not most, operators, but the difficulties considered there could be overcome to an increasing extent by an increase in the "size" of the measuring equipment. The superselection rules absoluteiy exciude the measurability of certain operators. This exclusion is demonstrated in the first

case, the boson-fermion superselection rule, on the basis of the postulate of the rotational invariance of the theory. The demonstration in the second case, the charge, baryon-number, etc. superselection rules, is more intricate and touches on a deeper philosophical problem.

The boson-fermion superselection rule tells us that no operator is measurable which has a finite matrix element between two states, one of which has an integer, the other a half-integer, angular momentum. The former states are associatcd with bosons, the latter with fermions but, of course, in the sense here considered, a hydrogen atom is a boson-the half-integer spins of the electron and of the proton combine to an integer spin. If an operator with a finite matrix element is measured, and the measurement results in characteristic vectors of the operator being produced, some of these characteristic vectors will have components with both integer and half integer spin: $b + f$.

From here on, the proof of the inconsistency with rotational invariance can proceed in many ways. A rather natural way to carry out the demonstiation starts from the decompositions of b and f in terms of (1) total angular momentum and (2) z-component of the angular momentum, as viewed from some arbitrary coordinate system:

$$b = \sum_{Jm} b_m^{Jm} \tag{67}$$

$$f = \sum_{Jm} f_m^{Jm} \tag{67a}$$

Naturally, the J and m in (67) are integers, in (67a) half integers-this is the definition of b and f. The index m appears in (67) and (67a) twice in order to remind us that the terms in (67) or (67a) are not partners in the sense of invariance theory. Rather, the effect of a rotation R on these is given by the formulae

$$O_{\underline{R}} b_m^{Jm} = \sum_{m'} D^{(J)}(R)_{m'm} b_{m'}^{Jm} \tag{68}$$

and the same formula applies to the $f_{m'}^{Jm}$, the $b_{m'}^{Jm}$ being the "partners" of b_m^{Jm}, the $f_{m'}^{Jm}$ partners of f_m^{Jm}. If the rotation R is applied on $b_{m'}^{Jm}$, we have

$$O_R b_{m'}^{Jm} = \sum_{m''} D^{(J)}(R)_{m''m} b_{m''}^{Jm} \tag{69}$$

and a similar formula applies to the rotation of the $f_{m'}^{Jm}$. The $D^{(J)}(R)$ are the matrices of the representations of the rotation group in our three-dimensional space (Wigner, 1959).

It now follows that the state vector of the state which looks like $b + f$ from the point of view of a coordinate system obtained from the original one by a rotation R is

$$\begin{aligned} O_R(b+f) &= \sum_{Jm} O_R b_m^{Jm} + O_R f_m^{Jm} \\ &= \sum_{Jm} \sum_{m'} D^{(J)}(R)_{m'm} b_{m'}^{Jm} + \omega_R \sum_{Jm} \sum_{m'} D^{(J)}(R)_{m'm} f_{m'}^{Jm} \end{aligned} \tag{70}$$

The ω_R, with absolute value 1 , had to be introduced in (70) because the effect of a transformation is always indefinite within a factor of absolute value 1the state determines the state vector only up to such a factor. Actually, the first term of (70) should also be provided with such a factor. However, one factor of this nature can be eliminated from all such equations. One has only to postulate that the state vector be one of the state vectors representing the state in question. The others can be obtained from it by multiplication with an arbitrary phase

factor, i.e., a factor of modulus 1. Actually, the omission of this phase factor simplifies the calculation relatively little.

It may be well to observe at this point that if the operator projecting into the state $b+f$ is observable -and we have assumed it is-then the operator projecting into $O_R(b \mid f)$ is likewise, by means of the same apparatus rotated by R. We shall take for R, first a rotation by π about z, to be denoted by Z. We then have, using the usual formulae for $D^{(J)}$ (remembering, though, that the m of b is an integer, that of f a half integer),

$$O_Z(b+f) = \sum_{Jm} i^{2m} \left(b_m^{Jm} + \omega_Z f_m^{Jm}\right) \tag{71}$$

and

$$O_Z^2(b+f) = \sum_{Jm} i^{4m} \left[b_m^{Jm} + \omega_Z \left(\omega_Z f_m^{Jm}\right)\right] \tag{71a}$$

We recall that O_Z^2 is the unit operation. Therefore (71a) should differ only by a factor from $b+f$. In the first term m is an integer and the factor in question indeed has the value unity. Hence $i^{4m}\omega_Z^2$ must also be 1 for the half integer m of the second term. It follows that $\omega_2^2 = -1$, or

$$\omega_Z = \pm i \tag{71b}$$

Let us observe that, in order to derive this result, it was necessary to assume that neither b nor f is a null-vector.

We consider next a rotation by π about the y axis. The standard formulae give

$$O_i(b+f) = \sum_{Jm} i^{2J-2m} \left(b_{im}^{Jm} + \omega_y f_{-m}^{Jm}\right) \tag{72}$$

Calculation of $O_Y^2(b+f)$ yields this time:

$$\begin{aligned} O_Y^2(b+f) &= \sum_{Jm} i^{2J-2m} O_Y \left(b_{-m}^{Jm} + \omega_Y f_{-m}^{Jm}\right) \\ &= \sum_{Jm} i^{2J-2m} i^{2J+2m} \left(b_m^{Jm} + \omega_Y^2 f_m^{Jm}\right) \end{aligned} \tag{72a}$$

The fact that the second ω_Z factor in (71a) and the second ω_Y factor in (72a) must be the same as the first follows from the unitary nature of the transformations O_Z and O_Y. Otherwise the scalar products $[b+f, O_Z(b+f)]$ and $[O_Z(b+f), O_Z^2(b+f)]$ would not be equal. A similar remark applies to O_Y. Now $O_Y^2(b+f)$ can again differ from $b+f$ only in a factor. Moreover, the first term shows that this factor is 1 . Also we have $i^{4J} = -1$ for the J of the second term. Therefore we arrive at a result similar to (71b),

$$\omega_Y = \pm i \tag{72b}$$

A similar calculation yields

$$\omega_x = \pm i \tag{73}$$

as was to be expected. However, the product of rotations by π about z and by π about y is a rotation by π about x. Therefore the vector $O_Y O_Z(b+f)$ can differ from $O_X(b+f)$ only by a factor. Contrary to this requirement we find

$$O_Y O_Z(b+f) = O_Y \sum_{Jm} i^{2m} \left(b_m^{Jm} + \omega_Z f_m^{Jm}\right)$$
$$= \sum_{Jm} i^{2m_i i^{2J-2m}} \left(b_{-m}^{Jm} + \omega_Y \omega_Z f_{-m}^{Jm}\right) \tag{74}$$

Comparison of this expression with that for $O_X(b+f)$ shows that the factor in the first term is 1 . Comparison of the second terms then shows that

$$\omega_X = \omega_Y \, (\omega_Z \tag{74a}$$

which is in contradiction to (71b), (72b), and (73). This disagreement shows that the existence of a state $b+f$, with finite b and finite f, is incompatible with the principle of rotational invariance. As was mentioned above, this "boson-fermion superselection rule" can be established in many different ways, each of which, however, relies to some degree on the theory of rotational invariance, in particular on the difference between the $D^{(t)}$ which apply to bosons and to fermions.

Superselection Rules for Charge, etc.

The creation of a state $b+f$ with both b (boson integer spin) and f (fermion, half-integer spin) finite, or, in other words, "any violation of the boson-fermion superselection rule," would conflict, as we have just seen, with the postulate of the rotational invariance of the theory, provided that the basic ideas of quantum mechanics are valid. This deduction may be a blemish on the very general principles of quantum theory, but it does not affect any of its practical applications or conceivable experimental conclusions.

According to the "charge superselection rule," it is also impossible to produce states

$$\sum c_n, \tag{75}$$

with c_n representing a state with electric charge number n and more than one of the vectors c_n finite. According to the "baryon superselection rule," the same prohibition applies to the baryon number. In contrast to the situation with the state vectors $b+f$, no conflict with any of the fundamental principles has been derived from the possibility of producing a state with the state vector (75). Rather, the validity of the somewhat controversial superselection rules for charge, etc. is based on the physical impossibility of producing states such as (75). We do not know of any macroscopic object that would be in a state such as (75). Even if we do not know the exact electric charge of an object - and in the case of a macroscopic object this is difficult to know-we cannot distinguish between (75) and other states, such as

$$\sum e^{i\phi_n} c_n, \tag{75a}$$

the exponentials in (75a) being phase factors of modulus 1 . In the mathematical terminology of quantum mechanics this ambiguity is expressed by the statement that the actual state is not a superposition of the states c_n but a mixture of them. The state then cannot be characterized by a state vector. The system can be in
any of the states c_n. The probability that a measurement of the charge will give the value n is (c_n, c_n). The theory of mixtures has been given an elegant mathematical form, but it will not be elaborated here.

State vectors with different charges do not interact with each other. Thus the time development of every c_n of (75) is the same as if it were present alone. Therefore the mixture character of the state remains preserved in time. Similarly, if two systems are united to form a joint system, and if each of the two is a mixture of states with definite charge numbers, the same

will be true of the united system. It follows from this reasoning that unless nature supplies some superposition of different charge states, such as (75), no such superposition state will ever be found. Then the superselection ruie for charge will be valid. The same applies to the superselection rules for baryon number, etc.

The law of conservation of electric charge, the independence of the time development of the states with different charges, and our observation on the union of two systems, remain equaiiy vaiid if "iinear momentum" is substituted for "electric charge." It is natural to ask, therefore, why no superselection rule applies for the components of linear momentum or angular momentum. How is it that one can produce a state which is a superposition of states with different linear momenta? And how is it that one can ascertain the coefficients $e^{i\phi_n}$ in the expression corresponding to (75a) with n now referring to a component of linear momentum (n a continuous variable) or to a component of the angular momentum? The answer to this question, it must be admitted, cannot be read out of the basic equations of quantum mechanics. We really do not know how we acquired the ability to see light signals and to feel objects, and why there are no similar phenomena in connection with electric charges. Superconductivity is often claimed to provide such signals. Indeed, the usual theory does use a description of the superconducting state which is a definite superposition of states with different electric charges. However, it is evident that the conclusions of the theory, describing currents, magnetic fields, and similar observable phenomena, would not change in any way if the different charge states were multiplied with different phase factors as they are in (75a). None of the observables used has matrix elements connecting states with different charges. Only the finiteness of such matrix elements could permit one to distinguish (75a) from (75). As far as linear momentum is concerned, the situation is entirely different. Any position operator, for instance, has major matrix elements between states with different momenta.

The question naturally arises whether and how phase relations between different charge states could manifest themselves. Surely the fact that the observed phenomena of superconductivity do not prove the existence of such phase relations does not prove their absence. Naturally, the existence of such phase relations, that is, the breakdown of the charge superselection rule, would be very surprising. Present quantum mechanics would do as little to explain such a breakdown as to explain how the states of different energy in a thermodynamic ensemble could
manifest phase relations. Nevertheless, it may be interesting to find an experimental criterion to tell whether such phase relations exist-that is, to tell whether superpositions such as (75) or (75a) with definite ψ_n are distinguishable.

The simplest experiment would consist in the uniting of two systems. Let each system be imagined to be in a superposition of states with the charges n and m. If these are superpositions such as (75) or (75a), their state vectors could be denoted by

$$\psi_n + e^{i\phi}\psi_m \quad \text{and} \quad \psi'_n + e^{i\phi'}\psi'_m \tag{76}$$

with definite ϕ and ϕ'. Their union would then have the state vector

$$\psi_n \otimes \psi'_n + \left[e^{i\phi}\psi_n \otimes \psi'_m + e^{i\phi}\psi_m \otimes \psi'_n\right] + e^{i\phi+i\phi'}\psi_m \otimes \psi'_m \tag{76a}$$

This formula indicates that the component with charge $n+m$, given in the brackets of (76a), would have a definite structure and might well be distinguished by conceivable experiments from a mixture of the two states $\psi_n \otimes \psi'_m$ and $\psi_m \otimes \psi'_n$. The factor $\exp\left[i\left(\phi - \phi'\right)\right]$ measuring the difference in phase between the two states of equal charge would be definite. There is no reason to believe that that factor would be unobservable. Needless to say, (76) and hence (76a) could be greatly generalized and, equally obvious, the experiment alluded to here is far from concrete. Moreover, it may be impossible to carry it out.

The Measurement of Position

As was mentioned at the beginning of this section, the early interest in the correspondence of a quantum-mechanical operator to classical expressions, such as x^2p^2, has largely ceased. Nevertheless, there are classical quantities, such as linear and angular momentum, energy, and position, to which one would like to coordinate an operator. It appears, at least superficially, that these quantities have a simple meaning, and can be measured, and that it should be possible to find the proper operator for them.

Whether easily measurable or not, the coordination of operators to energy, linear and angular momentum components (and the three other quantities associated with them in relativistic theory) can easily be made. The operators are the infinitesimal operators of the (special) relativistic invariance group, also called the Poincar group. Position is different. Quite apart from the difficulties of measuring position soon to be discussed, we find great problems in coordinating an operator to position. These difficulties have been most elegantly demonstrated by Hegerfeldt (1974) (see also Pryce, 1948; Mller, 1972; Wightman, 1962; and Fleming, 1965). The following discussion is based on his remark. It is more technical than the rest of these notes, being based on the theory of the Poincare invariance of quantum mechanics, and may be, for some, difficult to follow.

In order to simplify the demonstration, we shall use a spacetime with only one spacelike dimension. The generalization to three spacelike dimensions is not difficult but would make the discussion a good deal longer. The spirit of the demonstration is not impaired by the restriction to one spacelike dimension.

Let us assume that there is a position operator and consider its projection operators $P(x)$ as defined, for an arbitrary operator, by equations (21) of §2 ("all values up to x''). Let us then produce out of some initial state ϕ, by the operator $P\left(x_2\right)-P\left(x_1\right)$ (with $x_2>x_1$), a state ψ for which the position is confined to the x_1, x_2 interval. We express the state vector of such a state in the momentum representation, as is usual in the quantum-mechanical invariance theory. Thus we write $\psi=\psi(p, \sigma)$, where p is the momentum vector (one-dimensional for our world with one spacelike dimension) and o is a discrete variable, characterizing the other variables, such as spin component in one direction, etc. Because of the confinement of the position to the x_1, x_2 interval, that is, because of

$$\psi(p, \sigma)=\left[P\left(x_2\right)-P\left(x_1\right)\right] \phi$$

we have

$$P(x) \psi(p, \sigma)=0 \quad \text { for all } \quad x \leq x_1, \tag{77}$$

and

$$P(x) \psi(p, \sigma)=\psi(p, \sigma) \quad \text { for all } \quad x \geq x_2. \tag{77a}$$

The scalar product of two vectors ϕ and ϕ', cxpressed in the (ψ, σ)-representation, is

$$(\phi, \phi')=\sum_\sigma \int \phi(p, \sigma)^* \phi'(p, \sigma) dp / p_0 \tag{78}$$

Here cp_0 is the energy associated with the momentum p,

$$p_0=\left(m^2 c^2+p^2\right)^{1/2} \tag{78a}$$

The p_0 in the denominator of (78) will play no significant role. It is introduced in the usual definition for the scalar product because it simplifies the expressions for Lorentz transformations. We shall not make use of general transformations but only of displacements in space and

time. The operator for a displacement in space by a and displacement in time by t is simply multiplication by

$$e^{-ip_0t+ipa} \tag{79}$$

If $|a| > x_2 - x_1$, a space displacement by a moves the original confinement into a new, nonoverlapping one so that $e^{ipa}\psi(p,\sigma)$ will be orthogonal to $\psi(p,\sigma)$,

$$\big(e^{ipa}\psi(p,\sigma),\psi(p,\sigma)\big) = \int e^{-ipa}\sum_\sigma |\psi(p,\sigma)|^2 dp/p_0 = 0 \tag{80}$$

for $|a| > x_2 - x_1$. This can be proved also more formally by noting that

$$\bar{P}(x-a)e^{i\bar{p}\bar{u}} = e^{i\bar{p}\bar{u}}\bar{P}(x) \tag{79a}$$

and making use of (21c) of §2. From the validity of (79), and the confinement of x for $\psi(p,\sigma)$ to an interval of the width $x_2 - x_1$, (80) should be evident anyway. Equation (80) expresses the fact that the Fourier transform of

$$\sum_\sigma \psi(p,\sigma)^*\psi(p,\sigma)/p_0 \tag{80a}$$

is confined to a region of width $2\,(x_2 - x_1)$. It then follows from the expression of (80a) in terms of its Fourier transform-an integral over a region of width $2\,(x_2 - x_1)$-that the expression (80a) is a meromorphic function of p; that is, it has no singularity in the finite complex plane. The scalar product of a space displaced $\psi(p,\sigma)$ and a time displaced $\psi(p,\sigma)$,

$$\big(e^{ipa}\psi(p,\sigma), e^{-ip_0t}\psi(p,\sigma)\big) = \int e^{-ipa-ip_0t}\sum_\sigma |\psi(p,\sigma)|^2 dp/p_0, \tag{81}$$

evidently is the Fourier coefficient of the function

$$e^{-ip_0t}\sum_\sigma \psi(p,\sigma)^*\psi(p,\sigma)/p_0. \tag{81a}$$

This function, for finite t, is not a meromorphic function of p. To be sure, (80a) is such a function; but the p_0 in the exponent has singularities at $\pm imc$. Hence, there is no finite interval of a outside of which its Fourier transform, (81), will vanish. This means that the time displacement spreads the position, originally confined to the interval x_1, x_2, over all space. Otherwise there could be no finite transition probability to functions $e^{ipa}\psi(p,\sigma)$ for arbitrarily large a, since the latter state is confined to the interval $x_1 - a, x_2 - a$. No matter how one defines the position, one has to conclude that the velocity, defined as the ratio of two subsequent position measurements divided by the time interval between them, has a finite probability of assuming an arbitrarily large value, exceeding c. One either has to accept this, or deny the possibility of measuring the position precisely or even giving significance to this concept: a very difficult choice! And the author of these notes will admit that since writing them, he has devoted a good deal of attention to the problem (Ahmad and Wigner, 1975; O'Connell and Wigner, 1977, 1978).

25.2.8 Summary

The present section starts with the observation that the measured quantities correspond to (self-adjoint) operators, not to the quantities of classical physics. It then points to the demonstrable difficulties of certain measurements, i.e., where it can be shown that it is difficult

to find an apparatus the interaction of which with the object has the result indicated by the basic equation (34) of §3.

It is shown, first, that no precise measurement of any quantity is possible unless this commutes with all conserved additive quantities. In some cases this conclusion can be derived, at least qualitatively, with ease. In other cases, such as operators which do not commute with the operator of electric charge, the situation is less obvious. It is shown then that a measurement which has a small probability of giving an incorrect result surely needs a large apparatus, i.e., one in a state in which the additive conserved quantities, not commuting with the quantity to be measured, have probabilities for values spread over a wide spectrum.

The second type of case discussed refers to quantities which cannot be measured at all. Examples are, first, operators which have a finite matrix element between a state with integer and another state with half-integer angular momentum. The so-called boson-fermion superselection rule shows that it is impossible to produce states which are superpositions of states with integer and half-inieger angular momenta A similar statement is then made for the superposition of states with different electric charges and also with different baryon numbers, and perhaps other similar descriptors.

Finaliy, we had to recognize, every attempt to provide a precise definition of a position coordinate stands in direct contradiction with special relativity.

All these are concrete and clearly demonstrated limitations on the measurability of operators. They should not obscure the other, perhaps even more fundamental weakness of the standard theory, that it postulates the measurability of operators but does not give directions as to how the measurement should be carried out. This problem has already been emphasized at the end of §3, the description of the quantum theory of measurement.

All the preceding discussion is based on the usual quantum-mechanical theory, as taught in classes, not on the more advanced axiomatic quantum field theory. The question therefore arises whether quantum field theory avoids the difficulties mentioned. Surely, as far as the superselection rules are concerned, it does not. As to the rest, my opinion is negative also. The best known discussion of the measurement of field strengths, that given by Bohr and Rosenfeld, postulates an electric test charge with arbitrarily large charge and arbitrarily small size (Bohr and Rosenfeld, 1933, 1950). Naturally, the fact that the quantum field theory does not resolve our problems, though regrettable, should not be considered as an argument against that theory.

25.3 II. 3 "relative State" Formulation of Quantum Mechanics by Everett (1957)

25.3.1 1. Introduction

The task of quantizing general relativity raises serious questions about the meaning of the present formulation and interpretation of quantum mechanics when applied to so fundamental a structure as the space-time geometry itself. This paper seeks to clarify the foundations of quantum mechanics. It presents a reformulation of quantum theory in a form believed suitable for application to general relativity.

The aim is not to deny or contradict the conventional formulation of quantum theory, which has demonstrated its usefulness in an overwhelming variety of problems, but rather to supply a new, more general and complete formulation, from which the conventional interpretation can be deduced.

The relationship of this new formulation to the older formulation is therefore that of a metatheory to a theory, that is, it is an underlying theory in which the nature and consistency, as well as the realm of applicability, of the older theory can be investigated and clarified.

The new theory is not based on any radical departure from the conventional one. The special

postulates in the old theory which deal with observation are omitted in the new theory. The altered theory thereby acquires a new character. It has to be analyzed in and for itself before any identification becomes possible between the quantities of the theory and the properties of the world of experience. The identification, when made, leads back to the omitted postulates of the conventional theory that deal with observation, but in a manner which clarifies their role and logical position.

We begin with a brief discussion of the conventional formulation, and some of the reasons which motivate one to seek a modification.

25.3.2 2. Realm of Applicability of the Conventional or "external Observation" Formulation of Qm

We take the conventional or "external observation" formulation of quantum mechanics to be essentially

the following [1] : A physical system is completely described by a state function ψ, which is an element of a Hilbert space, and which furthermore gives information only to the extent of specifying the probabilities of the results of various observations which can be made on the system by external observers. There are two fundamentally different ways in which the state function can change:

Process 1: The discontinuous change brought about by the observation of a quantity with eigenstates $\phi_1, \phi_2, \cdots$, in which the state ψ will be changed to the state ϕ_j with probability $|(\psi, \phi_j)|^2$.

Process 2: The continuous, deterministic change of state of an isolated system with time according to a wave equation $\partial\psi/\partial t = A\psi$, where A is a linear operator.

This formulation describes a wealth of experience. No experimental evidence is known which contradicts it.

Not all conceivable situations fit the framework of this mathematical formulation. Consider for example an isolated system consisting of an observer or measuring apparatus, plus an object system. Can the change with time of the state of the total system be described by Process 2? If so, then it would appear that no discontinuous probabilistic process like Process 1 can take place. If not, we are forced to admit that systems which contain observers are not subject to the same kind of quantum-mechanical description as we admit for all other physical systems. The question cannot be ruled out as lying in the domain of psychology. Much of the discussion of "observers" in quantum mechanics has to do with photoelectric cells, photographic plates, and similar devices where a mechanistic attitude can hardly be contested. For the following one can limit himself to this class of problems, if he is unwilling to consider observers in the more familiar sense on the same mechanistic level of analysis.

What mixture of Processes 1 and 2 of the conventional formulation is to be applied to the case where only an approximate measurement is effected; that is, where an apparatus or observer interacts only weakly and for a limited time with an object system? In this case of an

approximate measurement a proper theory must specify (1) the new state of the object system that corresponds to any particular reading of the apparatus and (2) the probability with

[8]*Thesis submitted to Princeton University March 1, 1957 in partial fulfillment of the requirements for the Ph.D. degree. An earlier draft dated January, 1956 was circulated to several physicists whose comments were helpful. Professor Niels Bohr, Dr. H. J. Groenewald, Dr. Aage Peterson, Dr. A. Stern, and Professor L. Rosenfeld are free of any responsibility, but they are warmly thanked for the useful objections that they raised. Most particular

[8]thanks are due to Professor John A. Wheeler for his continued guidance and encouragement. Appreciation is also expressed to the National Science Foundation for fellowship support.

[1] We use the terminology and notation of J. von Neumann, Mathematical Foundations of Quantum Mechanics, translated by R. T. Beyer (Princeton University Press, Princeton, 1955).

which this reading will occur. von Neumann showed how to treat a special class of approximate measurements by the method of projection operators. [2] However, a general treatment of all approximate measurements by the method of projection operators can be shown (Sec. 4) to be impossible.

How is one to apply the conventional formulation of quantum mechanics to the space-time geometry itself? The issue becomes especially acute in the case of a closed universe. [3] There is no place to stand outside the system to observe it. There is nothing outside it to produce transitions from one state to another. Even the familiar concept of a proper state of the energy is completely inapplicable. In the derivation of the law of conservation of energy, one defines the total energy by way of an integral extended over a surface large enough to include all parts of the system and their interactions. [4] But in a closed space, when a surface is made to include more and more of the volume, it ultimately disappears into nothingness. Attempts to define a total energy for a closed space collapse to the vacuous statement, zero equals zero.

How are a quantum description of a closed universe, of approximate measurements, and of a system that contains an observer to be made? These three questions have one feature in common, that they all inquire about the quantum mechanics that is internal to an isolated system.

No way is evident to apply the conventional formulation of quantum mechanics to a system that is not subject to external observation. The whole interpretive scheme of that formalism rests upon the notion of external observation. The probabilities of the various possible outcomes of the observation are prescribed exclusively by Process 1. Without that part of the formalism there is no means whatever to ascribe a physical interpretation to the conventional machinery. But Process 1 is out of the question for systems not subject to external observation. [5]

25.3.3 3. Quantum Mechanics Internal to an Isolated System

This paper proposes to regard pure wave mechanics (Process 2 only) as a complete theory. It postulates that a wave function that obeys a linear wave equation

everywhere and at all times supplies a complete mathematical model for every isolated physical system without exception. It further postulates that every system that is subject to external observation can be regarded as part of a larger isolated system.

The wave function is taken as the basic physical entity with no a priori interprelation. Interpretation only comes after an investigation of the logical structure of the theory. Here as always the theory itself sets the framework for its interpretation. [5]

For any interpretation it is necessary to put the mathematical model of the theory into correspondence with experience. For this purpose it is necessary to formulate abstract models for observers that can be treated within the theory itself as physical systems, to consider isolated systems containing such model observers in interaction with other subsystems, to deduce the changes that occur in an observer as a consequence of interaction with the surrounding subsystems, and to interpret the changes in the familiar language of experience.

Section 4 investigates representations of the state of a composite system in terms of states of constituent subsystems. The mathematics leads one to recognize the concept of the relativity of states, in the following sense: a constituent subsystem cannot be said to be in any single well-defined state, independently of the remainder of the composite system. To any arbitrarily

[82] Reference 1, Chap. 4, Sec. 4.

[3] See A. Einstein, The Meaning of Relativity (Princeton University Press, Princeton, 1950), third edition, p. 107.

[4] L. Landau and E. Lifshitz, The Classical Theory of Fields, translated by M. Hamermesh (Addison-Wesley Press, Cambridge, 1951), p. 343.

[5] See in particular the discussion of this point by N. Bohr and L. Rosenfeld, Kgl. Danske Videnskab. Selskab, Mat.-fys. Medd. 12, No. 8 (1933).

chosen state for one subsystem there will correspond a unique rolative state for the remainder of the composite system. This relative state will usually depend upon the choice of state for the first subsystem. Thus the state of one subsystem does not have an independent existence, but is fixed only by the state of the remaining subsystem. In other words, the states occupied by the subsystems are not independent, but correlated. Such correlations between systems arise whenever systems interact. In the present formulation all measurements and observation processes are to be reparded simply as interactions between the physical systems involved-interactions which produce strong correlations. A simple model for a measurement, due to von Neumann, is analyzed from this viewpoint.

Section 5 gives an abstract treatment of the problem of observation. This uses only the superposition principle, and general rules by which composite system states are formed of subsystem states, in order that the results shall have the greatest generality and be applicable to any form of quantum theory for which these principles hold. Deductions are drawn about the state of the observer relative to the state of the object system. It is found that experiences of the observer (magnetic tape memory, counter system, etc.) are in full accord with predictions of the conventional "external observer" formulation of quantum mechanics, based on Process 1.

Section 6 recapitulates the "relative state" formulation of quantum mechanics.

25.3.4 4. Concept of Relative State

We now investigate some consequences of the wave mechanical formalism of composite systems. If a composite system S, is composed of two subsystems S_1 and S_2, with associated Hilbert spaces H_1 and H_2, then, according to the usual formalism of composite systems, the Hilbert space for S is taken to be the tensor product of H_1 and H_2 (written $H = H_1 \otimes H_2$). This has the consequence that if the sets $\left\{{\xi_i}^{S_1}\right\}$ and $\left\{{\eta_j}^{S_2}\right\}$ are complete orthonormal sets of states for S_1 and S_2, respectively, then the general state of S can be written as a superposition:

$$\psi^S = \sum_{i,j} a_{ij} {\xi_i}^{S_1} {\eta_j}^{S_2}. \tag{1}$$

from (3.1) although S is in a definite state ψ^S, the subsystems S_1 and S_2 do not possess anything like definite states independently of one another (except in the special case where all but one of the a_{ij} are zero).

We can, however, for any choice of a state in one subsystem, uniquely assign a corresponding relative state in the other subsystem. For cxample, if we choose ξ_k as the state for S_1, while the composite system S is in the state ψ^S given by (3.1), then the corresponding relative siate in $S_2, \psi\,(S_2;\ \text{rcl}\ \xi_k, S_1)$, will be:

$$\psi\,(S_2; \text{rel}\,\xi_k, S_1) = V_k \sum_j a_{kj} {\eta_j}^{S_2} \tag{2}$$

where N_k is a normalization constant. This relative state for ξ_k is independent of the choice of basis $\{\xi_2\}\,(i \neq k)$ for the orthogonal complement of ξ_k, and is hence determined uniquely by ξ_k alone. To find the relative state in S_2 for an arbitrary state of S_1 therefore, one simply carries out the above procedure using any pair of bases for S_1 and S_2 which contains the desired state as one element of the basis for S_1. To find states in S_1 relative to states in S_2, interchange S_1 and S_2 in the procedure.

In the conventional or "external observation" formulation, the relative state in $S_2, \psi\,(S_2; \text{rel}\,\phi, S_1)$, for a state ψ^{S_1} in S_1, gives the conditional probability distributions for the results of all measurements in S_2, given that S_1 has been measured and found to be in state

ψ^{S_1}-i.c., that ϕ^{S_1} is the eigenfunction of the measurement in S_1 corresponding to the observed eigenvalue.

For any choice of basis in $S_1, \{\xi_i\}$, it is always possible to represent the state of S, (1), as a single superposition of pairs of states, each consisting of a state from the basis $\{\xi_i\}$ in S_1 and its relative state in S_2. Thus, from (2), (1) can be written in the form:

$$\psi^{\mathrm{S}} = \sum_i \frac{1}{\mathrm{V}_2} \xi_i{}^{S_1} \psi\left(S_2; \mathrm{rel}\, \xi_i, S_1\right). \tag{3}$$

This is an important representation used frequently.
Summarizing: There does not, in general, exist anything like a single state for one subsystem of a composite system. Subsystems do not possess states that are independent of the states of the remainder of the system, so that the sub-
system states are generally correlated with one another. One can arbilrarily choose a slate for one subsystem, and be led to the relative state for the remainder. Thus we are faced with a fundamental relativity of states, which is implied by the formalism of composite systems. It is meaningless to ask the absolute slate of a subsystem-one can only ask the state relative to a given state of the remainder of the subsystem.

At this point we consider a simple example, due to von Neumann, which serves as a model of a measurement process. Discussion of this example prepares the ground for the analysis of "observation." We start with a system of only one coordinate, q (such as position of a particle), and an apparatus of one coordinate r (for example the position of a meter needle). Further suppose that they are initially independent, so that the combined wave function is ${\psi_0}^{S+A} = \phi(q)\eta(r)$ where $\phi(q)$ is the initial system wave function, and $\eta(r)$ is the initial apparatus function. The Hamiltonian is such that the two systems do not interact except during the interval $l = 0$ to $l = T$, during which time the total Hamiltonian consists only of a simple interaction,

$$H_I = -i\hbar q(\partial/\partial r) \tag{4}$$

Then the state

$${\psi_i}^{S+A}(q, r) = \phi(q)\eta(r - qt) \tag{5}$$

is a solution of the Schrödinger equation,

$$i\hbar\left(\partial {\psi_t}^{S+A}/\partial t\right) = H_I {\psi_t}^{S+A} \tag{6}$$

for the specified initial conditions at time $t = 0$.
From (5) at time $l = T$ (at which time interaction stops) there is no longer any definite independent apparatus state, nor any independent system state. The apparatus therefore does not indicate any definite object-system value, and nothing like process 1 has occurred.
Nevertheless, we can look upon the total wave function (5) as a superposition of pairs of subsystem states, each element of which has a definite q value and a correspondingly displaced apparatus state. Thus after the interaction the state (5) has the form:

$$\psi_T^{S+A} = \int \phi\left(q'\right) \delta\left(q - q'\right) \eta(r - qT) dq' \tag{7}$$

which is a superposition of states $\psi_{q'} = \delta\left(q - q'\right)\eta(r - qT)$. Each of these elements, $\psi_{q'}$, of the superposition describes a state in which the system has the definite value $q = q'$, and in which the apparatus has a state that is displaced from its original state by the amount $q'T$. These elements $\psi_{q'}$ are then superposed with coefficients $\phi\left(q'\right)$ to form the total state (7).

Conversely, if we transform to the representation where the apparatus coordinate is definite, we write (5) as

$$\psi_T{}^{S+A} = \int (1/V_{r'})\, \xi^{r'}(q)\delta\,(r - r')\, dr'$$

where

$$\xi^{r'}(q) = N_{r'}\phi(q)\eta\,(r' - qT) \tag{8}$$

and

$$(1/N_{r'})^2 = \int \phi^*(q)\phi(q)\eta^*\,(r' - qT)\,\eta\,(r' - qT)\, dq$$

Then the $\xi^{r'}(q)$ are the relative system state functions [6] for the apparatus states $\delta\,(r - r')$ of definite value $r = r'$.
If T is sufficiently large, or $\eta(r)$ sufficiently sharp (near $\delta(r)$), then $\xi^{r'}(q)$ is nearly $\delta\,(q - r'/T)$ and the relative system states $\xi^{r'}(q)$ are nearly eigenstates for the values $q = r'/T$.
We have seen that (8) is a superposition of states $\psi_{r'}$, for each of which the apparatus has recorded a definite value r', and ilie system is left in approximately the eigenstate of the measurement corresponding to $q = r'/T$. The discontinuous "jump" into an eigenstate is thus only a relative proposition, dependent upon the mode of decomposition of the total wave function into the superposition, and relative to a particularly chosen apparatus-coordinate value. So far as the complete theory is concerned all elements of the superposition exist simultaneously, and the entire process is quite continuous.
von Neumann's example is only a special case of a more general situation. Consider any measuring apparatus interacting with any object system. As a result of the interaction the state of the measuring apparatus is no longer capable of independent definition. It can be defined only relative to the state of the object system. In other words, there exists only a correlation between the states of the two systems. It seems as if nothing can ever be settled by such a measurement.

This indefinite behavior seems to be quite at variance with our observations, since physical objects always appear to us to have definite positions. Can we reconcile this feature wave mechanical theory built purely on Process 2 with experience, or must the theory be abandoned as untenable? In order to answer this question we consider the problem of observation itself within the framework of the theory.

25.3.5 5. Observation

We have the task of making deductions about the appearance of phenomena to observers which are considered as purely physical systems and are treated within the theory. To accomplish this it is necessary to identify some present properties of such an observer with features of the past experience of the observer.

---

[86] This example provides a model of an approximate measurement. However, the relative system states after the interaction $\xi^{r'}(q)$ cannot ordinarily be generated from the original system state ϕ by the application of any projection operator, E. Proof: Suppose on the contrary that $\xi'(q) = NE\phi(q) = N'\phi(q)\eta\,(r' - qt)$, where N, N' are normalization constants. Then

$$E(NE\phi(q)) = NE^2\phi(q) = N''\phi(q)\eta^2\,(r' - ql)$$

and $E^2\phi(q) = (N''/N)\,\phi(q)\eta^2\,(r' - ql)$. But the condition $E^2 = E$ which is necessary for E to be a projection implies that $N'/N''\eta(q) = \eta^{\bar{z}}(q)$ which is generally false.

Thus, in order to say that an observer 0 has observed the event α, it is necessary that the state of 0 has become changed from its former state to a new state which is dependent upon α.

It will suffice for our purposes to consider the observers to possess memories (i.e., parts of a relatively permanent nature whose states are in correspondence with past experience of the observers). In order to make deductions about the past experience of an observer it is sufficient to deduce the present contents of the memory as it appears within the mathematical model.

As models for observers we can, if we wish, consider automatically functioning machines, possessing sensory apparatus and coupled to recording devices capable of registering past sensory data and machine configurations. We can further suppose that the machine is so constructed that its present actions shall be determined not only by its present sensory data, but by the contents of its memory as well. Such a machine will then be capable of performing a sequence of observations (measurements), and furthermore of deciding upon its future experiments on the basis of past results. If we consider that current sensory data, as well as machine configuration, is immediately recorded in the memory, then the actions of the machine at a given instant can be regarded as a function of the memory contents only, and all relavant experience of the machine is contained in the memory.

For such machines we are justificd in using such phrases as "the machine has perceived A " or "the machine is aware of A " if the occurrence of A is represented in the memory, since the future bchavior of the machine will be based upon the occurrence of A. In fact, all of the customary language of subjective experience is quite applicable to such machines, and forms the most natural and useful mode of expression when dealing with their behavior, as is well known to individuals who work with complex automata.

When dealing with a system representing an observer quantum mechanically we ascribe a state function, ψ^0, to it. When the state ψ^0 describes an observer whose memory contains representations of the events $A, B, \cdots, C$ we denote this fact by appending the memory sequence in brackets as a subscript, writing:

$$\psi^0[\text{ A, B, } \cdots, c]. \tag{9}$$

The symbols $A, B, \cdots, C$, which we assume to be ordered time-wise, therefore stand for memory configurations which are in correspondence with the past experience of the observer. These configurations can be regarded as punches in a paper tape, impressions on a magnetic reel, configurations of a relay switching circuit, or even configurations of brain cells. We require only that they be capable of the interpretation "The observer has experienced the succession of events $A, B, \cdots, C$." (We sometimes write dots in a memory sequence, $\cdots A$, $B, \cdots, C$, to indicate the possible presence of previous
memories which are irrelevant to the case being considered.)

The mathematical model seeks to treat the interaction of such observer systems with other physical systems (observations), within the framework of Process 2 wave mechanics, and to deduce the resulting memory configurations, which are then to be interpreted as records of the past experiences of the observers.

We begin by defining what constitutes a "good" observation. A good observation of a quantity A, with eigenfunctions ϕ_i, for a system S, by an observer whose initial state is ψ^0, consists of an interaction which, in a specified period of time, transforms each (total) state

$$\psi^{S+0} = \phi_i \psi^0 [\ldots] \tag{10}$$

into a new state

$$\psi^{S+0'} = \phi_i \psi^0 [\ldots \alpha_i] \tag{11}$$

where α_i characterizes [7] the state ϕ_i. (The symbol, α_i, might stand for a recording of the eigenvalue, for example.) That is, we require that the system state, if it is air cigcnstate, shall be unchanged, and (2) that the observer state shall change so as to describe an observer that is "aware" of which eigenfunction it is; that is, some property is recorded in the memory of the observer which characterizes ϕ_i, such as the eigenvalue. The requirement that the eigenstates for the system be unchanged is necessary if the observation is to be significant (repeatable), and the requirement that the observer state change in a manner which is different for each eigenfunction is necessary if we are to be able to call the interaction an observation at all. How closely a general interaction satisfies the definition of a good observation depends upon (1) the way in which the interaction depends upon the dynamical variables of the observer system-including memory variables-and upon the dynamical variables of the object system and (2) the initial state of the observer system. Given (1) and (2), one can for example solve the wave equation, deduce the state of the composite system after the end of the interaction, and check whether an object system that was originally in an eigenstate is left in an eigenstate, as demanded by the repeatability postulate. This postulate is satisfied, for example, by the model of von Neumann that has already been discussed.

From the definition of a good observation we first deduce the result of an observation upon a system which is not in an eigenstate of the observation. We know from our definition that the interaction transforms states $\phi_i\psi^0[\cdots]$ into states $\phi_i\psi^0\,[\cdots\alpha_i]$. Consequently these solutions of the wave equation can be superposed to give the final state for the case of an arbitrary initial system state. Thus if the initial system state is not an eigenstate, but a general state $\sum_i a_i\phi_i$, the final total

state will have the form:

$$\psi^{S+0'} = \sum a_i\phi_i\psi^0\,[\cdots\alpha_i]\,. \tag{12}$$

This superposition principle continues to apply in the presence of further systems which do not interact during the measurement. Thus, if systems $S_1, S_2, \cdots, S_n$ are present as well as 0 , with original states $\psi^{S_1}, \psi^{S_2}, \cdots, \psi^{S_n}$, and the only interaction during the time of measurement takes place between S_1 and 0 , the measurement will transform the initial total state:

$$\psi^{S_1+S_2+\cdots+S_{n+0}} = \psi^{S_1}\psi^{S_2}\cdots\psi^{S_n}\psi^0[\cdots] \tag{13}$$

into the final state:

$$\psi'^{S_1+S_2+\cdots+S_n+0} = \sum_i a_i{\phi_i}^{S_1}\psi^{S_2}\cdots\psi^{S_n}\psi^0\,[\cdots\alpha_i] \tag{14}$$

where $a_i = \left({\phi_i}^{S_1}, \psi^{S_1}\right)$ and ${\phi_i}^{S_1}$ are eigenfunctions of the observation.

Thus we arrive at the general rule for the transformation of total state functions which describe systems within which observation processes occur:

Rule 1: The observation of a quantity A, with eigenfunctions ${\phi_i}^{S_1}$, in a system S_1 by the observer (), transforms the total state according to:

$$\psi^{S_1}\psi^{S_2}\cdots\psi^{S_n}\psi^0[\cdots] \rightarrow \sum_i a_i{\phi_i}^{S_1}\psi^{S_2}\cdots\psi^{S^n}\psi^0\,[\cdots\alpha_i] \tag{15}$$

[87] It should be understood that $\psi^0\,[\ldots\alpha_i]$ is a different state for each i. A more precise notation would write $\psi_i\,[\ldots\alpha_i]$, but no confusion can arise if we simply let the ${\psi_i}^0$ be indexed only by the index of the memory configuration symbol.

where

$$a_i = \left(\phi_i{}^{S_1}, \psi^{S_1}\right)$$

If we next consider a second observation to be made: where our total state is now a superposition, we can apply Rule 1 separately to each element of the superposition, since each element separately obeys the wave equation and behaves independently of the remaining elements, and then superpose the results to obtain the final solution. We formulate this as:

Rule 2: Rule 1 may be applied separately to each element of a superposition of total system states. the results being superposed to obtain the final total state. Thus, a determination of B, with eigenfunctions $\eta_j{}^{S_2}$, on S_2 by the observer 0 transforms the total state

$$\sum_i a_i \phi_i{}^S \psi^{S_2} \cdots \psi^S \psi^0 \left[\cdots \alpha_l\right] \tag{16}$$

into the state

$$\sum_{i,j} a_i b_j \phi_i{}^{S_1} \eta_j{}^{S_2} \psi^{S_3} \cdots \psi^S \psi^0 \left[\cdots \alpha_i, \beta_j\right] \tag{17}$$

where $b_j = \left(\eta_j{}^{S_2,\psi^{S_2}}\right)$, which follows from the application of Rule 1 to each element $\phi_i{}^{S_1} \psi^{S_2} \ldots \psi^{S_n} \psi^0 \left[\cdots \alpha_i\right]$, and then superposing the results with the coefficients a_i.

These two rules, which follow directly from the superposition principle, give a convenient method for determining final total states for any number of observation processes in any combinations. We now seek the interpretation of such final total states.

Let us consider the simple case of a single observation of a quantity A, with eigenfunctions ϕ_i, in the system S with initial state ψ^S, by an observer 0 whose initial state is $\psi^0[\cdots]$. The final result is, as we have seen, the superposition

$$\psi'^{S+0} = \sum_i a_i \phi_i \psi^0 \left[\cdots \alpha_i\right]. \tag{18}$$

There is no longer any independent system state or observer state, although the two have become correlated in a one-one manner. However, in each element of the superposition, $\phi_i \psi^0 \left[\cdots \alpha_i\right]$, the object-system state is a particular eigenstate of the observation, and furthermore the observer-system state describes the observer as definitely perceiving that particular system state. This correlation is what allows one to maintain the interpretation that a measurement has been performed.

We now consider a situation where the observer system comes into interaction with the object system for a second time. According to Rule 2 we arrive at the total state after the second observation:

$$\psi''^{S+0} = \sum_i a_i \phi_i \psi^0 \left[\cdots \alpha_i, \alpha_i\right]. \tag{19}$$

Again, each element $\phi_i \psi^0 \left[\cdots \cdots_i, \cdots i\right]$ describes a system eigenstate, but this time also describes the observer as having obtained the same resull for each of the two observations. Thus for every separate state of the observer in the final superposition the result of the observation was repeatable, even though different for different states. This repeatability is a consequence of the fact that after an observation the relative system state for a particular observer state is the corresponding eigenstate.

Consider now a different situation. An observersystem 0 , with initial state $\psi^0[\cdots]$, measures the same quantity A in a number of separate, identical, systems which are initially in the same

state, $\psi^{S_1} = \psi^{S_2} = \cdots = \psi^{S_n} = \sum_i a_i \phi_i$ (where the ϕ_i are, as usual, eigenfunctions of A). The initial total state function is then

$$\psi_0{}^{S_1+S_2+\cdots+S_n+0} = \psi^{S_1}\psi^{S_2}\cdots\psi^{S_n}\psi^0[\cdots]. \tag{20}$$

We assume that the measurements are performed on the systems in the order $S_1, S_2, \cdots S_n$. Then the total state after the first measurement is by Rule 1,

$$\psi_1{}^{S_1+S_2+\cdots+S_n+0} = \sum_i a_2 \phi_i{}^{S_i}\psi^{S_2\cdots}\psi^{S_n}\psi^0\left[\cdots \alpha_2{}^1\right] \tag{21}$$

(where $\alpha_i{}^l$ refers to the first system, S_1).
After the second measurement it is, by Rule 2,

$$\begin{aligned} &\psi_2{}^{S_1+S_2+\cdots} + \cdots S_n + 0 \\ &= \sum_{i,j} a_i a_j \phi_i{}^{S_1}\phi_j{}^{S}\psi^{S_3}\cdots\psi^{S^n}\psi^0\left[\cdots \alpha_i{}^l, \alpha_j{}^2\right] \end{aligned} \tag{22}$$

and in general, after r measurements have taken place ($r \leq n$), Rule 2 gives the result:

$$\begin{aligned} \psi_r = \sum_{i,j,\cdots k} &a_i a_j \cdots a_k \phi_i{}^{S_1}\phi_j{}^{S_2}\cdots\phi_k{}^{S_r} \\ &\psi^{S_r+1}\cdots\psi^{S^n\psi^0}\left[\cdots \alpha_{i^1,\alpha j^2}\cdots\alpha_k{}^r\right] \end{aligned} \tag{23}$$

We can give this state, ψ_r, the following interpretation. It consists of a superposition of states:

$$\begin{aligned} \psi'_{ij\cdots k} = \phi_i{}^{S_1}\phi_j{}^{S_2}\cdots&\phi_k{}^{S_r} \\ &\times \psi^{S_{r+1}}\cdots\psi^{S_m}\psi^0\left[\alpha_i{}^i, \alpha_j{}^2\cdots\alpha_k{}^r\right] \end{aligned} \tag{24}$$

each of which describes the observer with a definite memory sequence $[\alpha_i{}^1, \alpha_j{}^2, \cdots \alpha_k{}^r]$. Relative to him the (observed) system states are the corresponding eigenfunctions $\phi_i{}^{S_1}, \phi_j{}^{S_2}, \cdots, \phi_k{}^{S_\tau}$, the remaining systems, $S_{r+1}, \cdots, S_n$, being unaltered.

A typical element $\psi'_{ij\ldots k}$ of the final superposition describes a state of affairs wherein the observer has perceived an apparently random sequence of definite results for the observations. Furthermore the object systems have been left in the corresponding eigenstates of the observation. At this stage suppose that a redetermination of an earlier system observation (S_i) takes place. Then it follows that every element of the resulting final superposition will describe the observer with a memory configuration of the form $[\alpha_i{}^1, \ldots\ \alpha_j{}^l, \cdots \alpha_k{}^r, \alpha_j{}^l]$ in which the earlier memory coincides with the later-i.e., the memory states are correlated. It will thus appear to the observer, as described by a typical element of the superposition, that each initial observation on a system caused the system to "jump" into an eigenstate in a random fashion and thereafter remain there for subsequent measurements on the same system. Therefore-disregarding for the moment quantitative questions of relative frequencies the probabilistic assertions of Process 1 appear to be valid to the observer described by a typical element of the final superposition.

We thus arrive at the following picture: Throughout all of a sequence of observation processes there is only one physical system representing the observer, yet there is no single unique state of the observer (which follows from the representations of interacting systems). Nevertheless, there is a representation in terms of a superposition, each element of which contains

a definite observer state and a corresponding system state. Thus with each succeeding observation (or interaction), the observer state "branches" into a number of different states. Each branch represents a different outcome of the measurement and the corresponding eigenstate for the object-system state. All branches exist simultaneously in the superposition after any given sequence of observations. ‡

The "trajectory" of the memory configuration of an observer performing a sequence of measurements is thus not a linear sequence of memory configurations, but a branching tree, with all possible outcomes existing simultaneously in a final superposition with various coefficients in the mathematical model. In any familiar memory device the branching does not continue indefinitely, but must stop at a point limited by the capacity of the memory.

In order to establish quantitative results, we must put some sort of measure (weighting) on the elements of a final superposition. This is necessary to be able to make assertions which hold for almost all of the observer states described by elements of a superposition. We wish to make quantitative statements about the relative frequencies of the different possible results of observation-which are recorded in the memory-for a typical observer state; but to accomplish this we must have a method for selecting a typical element from a superposition of orthogonal states.

We therefore seek a general scheme to assign a measure to the elements of a superposition of orihogonal states $\sum_i a_i\phi_i$. We require a positive function m of the complex coefficients of the elements of the superposition, so that $m(a_i)$ shall be the measure assigned to the element ϕ_i. In order that this general scheme be unambiguous we must first require that the states themselves always be normalized, so that we can distinguish the coefficients from the states. However, we can still only determine the coefficients, in distinction to the states, up to an arbitrary phase factor. In order to avoid ambiguities the function m must therefore be a function of the amplitudes of the coefficients alone, $m(a_i) = m(|a_i|)$.

We now impose an additivity requirement. We can regard a subset of the superposition, say $\sum_{i=1}^{n} a_i\phi_i$, as a single element $\alpha\phi'$:

$$\alpha\phi' = \sum_{i=1}^{n} a_i\phi_i. \tag{25}$$

We then demand that the measure assigned to ϕ' shall be the sum of the measures assigned to the ϕ_i (i from 1

separate elements of a superposition individually obey the wave equation with complete indifference to the presence or absence ("actuality" or not) of any other elements. This total lack of effect of one branch on another also implies that no observer will ever be aware of any "splitting" process.

Arguments that the world picture presented by this theory is contradicted by experience, hecause we are unaware of any branching process, are like the criticism of the Copernican theory that the mobility of the earth as a real physical fact is incompatible with the common sense interpretation of nature because we feel no such motion. In both cases the argument fails when it is shown that the theory itself predicts that our experience will be what it in fact is. (In the Copernican case the addition of Newtonian physics was required to be able to show that the

[8]‡ Note added in proof —In reply to a preprint of this article some correspondents have raised the question of the "transition from possible to actual," arguing that in "reality" there is-as our experience testifies-no such splititing of observer states, so that only one branch can ever actually exist. Since this point may occur to other readers the following is offered in explanation.

The whole issue of the transition from "possible" to "actual" is taken care of in the theory in a very simple way there is no such transition, nor is such a transition necessary for the theory to be in accord with our experience. From the viewpoint of the theory all elements of a superposition (all "branches") are "actual," none any more "real" than the rest. It is unnecessary to suppose that all but one are somehow destroyed, since all the

earth's inhabitants would be unaware of any motion of the earth.)
to n) :

$$m(\alpha) = \sum_{i=1}^{n} m\left(a_i\right). \tag{26}$$

Then we have already restricted the choice of m to the square amplitude alone; in other words, we have $m\left(a_i\right) = {a_i}^* a_i$, apart from a multiplicative constant.

To see this, note that the normality of ϕ' requires that $|\alpha| = \left(\sum {a_i}^* a_i\right)^{\frac{1}{2}}$. From our remarks about the dependence of m upon the amplitude alone, we replace the a_i by their amplitudes $u_i = |a_i|$. Equation (26) then imposes the requirement,
$m(\alpha) = m\left(\sum {a_i}^* a_i\right)^{\frac{1}{2}} = m\left(\sum {u_i}^2\right)^{\frac{1}{2}}$

$$= \sum m\left(u_i\right) = \sum m\left(u_i^2\right)^{\frac{1}{2}}. \tag{27}$$

Defining a new function $g(x)$

$$g(x) = m(\sqrt{}x) \tag{28}$$

we see that (27) requires that

$$g\left(\sum u_i^2\right) = \sum g\left(u_i^2\right) \tag{29}$$

Thus g is restricted to be linear and necessarily has the form:

$$g(x) = cx \quad (c \text{ constant }). \tag{30}$$

Therefore $g\left(x^2\right) = cx^2 = m\left(\sqrt{x^2}\right) = m(x)$ and we have deduced that m is restricted to the form

$$m\left(a_i\right) = m\left(u_i\right) = cu_i^2 = ca_i^* a_i. \tag{31}$$

We have thus shown that the only choice of measure consistent with our additivity requirement is the square amplitude measure, apart from an arbitrary multiplicative constant which may be fixed, if desired, by normalization requirements. (The requirement that the total measure be unity implies that this constant is 1.)

The situation here is fully analogous to that of classical statistical mechanics, where one puts a measure on trajectories of systems in the phase space by placing a measure on the phase space itself, and then making assertions (such as ergodicity, quasi-ergodicity, etc.) which hold for "almost all" trajectories. This notion of "almost all" depends here also upon the choice of measure, which is in this case taken to be the Lebesgue measure on the phase space. One could contradict the statements of classical statistical mechanics by choosing a measure for which only the exceptional trajectories had nonzero measure. Nevertheless the choice of Lebesgue measure on the phase space can be justified by the fact that it is the only choice for which the "conservation of probability" holds, (Liouville's theorem) and hence the only choice which makes possible any reasonable statistical deductions at all.

In our case, we wish to make, statements about "trajectories" of observers. However, for us a trajectory is constantly branching (transforming from state to superposition) with each successive measurement. To
have a requirement analogous to the "conservation of probability" in the classical case, we demand that the measure assigned to a trajectory at one time shall equal the sum of the measures of its separate branches at a later time. This is precisely the additivity requirement

which we imposed and which leads uniquely to the choice of square-amplitude measure. Our procedure is therefore quite as justified as that of classical statistical mechanics.

Having deduced that there is a unique measure which will satisfy our requirements, the square-amplitude measure, we continue our deduction. This measure then assigns to the $i, j, \cdots k$ th element of the superposition (24),

$$\phi_i{}^{S_1}\phi_j{}^{S_2}\cdots\phi_k{}^{S_n}\psi^{S_{r+1}}\cdots\psi^{S_m}\psi^0\left[\alpha_i{}^1, \alpha j^2, \cdots \alpha_k{}^r\right] \tag{32}$$

the measure (weight)

$$M_{ij\cdots k} = (a_i a_j \cdots a_k)^* (a_i a_j \cdots a_k) \tag{33}$$

so that the observer state with memory configuration $[\alpha_i{}^1, \alpha_j{}^2, \cdots, \alpha_k{}^r]$ is assigned the measure $a_i{}^* a_i a_j{}^* a_j \cdots a_k{}^* a_k = M_{ij\ldots k}$. We see immediately that this is a product measure, namely,

$$M_{ij\cdots k} = M_i M_j \cdots M_k \tag{34}$$

where

$$M_l = a_l^* a_l$$

so that the measure assigned to a particular memory sequence $[\alpha_i{}^1, \alpha_j{}^2, \cdots, \alpha_k{}^r]$ is simply the product of the measures for the individual components of the memory sequence.

There is a direct correspondence of our measure structure to the probability theory of random sequences. If we regard the $M_{ij\ldots k}$ as probabilities for the sequences then the sequences are equivalent to the random sequences which are generated by ascribing to each term the independent probabilities $M_l = a_l^* a_l$. Now probability theory is equivalent to measure theory mathematically, so that we can make use of it, while keeping in mind that all results should be translated back to measure theoretic language.

Thus, in particular, if we consider the sequences to become longer and longer (more and more observations performed) each memory sequence of the final superposition will satisfy any given criterion for a randomly generated sequence, generated by the independent probabilities $a_l{}^* a_l$, except for a set of total measure which tends toward zero as the number of observations becomes unlimited. Hence all averages of functions over any memory sequence, including the special case of frequencies, can be computed from the probabilities $a_i^* a_i$, except for a set of memory sequences of measure zero. We have therefore shown that the statistical assertions of Process 1 will appear to be valid to the observer, in almost all elements of the superposition (24), in the limit as the number of observations goes to infinity.

While we have so far considered only sequences of
observations of the same quantity upon identical systems, the result is equally true for arbitrary sequences of observations, as may be verified by writing more general sequences of measurements, and applying Rules 1 and 2 in the same manner as presented here.

We can therefore summarize the situation when the sequence of observations is arbitrary, when these observations are made upon the same or different systems in any order, and when the number of observations of each quantity in each system is very large, with the following result:

Except for a set of memory sequences of measure nearly zero, the averages of any functions over a memory sequence can be calculated approximately by the use of the independent probabilities given by Plocess 1 for each initial observation, on a system, and by the use of the usual transition probabilities for succeeding observations upon the same system. In the limit, as the number of all types of observations goes to infinity the calculation is exact, and the exceptional set has measure zero.

This prescription for the calculation of averages over memory sequences by probabilities assigned to individual elements is precisely that of the conventional "external observation" theory (Process 1). Moreover, these predictions hold for almost all memory sequences. Therefore all predictions of the usual theory will appear to be valid to the observer in amost all observer states.
In particular, the uncertainty principle is never violated since the latest measurement upon a system supplies all possible information about the relative system state, so that there is no direct conrelation between any earlier results of observation on the system, and the succeeding observation. Any observation of a quantity B, between two successive observations of quantity A (all on the same system) will destroy the one-one correspondence between the earlier and later memory states for the result of A. Thus for alternating observations of different quantities there are fundamental limitations upon the correlations between mcmory states for the same observed quantity, these limitations expressing the content of the uncertainty principle.
As a final step one may investigate the consequences of allowing several observer systems to interact with (observe) the same object system, as well as to interact with one another (communicate). The latter interaction can be treated simply as an interaction which correlates parts of the memory configuration of one observer with another. When these observer systems are investigated, in the same manner as we have already presented in this section using Rules 1 and 2, one finds that in all elements of the final superposition:

1. When several observers have separately observed the same quantity in the object system and then communicated the results to one another they find that they
   are in agreement. This agreement persists even when an observer performs his observation after the result has been communicated to him by another observer who has performed the observation.

2. Let one observer perform an observation of a quantity A in the object system, then let a second perform an observation of a quantity B in this object system which does not commute with A, and finally let the first observer repeat his observation of A. Then the memory system of the first observer will not in general show the same result for both observations. The intervening observation by the other observer of the noncommuting quantity B prevents the possibility of any one to one correlation between the two observations of A.

3. Consider the case where the states of two object systems are correlated, but where the two systems do not interact. Let one observer perform a specified observation on the first system, then let another observer perform an observation on the second system, and finally let the first observer repeat his observation. Then it is found that the first observer always gets the same result both times, and the observation by the second observer has no effect whatsoever on the outcome of the tirst's observations. Fictitious paraduxes like that of Einstein, Podolsky, and Rosen [8] which are concerned with such correlated, noninteracting systems are easily investigated and clarified in the present scheme.

Many further combinations of several observers and systems can be studied within the present framework. The results of the present "relative state" formalism agree with those of the conventional "external observation" formalism in all those cases where that familiar machinery is applicable.
In conclusion, the continuous evolution of the state function of a composite system with time gives a complete mathematical model for processes that involve an idealized observer. When interaction occurs, the result of the evolution in time is a superposition of states, each element of which assigns a different state to the memory of the observer. Judged by the state of the

memory in almost all of the observer states, the probabilistic conclusion of the usual "external observation"

formulation of quantum theory are valid. In other words, pure Process 2 wave mechanics, without any initial probability assertions, leads to all the probability concepts of the familiar formalism.

25.3.6 6. Discussion

The theory based on pure wave mechanics is a conceptually simple, causal theory, which gives predictions in accord with experience. It constitutes a framework in which one can investigate in detail, mathematically, and in a logically consistent manner a number of sometimes puzzling subjects, such as the measuring process itself and the interrelationship of several observers. Objections have been raised in the past to the conventional or "external observation" formulation of quantum theory on the grounds that its probabilistic features are postulated in advance instead of being derived from the theory itelf. We believe that the present "relativestate" formulation meets this objection, while retaining all of the content of the standard formulation.

While our theory ultimately justifies the use of the probabilistic interpretation as an aid to making practical predictions, it forms a broader frame in which to understand the consistency of that interpretation. In this respect it can be said to form a melaiheory for the standard theory. It transcends the usual "external observation" formulation, however, in its ability to deal logically with questions of imperfect observation and approximate measurement.

The "relative state" formulation will apply to all forms of quantum mechanics which maintain the superposition principle. It may therefore prove a fruitful framework for the quantization of general relativity. The formalism invites one to construct the formal theory first, and to supply the statistical interpretation later. This method should be particularly useful for interpreting quantized unified field theories where there is no question of ever isolating observers and object systems. They all are represented in a single structure, the field. Any interpretative rules can probably only be deduced in and through the theory itself.

Aside from any possible practical advantages of the thcory, it remains a matter of intellectual interest that the statistical assertions of the usual interpretation do not have the status of independent hypotheses, but are deducible (in the present sense) from the pure wave mechanics that starts completely free of statistical postulates.

25.4 II. 4 the Problem of Measurement by Wgnek

25.4.1 Introduction

The last few years have seen a revival of interest in the conceptual foundations of quantum mechanics. [1] This revival was stimulated by the attempts to alter the probabilistic interpretation of quantum mechanics. However, even when these attempts turned out to be less fruitful than its protagonists had hoped, [2] the interest continued. Hence, after the subject had been dormant for more than two decades, we again hear discussions on the basic principles of quantum theory and the epistemologies that are compatible with it. As is often the case under similar

Reprinted by permission from the American Journal of Physics, Vol. 31, No. 1 (Januery, 1963).

[88] Einstein, Podolsky, and Rosen, Phys. Rev. 47, 777 (1935). For a thorough discussion of the physics of observation, see the chapter by N. Bohr in Albert Einstein, Philosopher-Scientist (The Library of Living Philosophers, Inc., Evanston, 1949).

[1] Some of the more recent papers on the subject are: Y. Aharonov and D. Bohm, Phys. Rev., 122, 1649 (1961), Nuovo Cimento, 17, 964 (1960); B. Bertotti, Nuovo Cimento Suppl., 17, 1 (1960); L. de Broglie, J. Phys. Radium, 20, 963 (1959); 251. 462 (1960). insi. Henti Fuincure, 16, 269 (1960); A. Datzen, Compt. Rend., Hele. Phys. Acta 33 711 Gatum, 21, 201 (1960); 22, 101 (1961); M. Jauch, (1961). Am. Phes 503 (1961). H M, Physk, A Phys., 26, 727 (1961); A. Peres and P. Singer, Nuovo Cimento 15, 907 (1960). H. Putnam, Phil. Sci., 28, 234 (1961): M. Renninger, Z. Physik, 158, 417 (1960). L. Rosenfeld, Nature, 190, 384 (1961); F. Schlögl, Z. Physik, 159, 411 (1960); J. Schwinger, Proc. Natl. Acad. Sci. U.S., 46, 570 (1960); J. Tharrats, Compt. Rend., 250, 3786 (1960); H. Wakital, Progr. Theoref. Phys., 23, 32 (1960); 27, 139 (1962); W. Weidlich, Z. Naturforsch., 15a, 651 (1960); J. P Wesley, Phys. Rev., 122, 1932 (1961). See also the articles of E. Teller, M. Born, A. Land, F. Bopp, and G. Ludwig in Werner Hoisenherg und die Physik unserer Zeit (Braunschweig: Friedrich Vieweg und Sohn, 1961).

asee the comments of V. Fock in the Max Planck Festschrift (Berlin: Deutscher Verlag der Wissenschaften, 1958), p. 177, particularly Sec. II.

Originally published in American Journal of Physics, 31, 6-15 (1963). Reprinted in E. Wigner (1967), Symmetries and Reflections, Indiana University Press, Bloomington, pp. 153-170, from which book this paper is reproduced here.

circumstances, some of the early thinking had been forgotten: in fact, a small fraction of it remains as yet unrediscovered in the modern literature. Equally naturally, some of the language has changed but, above all, new ideas and new attempts have been introduced. Having spoken to many friends on the subject which will be discussed here, it became clear to me that it is useful to review the standard view of the late "Twenties," and this will be the first task of this article. The standard view is an ougrowth of Heisenberg's paper in which the uncertainty relation was first formulated. [3] The far-reaching implications of the consequences of Heisenberg's ideas were first fully appreciated, I believe, by von Neumann, [4] but many others arrived independently at conclusions similar to his. There is a very nice little book, by London and Bauer," which summarizes quite completely what I shall call the orthodox view.

The orthodox view is very specific in its epistemological implications. This makes it desirable to scrutinize the orthodox view very carefully and to look for loopholes which would make it possible to avoid the conclusions to which the orthodox view leads. A large group of physicists finds it difficult to accept these conclusions and, even though this does not apply to the present writer, he admits that the far-reaching nature of the epistemological conclusions makes one uncasy. The misgivings, which are surely shared by many others who adhere to the orthodox view, stem from a suspicion that one cannot arrive at valid epistemological conclusions without a caretul analysis of the process of the acquisition of knowledge. What will be analyzed, instead, is only the type of information which we can acquire and possess concerning the external inanimate world, according to quantum-mechanical theory.

We are facing here the perennial question whether we physicists do not go beyond our competence when searching for philosophical truth.

[3] W. Heisentoge, Z. Physih, 40, 172 (1927); also his aticle in Niels Bohy and the Decelopment of Physics (London: Pergamon Press, 1955); N. Bohr, Nature, 121, 580 (1928); Nuturisissen., 17, 483 (1929) and particularly Atomic Physics and Iluman Knowledge (New York: John Wiley & Sons, Inc., 1958).

[4] See J. von Neumann, Mathematische Grundlagen der Quantenmechanik (Berlin: Verlag Julius Springer, 1932), English translation (Princeton, N.j.: Princeton University Press, 193) Searle (Berlin: Julius Springer, 1936), Chape La

$^{-F}$ F. London and E. Bater, Las a secanique quantique Proc. Cambridge Phil. Soc., 31, 555 (1935).

I believe inat we probably do." Nevertheless, the ultimate implications of quantum theory's

formulation of the laws of physics appear interesting even if one admits that the conclusions to be arrived at may not be the ultimate truth.

25.4.2 The Orthodox View

The possible states of a system can be characterized, according to quantum-mechanical theory, by state vectors. These state vectors-and this is an almost verbatim quotation of von Neumann-change in two ways. As a result of the passage of time, they change continuously, according to Schrödinger's time-dependent equation-this equation will be called the equation of motion of quantum mechanics. The state vector also changes discontinuously, according to probability laws, if a measurement is carried out on the system. This second type of change is ofter called the reduction of the wavefunction. It is this reduction of the state vector which is unacceptable to many of our colleagues.

The assumption of two types of changes of the state vector is a strange dualism It is good to emphasize at this point that the dualism in question has little to do with the oft-discussed wave-versus-particle dualism. This latter dualism is only part of a more general pluralism or even "infinitesilism" which refers to the infinity of noncommuting measurable quantities. One can measure the position of the particles, or one can measure their velocity, or, in fact, an infinity of other observables. The dualism here discussed is a true dualism and refers to the two ways in which the state vector changes. It is also worth noting, though only parenthetically, that the probabilistic aspect of the theory is almost diametrically opposite to what ordinary experience would lead one to expect. The place where one expects probability laws to prevail is the change of the system with time. The interaction of the particles, their collisions, are the events which are ordinarily expected to be governed by statistical laws. This is not at all the case here: the uncertainty in the behavior of a system does not increase in time if the system is left alone, that is, if it is not subjected to measurements. In this case, the properties of the system, as described by its state vector,

[6] This point is particularly well expressed by H. Margenat, in the first two sections of the article in Phil. Sci., 25, 23 (1958).

change causally, no matter what the period of time is during which it is left alone. On the contrary, the phenomenon of chance enters when a measurement is carried out on the system, when we try to check whether is properties did change in the way our causal equations told us they would change. However, the extent to which the results of all possible measurements on the system can be predicted does not decrease, according to quantum-mechanical theory, with the time during which the system was left alone; it is as great right after an observation as it is a long time thereafter. The uncertainty of the result, so to say, increases with time for some measurements just as much as it decreases for others. The Liouville theorem is the analog for this in classical mechanics. It tells us that, if the point which represents the system in phase space is known to be in a finite volume element at one given time, an equally large volume element can be specified for a given later time which will then contain the point representing the state of the system. Similarly, the uncertainty in the result of the measurement of Q, at time 0 , is exactly equal to the uncertainty of the measurement of $Q_t = \exp(-iHt/\hbar)Q_0 \exp(iHt/\hbar)$ at time t. The information which is available at a later time may be less valuable than the information which was available on an earlier state of the system (this is the cause of the increase of the entropy); in principle, the amount of information does not change in time.

25.4.3 Consistency Of the Orthodox View

The simplest way that one may try to reduce the two kinds of changes of the state vector to a single kind is to describe the whole process of measurement as an event in time, governed

by the quantum-mechanical equations of motion. One might think that, if such a description is possible, there is no need to assume a second kind of change of the state vector; if it is impossible, one might conclude, the postulate of the measurement is incompatible with the rest of quantum mechanics. Unfortunately, the situation will turn out not to be this simple.

If one wants to describe the process of measurement by the equations of quantum mechanics, one will have to analyze the interaction between object and measuring apparatus. Let us consider a measurement from the point of view of which the "sharp" states are $\sigma^{(1)}, \sigma^{(2)}, \cdots$. For these states of the object the measurement will surely yield the values λ_1, λ_2. $\cdots$, respectively. Let us further denote the initial state of the apparatus by a; then, if the initial state of the system was $\sigma^{(\nu)}$, the total systemapparatus plus object-will be characterized, before they come into inieraction, by $a \times \sigma^{(2)}$. The interaction should not change the state of the object in this case and hence will lead to

$$a \times \sigma^{(v)} \to a^{(v)} \times \sigma^{(v)} \tag{1}$$

The state of the object has not changed, but the state of the apparatus has and will depend on the original state of the object. The different states $a^{(\nu)}$ may correspond to states of the apparatus in which the pointer has different positions, which indicate the state of the object. The state $a^{(p)}$ of the apparatus will therefore be called also "pointer position v." The state vectors $a^{(1)}, a^{(2)}, \cdots$ are orthogonal to each other -usually the corresponding states can be distinguished even macroscopically. Since we have considered, so far, only "sharp" states, for each of which the measurement in question surely yields one definite value, no statistical element has yet entered into our considerations. [7]

Let us now see what happens if the initial state of the object is not sharp, but an arbitrary linear combination $\alpha_1\sigma^{(1)} + \alpha_2\sigma^{(2)} + \cdots$. It then follows from the linear character of the quantum-mechanical equation of motion (as a result of the so-called superposition principle) that the state vector of object-plus-apparatus after the measurement becomes the right side of

$$a \times \left[\sum \alpha_v \sigma^{(v)}\right] \to \sum \alpha_v \left[a^{(v)} \times \sigma^{(v)}\right] \tag{2}$$

Naturally, there is no statistical element in this result, as there cannot be. However, in the state (2), obtained by the measurement, there is a statistical correlation between the state of the object and that of the apparatus: the simultaneous measurement on the system-object-plus-apparatus-of the two quantities, one of which is the originally measured quantity of the object and the second the position of the pointer of the apparatus, always leads to concordant results. As a result, one of these measurements is unnecessary: The state of the object can be ascertained by an observation on the apparatus. This is a consequence of the special form of the state vector (2), of not containing any $a^{(\nu)} \times \sigma^{(\mu)}$ term with $\nu \neq \mu$.

[7] The self-adjoint (Hermitean) character of every observable can be derived from Eq. (1) and the unitary nature of the transformation indicated by the arrow. Cf. E. Wigner Z ploye arrow. Cf. E. Wigner, Z. Physik, 133, 101 (1952), footnote 2 on p. 102.

It is well known that statistical correlations of the nature just described play a most important role in the structure of quantum mechanics. One of the earliest observations in this direction is Moti's explanation of the straight track left hy the spherical wave of outgoing α particles. [8] In fact, the principal conceptual difference between quantum mechanics and the earlier Bohr-Kramers-Slater theory is that the former, by its use of configuration space rather than ordinary space for its waves, allows for such statistical correlations.

Returning to the problem of measurement, we see that we have not arrived either at a conflict between the theory of measurement and the equations of motion, nor have we obtained an explanation of that theory in terms of the equations of motion. The equations of motion permit the description of the process whereby the state of the object is mirrored by the state of an ap-

paratus. The problem of a measurement on the object is thereby transformed into the problem of an observation on the apparatus. Clearly, further transfers can be made by introducing a second apparatus to ascertain the state of the first, and so on. However, the fundamental point remains unchanged and a full description of an observation must remain impossible since the quantum-mechanical equations of motion are causal and contain no statistical element, whereas the measurement does.

It should be admitted that when the quantum theorist discusses measurements, he makes many idealizations. He assumes, for instance, that the measuring apparatus will yield some resuit, no matter what the initial state of the object was. This is clearly unrealistic since the object may move away from the apparatus and never come into contact with it. More importantly, he has appropriated the word "measurement" and used it to characterize a special type of interaction by means of which information can be obtained on the state of a definite object. Thus, the measurement of a physical constant, such as cross section, does not fall into the category called "measurement" by the theorist. His measurements answer only questions relating to the ephemeral state of a physical system, such as, "What is the x component of the momentum of this atom?" On the other hand, since he is unable to follow the path of the information until it enters his, or the observer's, mind, he considers the measurement completed as soon as a statistical relation has been established between the quantity to be measured and the state of some

[8] N. F. Mott, Proc. Roy. Soc. (London), 126, 79 (1929).

idealized apparatus. He would do well to emphasize his rather specialized use of the word "measurement."

This will conclude the review of the orihodox theory of measurement. As was mentioned before, practically all the foregoing is contained, for instance, in the book of London and Bauer.

25.4.4 Critiques Of the Orthodox Theory

There are attempts to modify the orthodox theory of measurement by a complete departure from the picture epitomized by Eqs. (1) and (2). The only attempts of this nature which will be discussed here presuppose that the result of the measurement is not a state vector, such as (2), but a so-called mixture, namely, one of the state vectors

$$a^{(\mu)} \times \sigma^{(\mu)} \tag{3}$$

and that this particular state will cmerge from the interaction between object and apparatus with the probability $|\alpha_\mu|^2$. If this were so, the state of the system would not be changed when one ascertains-in some unspecified way-which of the state vectors (3) corresponds to the actual state of the system; one would merely "ascertain which of various possibilities has occurred." In other words, the final observation only increases our knowledge of the system; it does not change anything. This is not true if the state vector, after the interaction between object and apparatus, is given by (2) because ine side represented by the vector (2) has properties which neither of the states (3) has. It may be worthwhile to illustrate this point, which is fundamental though often disregarded, by an example.

The example is the Stern-Gerlach experiment, [9] in which the projection of the spin of an incident beam of particles, into the direction which is perpendicular to the plane of the drawing, is measured. (See Fig. 1.) The index ν has two values in this case; they correspond to the two possible orientations of the spin. The "apparatus" is that positional coordinate of the particle which is also perpendicular to the plane of the drawing. If this coordinate becomes, in the experiment illustrated, positive, the spin is directed toward us; if it is negative, the spin is directed away from us. The experiment illustrates the statistical correla-

[9] The same experiment was discussed recently from another point of view by H. Wakita, Progr.

Theoret. Phys., 27, 139 (1962).
tion between the state of the "apparatus" (the position coordinate) and the state of the object (the spin) which we have discussed. The ordinary use of the experiment is to obtain the spin direction, by observing the position, i.e., the location of the beam. The measurement is, therefore, as far as the establishment of a statistical correlation is concerned, complete when the particle reaches the place where the horizontal spin arrows are located.

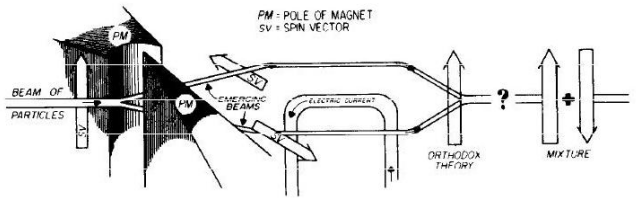


Fig. 1

What is important for us, however, is the right side of the drawing. This shows that the state of the system-object-plus-apparatus (spin and positional coordinates of the particle, i.e., the whole state of the particle)shows characteristics which neither of the separated beams alone would have. If the two beams are brought together by the magnetic field due to the current in the cable indicated, the two beams will interfere and the spin will he vertical again. This could be verified by letting the united beam pass through a second magnet which is, however, not shown on the figure. If the state of the system corresponded to the beam toward us, its passage through the second magnet would show that it has equal probabilities to assume its initial and the opposite directions. The same is true of the second beam which was deflected away from us. Even though the experiment indicated would be difficult to perform, there is little doubt that the behavior of particles and of their spins conforms to the equations of motion of quantum mechanics under the conditions considered. Hence, the properties of the system, object-plus-apparatus, are surely correctly represented by an expression of the form (2) which gives, in this case, properties which are different from those of either alternative (3).

In the case of the Stern-Gerlach experiment, one can thus point to a
specific and probably experimentally realizable way to distinguish between the state vector (2), furnished by the orthodox theory, and the more easily visualizable mixture of the states (3) which one would offhand expect. There is little doubt that in this case the orthodox theory is correct. It remains remarkable how difficult it is, even in this very simple case, to distinguish between the two, and this raises two questions. The first of these is whether there is, in more complicated cases, a principle which makes the distinction between the state vector (2), and the mixture of the states (3), impossible. As far as is known to the present writer, this question has not ever been posed seriously heretofore, and it will be considered in the present discussion also only obliquely. The second question is whether there is a continuous transition between (2) and the mixture of states (3) so that in simpler cases (2) is the result of the interaction between object and measuring apparatus, but in more complicated and more realistic cases the actual state of object-plusapparatus more nearly resembles a mixture of the states (3). Again, this question can be investigated within the framework of quantum mechanics, or one can postulate deviations from the quantum-mechanical equations of motion, in particular from the superposition principle.

"More complicated" and "more redistic" mean in the present contexi that the measuring apparatus, the state of which is to be correlated with the quantity to be measured, is of such a nature that it is easy to measure its states, i.e., correlate it with the state of another "apparatus." If this is done, the state of that second "apparatus" will be correlated also to the state of the object. The case of establishing correlations between the state of the apparatus which

came into direct contact with the object and another "apparatus" is usually greatest if the first one is of macroscopic nature, i.e., complicated from the quantum-mechanical point of view. The ease with which the secondary correlations can be established is a direct measure of how realistically one can say that the measurement has been completed. Clearly, if the state of the apparatus which carried out the primary measurement is just as difficult to ascertain as the state of the object, it is not very realistic to say that the establishment of a correlation between its and the object's state is a fully completed measurement. Nevertheless, it is so regarded by the orthodox theory. The question which we pose is, therefore, whether it is consistent with the principles of quantum mechanics to assume that at the end of a realistic measurement the state of object-plus-apparatus is not a
wavefunction, as given by (2), but a mixture of the states (3). We shall see that the answer is negative. Hence, the modification of the orihodox thcory of measurement mentioned at the beginning of this section is not consistent with the principles of quantum mechanics.

Let us now proceed with the calculation. Even though this point is not usually emphasized, it is clear that, in order to obtain a mixture of states as a result of the interaction, the initial state must have been a mixture already. [10] This follows from the general theorem that the characteristic values of the density matrix are constants of motion. The assumption that the initial state of the system, object-plus-apparatus, is a mixiure, is indeed a very natural one because the state vector of the apparatus, which is under the conditions now considered usually a macroscopic object, is hardly ever known. Let us assume, therefore, that the initial state of the apparatus is a mixture of the states $\dot{A}^{(i)}, \dot{A}^{(i)}, \cdots$, the probability of $A^{(\rho)}$ being p_ρ. The vectors $A^{(\rho)}$ can be assumed to be mutually orthogonal. The equations of motion will yield, for the state $A^{(\rho)}$ of the apparatus and the state $\sigma^{(\nu)}$ of the object, a final state

$$A^{(\rho)} \times \sigma^{(\nu)} \rightarrow A^{(\rho\nu)} \times \sigma^{(\nu)} \tag{4}$$

Every state $A^{(1\nu)}, A^{(2\nu)}, \cdots$ will indicate the same state $\sigma^{(\nu)}$ of the object; the position of the pointer is v for all of these. For different v, however, the position of the pointer is also different. It follows that the $A^{(\rho v)}$, for different v, are orthogonal, even if the ρ are also different. On the other hand, $A^{(\rho\nu)}$ and $A^{(\sigma\nu)}$, for $\rho \neq \sigma$, are also orthogonal because

[10] This point is disregarded by several authors who have rediscovered von Neumann's description of the measurement, as given by (1) and (2). These authors assume that it follows from the macroscopic nature of the measuring apparatus that if several values of the "pointer position" have finite probabilities tas is the case if the state vector is (2)], the state is necessarily a mixture (rather than a linear combination) of the states (3)-that is, of states in each of which the ponter po macrodefinite (sharp). The argument given is ave no counterpart in classical theory. This argument is contrary to present quantum-mechanical theory. It is true that the mution of a macroscopic bodv can be adequately described by the classical equations of motion if its state has a classical description. That this last premise is, according to present theore, not always fulfilled, is clearly, though in an extreme fashion, demonstrated by Schrödinger's cat-paradox (cf. reference 5). Further, the discussion of the Stem-Gerlach experiment, given in the text, illustrates the fact that there are, of principle, ohservable differences hetween state vector given definite position. Pro(2), and the mixture of the states (a), each equations of motion so as to permit a posature of the states (3) to be the result of the measurement even though the initial state was a state vector, will be touched upon later.

$A^{(\rho\nu)} \times \sigma^{(\nu)}$ and $A^{(\sigma\nu)} \times \sigma^{(\nu)}$ are obtained by a unitary transformation from two orthogonal states, $\dot{A}^{(p)} \times \sigma^{(v)}$ and $\dot{A}^{(v)} \times \sigma^{(v)}$ and the scalar product of $A^{(\rho\nu)} \times \sigma^{(\nu)}$ with $A^{(\sigma\nu)} \times \sigma^{(\nu)}$ is ($A^{(\rho\nu)}, A^{(\sigma\nu)}$). Hence, the $A^{(\rho\nu)}$ form an orthonormal (though probably not complete) system

$$\left(A^{(\rho\nu)}, A^{(\sigma\mu)}\right) = \delta_{\rho\mu\delta}\delta_{v\mu} \tag{5}$$

It again follows from the linear character of the equation of motion that, if the initial state

of the object is the linear combination $\sum \alpha_\nu \sigma^{(\nu)}$, the state of object-plus-apparatus will be, after the measurement, a mixture of the states

$$A^{(\rho)} \times \sum \alpha_v \sigma^{(\nu)} \rightarrow \sum_v \alpha_v \left[A^{(\rho\nu)} \times \sigma^{(\nu)}\right] = \Phi^{(\rho)}, \tag{6}$$

with probabilities p_ρ. This same mixture should then be, according to the postulate in question, equivalent to a mixture of orthogonal states

$$\Psi^{(\mu h^i)} = \sum_\rho x_\rho{}^{(\mu k)} \left[A^{(\rho\mu)} \times \sigma^{(\mu)}\right]. \tag{7}$$

These are the most general states for which the originally measured quantity has a definite value, namely λ_μ, and in which this state is coupled with some state (one of the states $\sum_\mu x_\mu{}^{(\mu\kappa)} A^{(\rho\mu)}$) with a pointer position μ. Further, if the probability of the state $\Psi^{(\mu k)}$ is denoted by $P_{\mu k}$, we must have

$$\Sigma k P_{\mu k} = |\alpha_\mu|^2 \tag{7a}$$

The $x_\rho{}^{(\mu^h)}$ will naturaliy depend on the α.
It turns out, however, that a mixture of the states $\Phi^{(\rho)}$ cannot be, at the same time, a mixture of the states $\Psi^{(\mu t^*)}$ (unless only one of the α is different from zero). A necessary condition for this would be that the $\Psi^{(\mu)^\circ)}$ are linear combinations of the $\Phi^{(\rho)}$, so that one should be able to find coefficients u so that

$$\sum \rho x_\rho^{(\mu z)} \left[A^{(\rho\mu)} \times v^{(\mu)}\right] - \Psi^{(\mu,l)} - \sum \rho u_\rho \Psi^{(\rho)}$$

$$= \sum_{\rho\nu} u_\rho \alpha_\nu \left[A^{(\rho\nu)} \times \sigma^{(\nu)}\right]. \tag{8}$$

From the linear independence of the $A^{(\rho\nu)}$ it then follows that

$$u_\rho \alpha_\nu = \delta_{\nu\mu} x_\rho{}^{(\mu k)} \tag{8a}$$

which cannot be fulfilled if more than one α is finite. It follows that it is not compatible with the equations of motion of quantum mechanics to assume that the state of object-plus-apparatus is, after a measurement, a mixture of states each with one definite position of the pointer.
It must be concluded that measurements which leave the system ob-jeci-plus-apparatus in one of the states with a definite position of the pointer cannot be described by the linear laws of quantum mechanics. Hence, if there are such measurements, quantum mechanics has only limited validity. This conclusion must have been familiar to many even though the detailed argument just given was not put forward before. Ludwig, in Cermany, and the present writer have independently suggested that the equations of motion of quantum mechanics must be modified so as to permit measurements of the aforementioned type. [11] These suggestions will not be discussed in detail because they are suggestions and do not have convincing power at present. Even though either may well be valid, one must conclude that the only known theory of measurement which has a solid foundation is the orthodox one and that this implies the dualistic theory concerning the changes of the state vector. It implies, in particular, the so-called reduction of the state vector. However, to answer the question posed earlier: yes, there is a continuous transition between the state vector (2), furnished by orthodox theory, and the requisite mixture of the states (3), postulated by a more visualizable theory of measurement.
[11]

25.4.5 What Is the State Vector?

The state vector concept plays such an important part in the formulation of quantum-mechanical theory that it is desirable to discuss its role and the ways to determine it. Since, according to quantum mechanics, all information is obtained in the form of the results of measurements, the standard way to obtain the state vector is also by carrying out measurements on the system. [12]

In order to answer the question proposed, we shall first obtain a for-

[11] See G. Ludwig's article "Solved and Unsolved Problems in the Quantum Mechanics of Measurement" (reference 1) and the present author's article Remarks on the Mind-Body Question in The Scientist Speculates, edited by I. J. Good (London: William Heinemann, 1962), p. 284, reprinted in this volume.

12 There are, nevertheless, other procedures to bring a system into a definite state. These are based on the fact that a small system, if it interacts with a large system in a definite and well-known state, may assume itself a definite state with almost absolute certainty. Thus, a hydrogen atom, in some state of excitation, if placed into a large container with no radiation in it, willor preparing a state has been particularly stressed by H. Margenau.

mula for the probability that successive measurements carried out on a system will give certain specified results. This formula will be given both in the Schrödinger and in the Heisenberg picture. Let us assume that n successive measurements are carried out on the system, at times $t_1, t_2, \cdots, t_n$. The operators of the quantities which are measured are, in the Schrodinger picture, $Q_1, Q_2, \cdots, Q_n$. The characteristic vectors of these will all be denoted by ψ with suitable upper indices. Similarly, the characteristic values will be denoted by q so that

$$Q_i \psi_\kappa^{(j)} = q_\kappa^{(j)} \psi_\kappa^{(j)} \tag{9}$$

The Heisenberg operators which correspond to these quantities, if measured at the corresponding times, are

$$Q_j^H = e^{iHi}{}_j Q_j e^{-iIIi}{}_j \tag{10}$$

and the characteristic vectors of these will be denoted by ${\varphi_\kappa}^{(j)}$, where

$${\varphi_\kappa}^{(j)} = e^{iHt}{}_j {\psi_\kappa}^{(j)} \quad {Q_j}^H {\varphi_\kappa}^{(j)} = {q_\kappa}^{(j)} {\varphi_\kappa}^{(j)}. \tag{10a}$$

If the state vector is originally Φ, the probability for the sequence ${q_\alpha}^{(1)}, {q_\beta}^{(2)}, \ldots, {q_\mu}^{(n)}$ of measurement-results is the absolute square of

$$\left(e^{-iHt_1}\Phi, \psi_\alpha^{(1)}\right)\left(e^{-iH(t_2-t_1)}\psi_\alpha^{(1)}, \psi_\beta^{(2)}\right)\cdots\cdots \left(e^{-iH(t_n-t_{n-1})}\psi_\lambda^{(n-1)}, \psi_\mu^{(n)}\right) \tag{11}$$

The same expression in terms of the characteristic vectors of the Heisenberg operators is simpler,

$$\left(\Phi, \varphi_\alpha^{(1)}\right)\left(\varphi_a^{(1)}, \varphi_\beta^{(2)}\right)\cdots\left(\varphi_\lambda^{(n-1)}, \varphi_\mu^{(n)}\right). \tag{11a}$$

It should be noted that the probability is not determined by the n Heisenberg operators ${Q_j}^H$ and their characteristic vectors: the time order in which the measurements are carried out enters into the result essentially. Von Neumann already derived these expressions as well as their generalizations for the case in which the characteristic values ${q_\alpha}^{(1)}, {q_\beta}^{(2)}, \cdots$ have several characteristic vectors. In this case, it is more appropriate to introduce projection operators for every characteristic value $q^{(j)}$ of every Heisenberg operator ${Q_j}^H$. If the projection

opcrator in question is denoted by $P_{j\kappa}$, the probability for the sequence ${q_\alpha}^{(1)}, {q_\beta}^{(2)}, \cdots, {q_\mu}^{(n)}$ of measurement-results is

$$(P_{n\mu} \cdots P_{2\beta} P_{1\alpha\Phi}, P_{n\mu} \cdots P_{2\beta} P_{1\alpha} \Phi) \tag{12}$$

The expressions (11) or (11a) can be obtained also by postulating that the state vector became ${\psi_\kappa}^{(j)}$ when the measurement of $Q^{(j)}$ gave the result ${q_\kappa}^{(j)}$. Indeed, the statement that the state vector is ${\psi_\kappa}^{(j)}$ is only a short expression for the fact that the last measurement on the system, of the quantity $Q^{(j)}$, just carried out, gave the result ${q_\kappa}^{(j)}$. In the case of simple characteristic values the state vector depends only on the result of the last measurement and the future behavior of the system is independent of the more distant past history thereof. This is not the case if the characteristic value $\boldsymbol{q}^{(j)}$ is multiple.

The most simple expression for the Heisenberg state vector, when the j th measurement gave the value $q_\kappa^{(j)}$, is, in this case,

$$P_{jk} \cdots P_{2\beta} P_{1\kappa} \Phi \tag{12a}$$

properly normalized. If, after normalization, the expression (12a) is independent of the original state vector Φ, the number of measurements has sufficed to determine the state of the system completely and a pure state has been produced. If the vector (12a) still depends on the original state vector Φ, and if this was not known to begin with, the state of the system is a mixture, a mixture of all the states ($12a$), with all possible Φ. Evidently, the measurement of a single quantity Q, the characteristic values of which are all nondegenerate, suffices to bring the system into a pure state though it is not in general foreseeable which pure state will result.

We recognize, from the preceding discussion, that the state vector is only a shorthand expression of that part of our information concerning the past of the system which is relevant for predicting (as far as possible) the future behavior thereof. The density matrix, incidentally, plays a similar role except that it does not predict the future behavior as completely as does the state vector. We also recognize that the laws of quantum mechanics only furnish probability connections between results of subsequent observations carried out on a system. It is true, of course, that the laws of classical mechanics can also be formulated in terms of such probability connections. However, they can be formulated also in terms of objective reality. The important point is that the laws of quantum mechanics can be expressed only in terms of probability connections.

25.4.6 Problems Of the Orthodox View

The incompatibility of a more visualizable interpretation of the laws of quantum mechanics with the equations of motion, in particular the superposition principle, may mean that the orthodox interpretation is here to stay; it may also mean that the superposition principle will have to be abandoned. This may be done in the sense indicated by Ludwig, in the sense proposed by me, or in some third, as yet unfathomed sense. The dilemma which we are facing in this regard makes it desirable to review any possible conceptual weaknesses of the orthodox interpretation and the present, last, section will be devoted to such a review.

The principal conceptual weakness of the orthodox view is, in my opinion, that it merely abstractly postulates interactions which have the effect of the arrows in (1) or (4). For some observables, in fact for the majority of them (such as xyp), nobody seriously believes that a measuring apparatus exists. It can even be shown that no observable which does not commute with the additive conserved quantities (such as linear or angular momentum or electric charge) can be measured precisely, and in order to increase the accuracy of the measurement one has to use a very large measuring apparatus. The simplest form of the proof heretofore was given

by Araki and Yanase. [13] On the other hand, most quantities which we believe to be able to measure, and surely all the very important quantities such as position, momentum, fail to commute with all the conserved quantities, so that their measurement cannot be possible with a microscopic apparatus. This raises the suspicion that the macroscopic nature of the apparatus is necessary in principle and reminds us that our doubts concerning the validity of the superposition principle for the measurement process were connected with the macroscopic nature of the apparatus. The oint state vector (2), resulting from a measurement with a very large apparatus, surely cannot be distinguished as simply from a mixture as was the state vector obtained in the Stern-Gerlach experiment which we discussed. [14]

A second, though probably less serious, difficulty arises if one tries to

13 H. Araki and M. Yanase, Phys. Rev., 120, 666 (1961); cf. also E. P. Wigner, Z. Physik, 131, 101 (1952).

14 This point was recognized already by D. Bohm. See Section 22.11 of his Quantum Theory (Englewood Cliffs, New Jersey: Prentice-Hall, Inc., 1951).

calculate the probability that the interaction between object and apparatus be of such nature that there exist states $\sigma^{(\nu)}$ for which (1) is valid. We recall that an interaction leading to this equation was simply postulated as the type of interaction which leads to a measurement. When I talk about the probability of a certain interaction, I mean this in the sense specified by Rosenzweig or by Dyson, who have considered ensembles of possible interactions and defined probabilities for definite interactions. [15] If one adopts their definition (or any similar definition) the probability becomes zero for the interaction to be such that there are states $\sigma^{(\nu)}$ satisfying (1). The proof for this is very similar to that [16] which shows that the probability is zero for finding reproducing systems-in tact, according to (1), each $\sigma^{(\nu)}$ is a reproducing system. The resolution of this difficulty is prosumably that if the system with the state vector a-that is, the apparatus-is very large, (1) can be satisfied with a very small error. Again, the large size of the apparatus appears to be essential for the possibility of a measurement.

The simplest and least technical summary of the conclusions which we arrived at when discussing the orthodox interpretation of the quantum laws is that these laws merely provide probability connections between the results of several consecutive observations on a system. This is not at all unreasonable and, in fact, this is what one would naturally strive for once it is established that there remains some inescapable element of chance in our measurements. However, there is a certain weakness in the word "consecutive," as this is not a relativistic concept. Most observations are not local and one will assume, similarly, that they have an irreducible extension in time, that is, duration. However, the "observables" of the present theory are instantaneous, and hence unrelativistic, quantities. The only exceptions from this are the local field operators and we know, from the discussion of Bohr and Rosenfeld, how many extreme abstractions have to be made in order to describe their measurement. [15] This is not a reassuring state of affairs.

15 C. E. Porter and N. Rosenzweig, Suomalaisen Tiedeakatemian Toimotuksia, VI, No. 44 (1960); Phys. Rev., 120, 1698 (1960); F. Dyson, J. Math. Phys., 3, 140, 157, 166 (1962). See also E. P. Wigner, Proceedings of the Fourth Canadian Mathematics Congress (Toronto: University of Toronto Press, 1959), p. 174, reprinted in this volume.

[16] Cf. the writer's article in The Logic of Personal Knowledge (London: Routledge and Kegan Paul, 1961), p. 231, reprinted in this volume.

N. Bohr and L. Rosenteld, Kgl. Danske Videnskab. Selskab, Mat.-fys. Medd., 12, No. (1. B. Corinaldesi, Nuovo Cimento, 8, 494 (1951); B. Ferretti, ibid., 12, 558 (1954).

The three problems just discussed-or at least two of them-are real. It may be useful, therefore, to re-emphasize that they are problems of the formal mathematical theory of measurement, and of the descripition of measurements by macroscopic apparatus. They do not affect the conclusion that a "reduction of the wave packet" (however bad this terminology may be) takes

place in some cases. Let us consider, for instance, the collision of a proton and a neutron and let us imagine that we view this phenomenon from the coordinate system in which the center of mass of the colliding pair is at rest. The state vector is then, if we disregard the unscattered beam, in very good approximation (since there is only S -scattering present),

$$\psi(r_n, r_n) = r^{-1} e^{ikr} w(r) \tag{13}$$

where $r = |r_p - r_n|$ is the distance of the two particles and $w(r)$ some very slowly varying damping function which vanishes for $r < r_0 - 1/2c$ and $r > r_0 + 1/2c$, where r_0 is the mean distance of the two particles at the time in question and c the coherence length of the beam. If a measurement of the momentum of one of the particles is carried out-the possibility of this is never questioned-and gives the result **p**, the state vector of the other particle suddenly becomes a (slightly damped) plane wave with the momentum - **p**. This statement is synonymous with the statement that a measurement of the momentum of the second particle would give the result - **p**, as follows from the conservation law for linear momentum. The same conclusion can be arrived at also by a formal calculation of the possible results of a joint measurement of the momenta of the two particles.

One can go even further [1 K] : instead of measuring the linear momentum of one particle, one can measure its angular momentum about a fixed axis. If this measurement yields the value $m\hbar$, the state vector of the other particle suddenly becomes a cylindrical wave for which the same component of the angular momentum is - $m\hbar$. This statement is again synonymous with the statement that a measurement of the said component of the angular momentum of the second particle certainly would give the value - $m\hbar$. This can be inferred again from the conservation law of the angular momentum (which is zero for the two

18 See, in this connection, the rather similar situation discussed by A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev., 47, 777 (1935).
particles together) or by means of a formal analysis. Hence, a "contraction of the wave packet" took place again.

It is also clean inat it would be wrong, in the preceding example, to say that even before any measurement, the state was a mixture of plane waves of the two particles, traveling in opposite directions. For no such pair of plane waves would one expect the angular momenta to show the correlation just described. This is natural since plane waves are not cylindrical waves, or since (13) is a state vector with properties dif. ferent from those of any mixture. The statistical correlations which are clearly postulated by quantum mechanics (and which can be shown also experimentally, for instance in the Bothe-Geiger experiment) demand in certain cases a "reduction of the state vector." The only possible question which can yet be asked is whether such a reduction must be postulated also when a measurement with a macroscopic apparatus is carried out. The considerations around Eq. (8) show that even this is true if the validity of quantum mechanics is admitted for all systems.

25.5 II. 5 on the Interpretation of Measurement in Quantum Theory by Zen (1969)

It is demonstrated that neither the arguments leading to inconsistencies in the description of quantum-mechanical measurement nor those "explaining" the process of measurement by means of thermodynamical statistics are valid. Instead, it is argued that the probability inierpretuion is compailite with un objective interpretuitun of the wave function.

1. INTRODUCTION

The problem of measurement in quantum theory and the related problem of how to describe classical phenomena in the framework of quantum theory have received increased attention during recent years. The various contributions express very different viewpoints, and may roughly be classified as follows:

1. Those emphasizing contradictions obtained when the process of measurement is itself described in terms of quantum theory. (1)

2. Those claiming that measurement may well be explained by quantum theory in the sense that "quantum-mechanical noncausality" can be derived from statistical uncertainties inherent in the necessarily macroscopic apparatus of measurement. (2)

3. Those introducing new physical concepts like hidden variables. (3)

Suggestions of the third group are usually based on the first viewpoint, and are meaningful only if they lead to experimental consequences. These have not been confirmed so far.

Originally published in Foundations of Physics, 1, 69-76 (1970).

A measurement in quantum theory is axiomatically described by means of a Hermitian operator. If the eigenstates of this operator are φ_n, and the state of the measured system S is $\varphi = \sum c_n \varphi_n$, then, according to the axiom, the result of the measurement will, with probability $| c_n!^2$, be the corresponding eigenvalue a_n represented physically by a "pointer position," i.e., by an appropriate state of the measuring device M. For the most frequent class of measurements, it is furthermore predicted that any following measurement can be described by assuming S to be in the state φ_n after the measurement.

When describing the process of measurement as a whole in the framework of quantum theory, it is assumed that the apparatus M can be described by a wave function ϕ_ν, the state of the total system $M + S$ obeying the Schrödinger equation,

$$\dot{\psi}(t) = \mathrm{e}^{iH^t} \dot{\phi}_\alpha \sum_n c_n \varphi_n = \sum_{n,m,\beta} c_n U^{nm}_{\alpha\beta}(i) \dot{\phi}_\beta \varphi_m \tag{1}$$

with $U^{nm}_{\alpha\beta}(0) = \delta_{nm}\delta_{\alpha\beta}$. As the state of a macrosconic anparatus can be determined only incompletely, there must be a large set of states $\{\phi\}_0$ compatible with the knowledge about M. If this set of states is assumed to be independent of the state of S bcforc mcasurement, a condition on the coefficients $U^{nm}_{\alpha\beta}(t)$ can be derived from the requirement that the axiom of measurement be fulfilled in the case $c_n = \delta_{nn_0}$, i.e., $\varphi = \varphi_{n_0}$. The interaction must be of the von Neumann type (4)

$$U^{nm}_{\approx\Omega}(t) = \delta_{nm} u^n_{\Omega R}(t) \tag{2}$$

for all but a negligible measure of states of the set $\{\phi\}_0$, and for times t larger than the duration of the measurement. Furthermore, practically all states $\sum_\beta u^n_{\alpha,\beta}(t)\phi_\beta$ must be members of a set $\{\phi\}_n$ corresponding to a "pointer position n " of M.

In the case of a general state φ, the final total state now takes the form

$$\psi(t) = \sum_{n,\beta} c_n u^n_{xB}(t) \phi_B \varphi_n \tag{3}$$

It represents a superposition of different pointer positions. This result is said to be in contradiction to the axiom of measurement, because the latter states that the result of the measurement is one of the states $\sum_\beta u^n_{\alpha\beta}(t)\phi_\beta\varphi_n$. It is of course very unsatisfactory to assume that the laws of nature change according to whether or not a physical process is a measurement.

The difficulties arising when a macroscopic system is described by quantum theory can be seen more directly by applying the main axiom of quantum theory, i.e., the superposition principle. If there are two possible pointer positions $\{\phi\}_{n_1}$ and $\{\phi\}_{n_2}$, any superposition $c_1\phi_{n_1} + c_2\phi_{n_2}$ must be a possible state. As such superpositions have never been observed (see Wigner [1]) one should at least find dynamical causes for their nonoccurrence. Although recent work [5] has shown that dynamical stability conditions in the original sense of Schrödinger's [6] have a much wider field of applicability than previously expected, the process of measurement does not, because of the above arguments, belong to this class of phenomena.

2. CRITICISM OF STATISTICAL INTERPRETATIONS

Resuits apparentiy in contradiction to those of the preceding section have been derived in a series of papers [2] which try to make use of the uncertainties in the microscopic properties of the apparatus of measurement. The mathematical concept used in these theories is the density matrix formalism.

A simple example may illustrate such theories. If the density matrix describing M is $\sum_\alpha p_\alpha \phi_\alpha \phi_\alpha{}^*$, the total system is described by

$$\rho(0) = \sum_{\alpha,n,n'} p_\alpha c_n c_n^* \phi_\alpha \phi_\alpha^* \varphi_n \varphi_{n'}^* \tag{4}$$

For a von Neumann interaction, one obtains

$$\bar{\rho}(t) = \mathrm{e}^{iHt}\hat{\rho}(0)\mathrm{e}^{-iHt} = \sum_{\alpha n n' \beta \beta'} \bar{\rho}_\alpha c_n c_n^*, \dot{u}_{\alpha\beta}^n(t) u_{\alpha\beta'}^{*n'}(t) \phi_\beta \phi_{\beta'}^* \varphi_n \widetilde{\varphi}_{n'}^* \tag{5}$$

Provided the coefficients $u_{\alpha\beta}^n(t)$ possess arbitrarily distributed phases guaranteeing that

$$\sum_\alpha p_\alpha u_{\alpha\beta}^*(i) u_{\alpha\beta'}^{**\prime}(i) \approx \delta_{nn'} q_{\beta\beta'}^*(i) \tag{6}$$

(the diagonality in $\beta\beta'$ is not needed), $\rho(t)$ becomes

$$\rho(t) \approx \sum_n |c_n|^{\bar{z}} \varphi_n \varphi_n^* \sum_{BB'} q_{BB'}^n(t) \dot{\phi}_B \dot{\phi}_{B'}^* \tag{7}$$

This density matrix describes exactly the situation postulated by the axiom of measurement. [4]

It is tempting to interpret this result by saying that the statistical uncertainty inherent in the macroscopic apparatus is transferred by means of the interaction to the system S. This means that the outcome of a measurement, i.e., the pointer position, should be exactly predictable if we knew the microscopic state of M. Equation (3) demonstrates that this interpretation is wrong. [1]

The contradiction hetween Fqs. (3) and (7) is-aside from the dubious nature of the statistical assumption-due to a circular argument. The density matrix formalism is itself based upon the axiom of measurement. In order to see this, consider the case of a set of states $\psi^{(i)} = \sum_n c_n^{(i)} \psi_n$ prepared with probabilities $p^{(i)}$. The probability of finding the eigenvalue a_n is then

$$w_n = \sum_i p^{(i)} \left| c_n^{(i)} \right|^2 = \mathrm{tr}\,\{P_n \rho\} \tag{8}$$

[1] The above example is not identical with any of the theories of Ref. 2. It does not, however, use any additional assumptions. As it leads to a contradiction, one of the assumptions used must be wrong. Some of these theories do not start with an ensemble for the initial state of the apparatus, but assume instead that the "pointer position" is represented by some time average.

The latter is then transformed into an ensemble average by means of the ergodic theorem. Interpreted rigorously, these theories would prove that the pointer position fluctuates in time. if $P_n = \psi_n {\psi_n}^*$, and $\rho = \sum_i p^{(i)} \psi^{(i)} \psi^{(i)*}$. The states $\psi^{(i)}$ will in general not be linearly independent, although ρ may of course be expanded quadratically in terms of a complete orthogonal set. The reason for the usefulness of p is that, according to the axiom of measurement, all observable quantities can be expressed as linearantilinear functionals of the wave function.

For example, the statistical ensemble consisting of equal probabilities of neutrons with spin up and spin down in the x direction cannot be distinguished by measurement from the analogous ensemble having the spins parallel or antiparallel to the y direction. Both ensembles, however, can be easily prepared by appropriate versions of the Stern-Gerlach experiment. One is justified in describing both ensembles by the same density matrix as long as the axiom of measurement is accepted. However, the density matrix formalism cannot be a complete description of the ensemble, as the ensemble cannot be rederived from the density matrix. The discrepancy between Eqs. (3) and (7) arises since, on the one hand, Eq. (3) must hold for all but a negligible number of members of the ensemble, whereas Eq. (7) is interpreted as describing an ensemble of states $\varphi_n \sum_\beta u^*_{\alpha\beta}(I)\dot{\phi}_\beta$, i.e., each state being essentially different from (3). Only if the measurement axiom is accepted can these ensembles not be distinguished by subsequent observations.

The circularity is more obvious in some versions which avoid the density matrix formalism (e.g., Rosenfeld [2] who made repeated use of the probability interpretation although the latter is to be derived). In such cases, the circular argument is considered a "proof of consistency." This viewpoint cannot be accepted, as it would mean that the secondary observation of the pointer position (by a conscious observer or a second apparatus) is a measurement in the axiomatic sense. It corresponds to the interpretation of measurement due to Heisenberg and von Neumann [4] (claiming the arbitariness of the position of the "Heisenbergscher Schniti"), and does not require any contribution from thermodynamics. Bohm's analysis of the process of measurement, [i] however, shows the importance of the amplification of the result of a measurement up to the macroscopic scale, thus leading to a natural position of the "Heisenbergscher Schnitt." (Relative phases between microscopically realized pointer positions could still be measured.)

The secondary (macroscopic) observation is significantly different from the primary (microscopic) one, for the physical situation between these two observations is described by the reduced wave function. The macroscopic observation can thus be performed in a reversible way, in contrast to the microscopic one, which must result in the reduction. It is implicitly assumed in applying the density matrix formalism that the macroscopic measurement is accompanied by a reduction of the wave function.

3. CONSEQUENCES OF A UNIVERSAIIY VALID QUANTUM THEORY

The arguments presented so far were based on the assumption that a macroscopic system (the apparatus of measurement) can be described by a wave function ϕ. It appears that this assumption is not valid, for dynamical reasons:

If two systems are described in terms of basic states $\phi^{(1)}_{k_1}$ and $\phi^{(2)}_{k_2}$, the wave function of the total system can be written as $\phi = \sum_{k_1 k_2} c_{k_1 k_2} \phi^{(1)}_{k_1} \phi^{(2)}_{k_2}$. The case where the subsystems are in definite states ($\phi = \phi^{(1)}\phi^{(2)}$) is therefore an exception. Any sufficiently effective interaction will induce contelations. The effectivencss may be measured by the ratios of the interaction matrix elements and the separation of the corresponding unperturbed energy levels. Macroscopic systems possess extremely dense energy spectra. The ievel distances, for example, of a rotator with moment of inertia 1 g cm^2 are of the order 10^{-42}eV, which value may be compared with the interaction between two electric dipoles of 1e $\times$ cm at distance R, e^2 $\times$ cm$^2/R^3 \approx 10^{-7}$(cm$/R)^3$eV. It must be concluded that macroscopic systems are always strongly

correlated in their microscopic states. They still do have uncorrelated macroscopic properties, however, if the summations over k_1 and k_2 are each essentially limited to macroscopically equivalent states. [8] Since the interactions between macroscopic systems are effective even at astronomical distances, the only "closed system" is the universe as a whole. The assumption of a closed system $M + S$ is hence unrealistic on a microscopic scale.

The arguments leading to Eq. (3) can be accepted oniy if the states $\dot{\phi}_a$ are interpreted as those of the "remainder of the universe" including the apparatus of measurement, instead of those of the latter alone. It is of course very questionable to describe the universe by a wave function that obeys a Schrödinger equation. Otherwise, however, there is no inconsistency in measurement, as there is no theory. This assumption is referred to as that of "universal validity of quantum theory." It leads-as is demonstrated below-to some unusual consequences, but is able to avoid the discrepancies of quantum theory.

The nonexistence of the microscopic states of macroscopic subsystems of the universe leads to severe difficulties in the interpretation of observation or measurement in terms of information transfer between systems. In particuiar, since no microscopic state of an organism exists, the principle of "psychophysical parallelism" [4] does not apply.

In order to understand Eq. (3), the meaning of superpositions of macroscopically different states has to be investigated. Consider, for the moment, a right-handed sugar molecule with wave function φ_R. This is different from an eigenstate of its Hamiltonian $H_S, \varphi_R \pm \varphi_L$. In contrast to the analogous situation for an ammonia molecule, the tunneling time from φ_R to φ_L is much larger than the age of the universe. The interaction matrix element $\langle \varphi_R | H_S | \psi_L \rangle$ is extremely small, as H_S can at most change the state of two particles. Assume now that an eigenstate $\varphi_R \pm \varphi_L$ had been prepared. The two components would then interact in different ways with their environment,

$$\mathrm{e}^{iHt}\phi\left(\varphi_R \pm \varphi_L\right) \approx \phi^{(R)}(t)\varphi_R \pm \phi^{(L)}(t)\varphi_L \equiv \psi^{(R)}(t) \pm \psi^{(L)}(t) \tag{9}$$

(Destruction of the sugar molecule is neglected, and excitations may be taken into ϕ.) With respect to the parity quantum number, the sugar molecule behaves like a macroscopic object-the energy difference between the eigenstates is extremely small. The two world components $\psi^{(R)}$ and $\psi^{(L)}$ will behave practically independently after they have been prepared, since $\left\langle \psi^{(R)} \right| H \left| \psi^{(L)} \right\rangle$ becomes even smaller with increasing time. There are no transitions between them any more. The "handedness" of the sugar is dynamically stable, whereas one component of the oriented ammonia molecule would emit a photon.

Such a dynamical decoupling of components is even more extreme if φ_R and φ_L represent two states of a pointer corresponding to different positions. Each state will now produce macroscopically correlated states: different images on the retina, different events in the brain, and different reactions of the observer. The different components represent two completely decoupled worlds. This decoupling describes exactly the "reduction of the wave function." As the "other" component cannot be observed any more, it serves only to save the consistency of quantum theory. Omitting this component is justified pragmatically, but leads to the discrepancies discussed above.

I his interpretation, corresponding to a "Iocalization of consciousness" not only in space and time, but also in certain Hilbert-space components, has been suggested by Everett [9] in connection with the quantization of general relativity, and called the "relative state interpretation" of quantum theory. It amounts to a reformulation of the "psychophysical parallclism" which has in any case become necessary as a consequence of the above discussion of dynamical correlations between states of macroscopic systems. [2] A theory of measurement must necessarily be empty if it does not have a substitute for psychophysical paralielism. Everett's relative state interpretation is ambiguous, however, since the dynamical stability conditions [3] are not considered. This ambiguity is present in the orthodox interpretation of quantum theory as well, where

it has always been left to intuition which property of a system is measured "automatically" (e.g., handedness for the sugar, but parity for the ammonia molecule). The dynamical stability appears also to be the cause why microscopic oscillators are observed in energy eigenstates, whereas macroscopic ones occur in "coherent states." [5]

According to the twofold localization of consciousness, there are two kinds of subjectivity: The result of a measurement is subjective in that it depends on the world component of the observer; it is objective in the sense that all observers of this world component observe the same resuit. The question of whether the other components still "exist" after the measurement is as meaningless as asking about the existence of an object while it is not being observed. It is meaningful, however, to ask whether or not the assumption of this existence (i.e., of an objective world) leads to a contradiction.

The probability postulate of quantum theory can be formulated in the following way: Suppose a sequence of equivalent measurements have been performed, each creating an equivalent "branching of the universe." The observer can explain the results by assuming that his final branch has been "chosen randomly" if the components are weighted by their norm. The irreversibility connected with this branching is different from that due to thermodynamical statistics, and thus cannot be explained in terms of the latter. Instead, the effect of branching, i.e., measurement, should be of importance for the foundation of thermodynamics. It seems to be partly taken into account by using the density matrix formalism. [4]

The famous paradox of Einstein, Rosen, and Podolski [12] is solved straightforwardly: A particle of vanishing spin is assumed to decay into two spin $-\frac{1}{2}$ particles. As a consequence, and according to the axiom of measurement, each particle possesses spin projections of equal probability with respect to any direction in space. After measuring the spin of one particle, however, the spin of the other one is determined. According to Einstein et al., this cannot be true if quantum theory is complete, as there is no interaction with the second particle. The interpretation is that the measurement corresponds to the transformation

$$\mathrm{e}^{iHt}\phi\left(\varphi_1^+\varphi_2^{--}-\varphi_1^-\varphi_2^+\right)=\varphi_1^+\varphi_2^-\phi^{(+)}(t)-\varphi_1^{--}\varphi_2^+\phi^{(-)}(t) \tag{10}$$

where $\phi^{(+)}$and $\phi^{(-)}$are dynamically decoupled after a short time. Hence, there is one world component in which the experimentalists observe ${\varphi_1}^+$and ${\varphi_2}^-$, another one in which they observe ${\varphi_1}^-$and ${\varphi_2}^+$. As these components cannot "communicate," the result is in accord with the axiom of measurement.

This interpretation of measurement may also explain certain "superselection rules" [13] which state, for example, that superpositions of states with different charge cannot occur. It is very plausible that any measurement performed with such a system must necessarily also be a measurement of the charge. Superpositions of states with different charge therefore cannot be observed for similar reasons as those valid for superpositions of macroscopically different states: They cannot be dynamically stable because of the significantly different interaction of their components with their environment, in analogy to the different handedness components of a sugar molecule.

If experimental evidence verifies a spontaneous symmetry-breaking of the vacuum as predicted by many field theories [11] this would not prove an asymmetry of the world. One may formally construct invariant wave functions $\Psi=\int d\Omega U_\rho\phi$ from symmetry-violating wave functions ϕ (as done for microscopic systems [15]). The former cannot be distinguished from its

[82] Another suggestion of Wigner's, [10] which postulates an active role of consciousness, would require corrections to the equations of motion.

[3] The importance of stability for organic systems has been emphazised by Elsasser. [11]

[4] This may indeed be the reason why the foundation of quantum-mechanical thermodynamics appears simpler than that of classical thermodynamics. Proofs of the master equation would, however, be circular again if the process of measurement and hence the density matrix formalism were themselves based on thermodynamics.

components $U_\Omega \phi$ if the relative state interpretation is accepted.

It appears that the objective interpretation of quantum theory does not contradict the probability interpretation. It has to be admitted, however, that the "relative state wave function" describes only part of the universe. There is no information on other components except for those which have been created by branching in the past. No estimate can therefore be made on the probability of an inverse branching process, i.e., the spontaneous occurrence of components by accidental overlap.

References

1. E. P. Wigner, Am. J. Phys. 31, 6 (1963); B. d'Espagnat, Nuovo Cimento (Suppl.) 4, 828 (1966); T. Earman and A. Shimony, Nuovo Cimento 54B, 332 (1968); J. M. Jauch, E. P. Wigner, and
M. M. Yanase, Nuovo Cimento 48B, 144 (1967); G. Ludwig, in Werner Heisenberg und die Physik unserer Zeit (Braunschweig, 196i).

2. G. Ludwig, Die Grundlagen der Quantenmechanik (Berlin, 1954), p. 122 ff.; Z. Physik 135, 483
(1953); A. Danieri, A. Loinger, and G. M. Prosperi, Nucl. Phys. 33, 297 (1962); Nuovo Cimento 44B. 119 (1966); L. Rosenfeld, Progr. Theoret. Phys. (Suppl.) p. 222 (1965); W. Weidlich, Z. Physik 205, 199 (1967).

3. J. S. Bell, Rev. Md. Rhys. 38, 447 (1966); D. Bohm and J. Bub, Rev. Mod. Phys. 38, 453 (1966).

4. J. von Neumann, Mathematische Grundlagen der Quantenmechanik (Springer, Berlin, 1932) [English translation: Mathematical Foundations of Quantum Mechanics (Princeton University Press, Princeton, N. J., 1955)].

5. R. J. Glauber, Phys. Rev. 131, 2766 (1963); P. Caruthers and M. M. Nieto, Am. J. Phys. 33, 537 (1965); B. Jancovici and D. Schiff, Nucl. Phys. 58, 678 (1964); C. L. Mehta and E. C. G. Sudarshan, Phys. Rev. 138, B274 (1965).

6. E. Schrödinger, Z. Fiysik 14, 6064 (1920).

7. D. Bohm, Quantum Theory (Prentice-Hall, Englewood Cliffs, N.J., 1951).

8. J. M. Jauch, Helv. Phys. Acta 33, 711 (1960).

9. H. Fverett, Rev. Mod. Phys. 29, 454 (1957): J. A. Wheeler, Rev. Mod. Phys. 29, 463 (1957).

10. E. P. Wigner, in The Scientist Speculates, L. J. Good, ed. (Heinemann, London, 1962), p. 284.

11. W. M. Elsasscr, The Physical Foundation of Biology (Pergamon Press, New York and Iondon, 1958).

12. A. Einstein, N. Rosen, and B. Podolski, Phys. Rev. 47, 777 (1935): D. Bohm and Y. Aharonov, Phys. Rev. 108, 1070 (1957).

13. G. C. Wick, A. S. Wightman, and E. P. Wigner, Phys. Rev. 88, 101 (1952); E. P. Wigner and M. M. Yanase, Proc. Natl. Acad. Sci. (US) 49, 910 (1963).

14. W. Heisenberg, Rev. Mod. Phys. 29, 269 (1957); Y. Nambu and G. Jona-Lasinio, Phys. Rev. 122, 345 (1961).

15. H. D. Zeh, Z. Physik 202, 38 (1967).

26 III "Hidden Variables" versus "Phenomenon" and Complementarity

26.1 III.1 Polyelectrons

26.1.1 Summary

Theoretical evidence for the existence of entities composed entirely of electrons and positions is presented in the following article, together with a discussion of their properties. [1] The simplest of these entities consists of one electron and one positron, bound together in a structure similar to that of the hydrogen atom. The next higher entity is composed of two positrons and one electron or of two electrons and one positron. The bi-electron system is stable by 6.77 ev against dissociation. Against annihilation, it has a life time of 1.24×10^{-10}sec., when the spins of the two particles are parallel, and a life several orders of magnitude greater, when the spins are antiparallel. The tri-electron system also has a radioactive mean life of the order of 10^{10} sec., and is calculated to be stable by at least 0.19 ev against dissociation into a bi-electron and a free electron or positron. The production of a bielectron, by interaction of an energetic gamma ray with the field of force of an atomic nucleus, is calculated to occur with a probability about 10^{-6} times less than that for production of an electron-positron pair. The possibilities are discussed for observing atomic and molecular spectra in which the positron plays the role of an especially light hydrogen ion. An experiment is suggested which can be used to check the theory of the perpendicular polarization of the gamma rays given off in the annihilation process. The similarities and distinct differences between polyelectrons and cosmic ray mesons are discussed.

26.1.2 Possibility Of Testing Some of the Present Predictions of Pair Theory

Quite apart from the possibly questionable direct bearing of polyelectrons upon cosmic ray phenomena, it is natural to ask if there are any experimental implications which may be examined in the laboratory as new tests of the validity of pair theory itself.

One of the most interesting possibilities for a test is suggested by the existence of excited energy levels in the polyelectron, P^{+-}. Radiative trausition of the system between these energy levels generates an optical
spectrum which differs from that of hydrogen, in iis major features, only through the displacement of all lines to the red by a displacement factor of two. To observe any well-defined spectrum of such a character would, of course, appear to cali, in the first piace, for a gaseous emitter. In addition, the securing of slow polyelectrons requires that a slow positron should be able easily to detach an electron from an atom of the gas. This condition requires that the first ionization potential of the substance of the gas should be close to 6.7 volts. Finally, the means of observation must be capable of picking up over the background spectral lines which have been considerably broadened by the Doppler effect, inevitable in systems which have only twice the electronic mass and which are in thermal equilibrium near room temperature.

The difficulties about Doppler effect and choice of substance with suitable ionization potential are considerably alleviated by renouncing, in the beginning, the study of the particular

entity, P^{+-}, and looking at the problem of the test of pair theory in a broader light. The essential point is to find an atomic or molecular system which contains a positron and which possesses several optically combining energy levels. In looking for such a system, it is only necessary to remember that the positron may be regarded as a superlight isotope of the highly reactive hydrogen ion. Consequently, one can look among such compounds as $e^+Cl^-$for systems which may possess the desired type of energy levels and which will be free of objectionable Doppler cffect, on account of their substantial mass.

The actual experiment would consist in irradiation of a suitable gas with slow positrons, the radiative capture of some of these positrons into excited states of entities having somewhat the character of molecules, the transition of these entities to lower levels with the emission of characteristic spectral lines lying in, or near, the visible region, the observation of this spectrum, and the annihilation of each positron by an electron of the corresponding molecule-like entity. The gamma rays given off in this experiment would be of no direct concento the problem at issue. The test of the pair theory would come in the comparison of the observed and calculated positions of the spectral lines. Obviously, the experiment, though interesting, is difficuli.

A second and somewhat simpler experiment would seem to offer a means to check on one of the details of the annihilation process itself. We have already remarked that by far the dominating type of anniliitation is that in which the positron combines with an electron whose spin forms a singlet state with respect to the spin of the positron. Associated with this selection of pairs which have zero relative angular monentum, before the annihilation process, is an analogous polarization phenomenon in the two quanta which are left at the end of the process. According to the pair theory, if one of these photons is linearly polarized in one plane, then the photon which goes off in the opposite direction with equal momentum is linearly polarized in the perpendicular plane.

To test this prediction, the following experimental arrangement suggests itself: A radioactive source of slow positrons is covered with a foil thick enough to guarantee annihilation of all the positrons. A sphere of lead centered on this source prevents the escape of any of the annihilation quanta, except through a relatively narrow hole drilled through the sphere along one of its diameters. When a photon of energy mc^2 comes out of one end of this channel, we expect a photon also of eneigy mc^2 to emerge simultaneously from the other end. At each end, a carbon scatterer is placed. Photons scattered by one of these blocks through approximately ninety degrees and into the proper azimuih pass ilirough a gamma ray counter. The scattering process gives a preference to the recording of photons with a selected polarization. A similar arrangement applies at the other end of the channel. The relative azimuth of the two counters may be varied at will. Coincidences between the two counters are recorded, (a) when the azimuths of the two counters are identical, (b) when the azimuths differ by a right angle. The observed ratio of (b) to (a) is compared with the computed ratio, as a check on the theory of the annihilation process. The calculated ratio for the case of ideal geometry is 1.080 , when the arrangement requires the photons to be scattered through 90°. The theoretically most favorable ratio of 1.100 is obtained when the scattering angle is reduced to 74°30′.
[To be corrected to 2.60 at 90° and maximum of 2.85 at 82° : Pryce and Ward (1947), Snyder, Pasternack, and Hornbostel (1948)-Eds.]

Another possible means of studying this scattering is to use the knockon electrons, instead of the recoil photons. The polarization is, obviously, as complete for the particles as for the radiation. In case this arrangement is employed, the detecting counters are set to catch electrons knocked on at an angle of about 30°, with respect to the annihilation radiation. The efficiency of counting is increased by this alteration in the plan of the experiment.

Evidently, it is possible, by means of a reasonable experimental procedure, to obtain information bearing most closely upon the problem of the intimate interaction of an electron and a positron.

References AND NOTES

1. On October S. four days after the present paper was submitted to the New York Indemy of Sciences, the anthor learned from Professor Arthur Ruark that he had previously envisiged the existence of the particular entity composed of one electron and one positron. and he respical Review in the form when he ther the diitor " a reference io unpublixivi woth by L. Landau of a detter to the Editor. A reference io unpulisited work **L**. Landau Asetiani. 1916. J. Phyr. U.S.S.IR. 9:56.

26.2 III.2 Paradox of Einstein, Rose, and Podolsky by Bohm

15. The Paradox of Einstein, Rosen, and Podolsky. In an article in the Physical Review, † Einstein, Rosen, and Podolsky raise a serious criticism of the validity of the generally accepted interpretation of quantum theory. This objection is raised in the form of a paradox to which they are led on the basis of their analysis of a certain hypothetical experiment, which we shall discuss in detail later. Their criticism has, in fact, been shown to be unjustified, ‡ and based on assumptions concerning the nature of matter which implicitly contradict the quantum theory at the outset. Nevertheless, these implicit assumptions seem, at first sight, so natural and inevitable that a careful siudy of the points which the authors raised affords deep and penetrating insight into the difference between classical and quantum concepts of the nature of matter.

The authors first undertook to define criteria for a complete physical

Originally published as sections 15-19, Chapter 22 of Quantum Theory, David Bohm, pp. 611-23, Prenticc-IIali, Englewood Cliffs (1951).

theory. It seemed to them that a necessary requirement for a complete physical theory was the following:

(1) Every element of physical reality must have a counterpart in a complete physical theory.

As to what actually constituted the correct elements in terms of which physical theory should be expressed, they felt that this question can be decided finally only by recourse to experiments and observations. They nevertheless suggested the following criterion for recognizing an element of reality, which seemed io them a sufucient criterion:

(2) If, without in any way disturbing the system, we can predict with certainty (i.e., with probability equal to unity) the value of a physical quantity, then there exists an element of reality contesponding to this physical quantity.

The authors agreed that elements of physical reality might well be recognized in other ways also, but they intended to show that even if one restricted oneself to elements that could be recognized by means of this criterion alone, quantum theory as now interpreted led to contradictory results.

The use of the above explicit criteria rests, however, on certain implicit assumptions, which are an integral part of the treatment given by the authors, but which are never explicitly stated. These assumptions are:

(3) The world can correctly be analyzed in terms of distinct and separately existing "elements of reality,"

(4) Every one of these elements must be a counterpart of a precisely defined mathematical quantity appearing in a complete theory.*

We shall temporarily accept the above criteria and assumptions, in order to permit the further development of the arguments given by the authors, but in Sec. 18 we shall show that these criteria should not be applied at the quantum level of accuracy.

[8] † Phys. Rev., 47, 777 (1935).

‡ N. Bohr, Phys. Rev. 48, 696 (1935); W. H. Furry, Phys. Rev. 49, 393, 476 (1936).

Now, let us recall that in the present quantum theory, one assumes that all relevant physical information about a system is contained in its wave function, so that when two systems have wave functions which differ by at most a constant phase factor, they are said to be in the same quantum state † What the authors wished to do with their criteria for reality was to show that the above interpretation of the present quantum theory is untenable and that the wave function cannot possibiy contail a complete description of all physically significant factors (or "elements of reality") existing within a system. If their contention could be proved, then one would be led to search for a more complete theory

This criterion is essentially a strengthened form of (1). Einstein, Rosen, anc Podelely do not restrict themselves to the assumption (1), that every element o reality always has a counterpart in a complete theory, but they also assume implicitly that this counterpart must always be precisely definable.

† *See Chap. 9, Sec. 4. .*

perhaps containing something like hidden variables, in terms of which the present quantum theory would be a limiting case.

Let us now consider an arbitrary observable A having a sei of eigenfunctions, ψ_a, belonging to a series of eigenvalues which are denoted by a. When the wave function is ψ_a, then the system is said to be in a quantum state in which the observable A has the definite value a. In this situation, ERP would say that there is in the system an element of reality corresponding to the observable, A. But now let us consider another observable $\bar{B}$ which does not commute with A, so that there exists no wave function for which A and B have simultaneously definite values. Now if we adopt the implicit assumption (4) that every element of reality must be a counterpart of a precisely defined mathematical quantity appearing in a complete theory, then the usual assumption that the wave function provides a complete description of reality leads to the conclusion that A and B cannot exist simultaneously. † This follows from the fact that the supposedly complete wave theory contains no precisely defined mathematical elements corresponding to the simultaneous existence of A and B. From this point of view, we must also assume, however, that when B is measured and obtains a definite value, the elements corresponding to A are destroyed (since we have assumed that they cannot exist together with those corresponding to B). It seems natural to suppose that this destruction is brought about by the quanta that are transferred from the measuring apparatus to the system under observation. It is clear, however, that in such an interpretation of the noncommutativity of two observables, it is essential that in every measurement there shall actually be a disturbance arising from the apparatus that destroys all elements of reality corresponding to observables that do not commute with the measured variable. For if there were no such disturbance, then one could take a system initially having a definite value of A and then measure B without in any way altering the elements corresponding to A, thus obtaining a system in which the elements of reality corresponding to A and B exist together at the same time. Now, in the next section, we shall discuss a type of hypothetical experiment suggested by ERP that actually permits us io measure a given observable without in any way disturbing the associated system. With the aid of this type of hypothetical experiment, they are then able to obtain a contradiction between the assumption that the quantum theory provides a complete description of reality and the assumption that their criteria for reality must necessarily apply in any complete theory. If one accepts their

- Chap. 2, Sec. 5; Chap. 5, Sec. 3.
  † in Sec. ir, we shall make the aiternative assumption that eiements of reality exist in a roughly defined form and do not necessarily have to be counterparts of precisely defined mathematical quantities appearing in a compiete theory. Thus, we shall give up the implicit assumptions (3) and (4).
  criteria, one is left, with a single remaining alternative, viz., that quantum theory does

not provide a complete description of reality. This is the conclusion that they originally set out to obtain.

16. The Hypothetical Experiment of Einstein, Rosen, and Podolsky. We shall now describe the hypothetical experiment of Einstein, Rosen, and Podolsky. We have modified the experiment somewhat, but the form is conceptually equivalent to that suggested by them, and considerably easier to treat mathematically.

Suppose that we have a molecule containing two atoms in a state in which the total spin is zero and that the spin of each atom is $\hbar/2$. Roughly speaking, this means that the spin of each particle points in a direction exactly opposite to that of the other, insofar as the spin may be said to have any definite direction at all. Now suppose that the molecule is disintegrated by some process that does not change the total angular momentum. The two atoms will begin to separate and will soon cease to interact appreciably. Their combined spin angular momentum, however, remains equal to zero, because by hypothesis, no torques have acted on the system.

Now, if the spin were a classical angular momentum variable, the interpretation of this process would be as follows: While the two atoms were together in the form of a molecule, each component of the angular momentum of each atom would have a definite value that was always opposite to that of the other, thus making the total angular momentum equal to zero. When the atoms separated, each atom would continue to have every component of its spin angular momentum opposite to that of the other. The two spin-angular-momentum vectors would therefore be correlated. These correlations were originally produced when the atoms interacted in such a way as to form a molecule of zero total spin, but after the atoms separate, the correlations are maintained by the deterministic equations of motion of each spin vector separately, which bring about conservation of each component of the separate spin-angularmomentum vectors.

Suppose now that one measures the spin angular momentum of any one of the particles, say No. 1. Because of the existence of correlations, one can immediately conclude that the angular-momentum vector of the other particle (No. 2) is equal and opposite to that of No. 1. In this way, one can measure the angular momentum of particle No. 2 indirectly by measuring the corresponding vector of particle No. 1.

Let us now consider how this experiment is to be described in the quantum theory. Here, the investigator can measure cither the x, y, or z component of the spin of particle No. 1, but not more than one of these components, in any one experiment. Nevertheless, it still turns out as We shall see that whichever component is measured, the results are correlated, so that if the same component of the spin of atom No. 2 is
measured, it will always turn out to have the opposite value. This means that a measurement of any component of the spin of atom No. 1 provides, as in classical theory, an indirect measurement of the same component of the spin of atom No. 2. Since, by hypothesis, the two particles no longer interact, we have obtained a way of measuring an arbitrary component of the spin of particle No. 2 without in any way disturbing that particle. If we accept the definition of an element of reality (2) suggested by ERP, it is clear that after we have measured σ_z for particle 1 , then σ_z for particle 2 must be regarded as an element of reality; existing separately in particle No. 2 alone. If this is true, however, this element of reality must have existed in particle No. 2 even before the measurement of σ_z for particle No. 1 took place. For since there is no interaction with particle No. 2, the process of measurement cannot have affected this particle in any way. But now let us remember that, in each case, the observer is always free to reorient the apparatus in an arbitrary direction while the atoms are still in flight, and thus to obtain a definite (but unpredictable) value of the spin component in any direction that he chooses. Since this can be accomplished without in any way disturbing the second atom, we conclude that if criterion (2) of ERP is applicable, precisely defined elements of reality must

exist in the second atom, corresponding to the simultaneous definition of all three components of its spin. Because the wave function can specify, at most, only one of these components at a time with complete precision, we are then led to the conclusion that the wave function does not provide a complete description of all elements of reality existing in the second atom.

If this conclusion were valid, then we should have to look for a new theory in terms of which a more nearly complete description was possible. We shall see, however, in Sec. 18, that the analysis given by ERP involves in an integral way the implicit assumptions (3) and (4) that the world is actually made up of separately existing and precisely defined "elements of reality." Quantum theory, however, implies a quite different picture of the structure of the world at the microsconic level. This picture leads, as we shall see, to a perfectly rational interpretation of the hypothetical experiment of ERP within the present framework of the theory.

17. Mathematical Analysis of Experiment According to Quantum Theory. Before discussing the physical interpretation that the present quantum theory gives to the hypothetical experiment of Einstein, Rosen and Podnlsky, we shall first show how this experiment is to be described in mathematical terms.

The system containing the spin of two atoms has four basic wave functions, from which an arbitrary wave function can be constructed.*

- The complete wave function for the system is then obtained by multiplying the spin wave functions by appropriate space wave functions, which depend on the space eo-ordinates of both particles.

These are

$$\psi_a = u_+(1)u_+(2) \quad \psi_c = u_+(1)u_-(2)$$
$$\psi_b = u_-(1)u_-(2) \quad \psi_d = u_-(1)u_+(2)$$

where $u_+$and $u_-$are the one-particle spin wave functions representing, respectively, a spin $k/2$ and $k/2$, and the argument (1) or (2) refers, respectively, to the particle which has this spin. Now ψ_c and ψ_d represent the two possible situations in which each particle has a definite z component of the spin in a direction which is opposite to that of the other. The wave function for a system of total spin zero is the following linear combination of ψ_c and ψ_d (see Chap. 17, Sec. 9):

$$\psi_0 = \frac{1}{\sqrt{2}}(\psi_c - \psi_d) \tag{26}$$

The particular sign with which ψ_c and ψ_d are combined is of crucial importance in determining the combined spin, for if they are combined with a + sign, one obtains an angular momentum of $\hbar$ (but with a zero value of the z component of the angular momentum). We denote this result below:

$$\psi_1 = \frac{1}{\sqrt{2}}(\psi_c + \psi_d) \tag{27}$$

It is clear, then, that the total angular momentum is an interference property of ψ_c and ψ_d. On the other hand, the only states in which each particle has a definite spin opposite to that of the other are represented either by ψ_c or by ψ_d separately. Thus, in any state in which the value of σ_z for each particle is definite, the total angular momentum must be indefinite. Vice versa, whenever the total angular momentum is definite, then neither atom can correctly be regarded as having a definite value of its own spin, for if it did, there could be no interference between ψ_c and ψ_d, and it is just this interference which is required to produce a definite total angular momentum.

Besides leading to a definite value of the combined spin, however, definite phase relations between $\dot{\psi}_c$ and $\dot{\psi}_d$ have additional physical meaning, for they also imply that if the same component of the spin of each atom is measured, the results will be correlated. Such correlations can be demonstrated, for example, in a process in which the z component of the spin of each atom is measured by allowing each atom to pass through a separate Stern-Gerlach apparatus (see Fig. 1). For the sake of simplicity, we can suppose that boil spins are measured at the same time, although no results will depend significantly on this assumption. The Hamiltonian at the time of measurement is then [see eqs. (10a) and (10b)]:

$$W = \mu\left(\mathfrak{H}_0 + z\mathfrak{H}_0'\right)\sigma_{1,z} + \mu\left(\mathfrak{H}_0 + z_2\mathfrak{H}_0'\right)\sigma_{2,*}$$

where z_1 is the z co-ordinate of the first atom and z_2 is the z co-ordinate of the second atom. (We assume that both pieces of apparatus are identical in construction.)

We now expand the spin wave function during the course of the measurement in terms of the four basic functions, ψ_a, ψ_b, ψ_c, and ψ_d. Since this measurement does not change σ_z, it will remain true that only ψ_c and *a are needed during the course of the measurement.* Thus, we write

$$\frac{\psi}{\tau} = f_{ci}\psi_u + f_{a\tau_u}$$

In our case, the initial value of f_c is $1/\sqrt{2}$, and the intial value of f_d is $-1/\sqrt{2}$. By methods similar to those leading to equation (13b), one derives

$$i\hbar\frac{\partial f_c}{\partial t} = \mu f_c\left[\left(\mathfrak{K}_0 + \mathfrak{K}_0' z_1\right) - \left(\mathfrak{K}_0 + \mathfrak{K}_0' z_2\right)\right]$$
$$i\hbar\frac{\partial f_d}{\partial t} = -\mu f_d\left[\left(\mathfrak{K}_0 + \mathfrak{K}_0' z_1\right) - \left(\mathfrak{K}_0 + \mathfrak{K}_0' z_2\right)\right]$$

The solution for f_c and f_d with the proper boundary conditions yields for the wave function just after the particles leave the magnetic field

$$f_c = \frac{1}{\sqrt{2}}e^{-\frac{\mu\mathcal{K}_0'}{\hbar}(z_1-z_2)\Delta t} \quad f_d = -\frac{1}{\sqrt{2}}e^{\frac{\mu\mathcal{H}_0}{\hbar}(z_1-z_2)\Delta t}$$

where we have inserted $t = \Delta t =$ time of interaction between atoms and the inhomogeneous magnetic field.

This wave function implies that the two results represented, respectively, by ψ_c and by ψ_d are equally probable. In the first possible result, atom No. 1 has a positive value of σ_z, while atom number 2 has a negative value. The factor $e^{-i\mu\mathcal{H}\mathcal{C}_0'\Delta t(z_1-z_2)/\hbar}$ represents the fact that in the SternGerlach experiment, each atom obtains an opposite momentum corresponding to its opposite spin. Similarly, in the second possible result, atom No. 2 has a negative value of σ_2, whereas atom No. 1 has a positive vaiue. As in Secs. 9 and 11, we can show that because the apparatus is classically describable, the apparatus wave functions (which depend on z_1 and z_2), multiply the spin wave function by uncontrollable phase factors, so that we finally obtain

$$\psi = \frac{1}{\sqrt{2}}\left(\psi_0 e^{i\alpha_0} + \psi_d e^{i\alpha_d}\right)$$

where α_c and α_d are separate and uncontroliable phase factors.
This result shows that if the value of σ_z is measured for each atom, the result will come out a definite number for each, which is always

8

- Note that these are the only terms present initially.

opposite to that of the other. In this way, we prove that correlations resembling those of classical theory will also be obtained in the quantum theory. After the measurement is over, however, the system has been transformed from one that had a definite combined angular momentum and an indefinite value of σ_z for each particle to one which has a definite value of σ_z for each particle, but an indefinite combined angular momenturu. Moreover, the precise value of σ_z which will be obtained for each particle is not related deterministically to the state of the system before the measurement, but only statistically.

Let us now describe the process of measurement of σ_x. The results are very similar, because the wave function for a system of zero total spin is the same when expressed in terms of v_+, v_-(the eigenfunctions of σ_x) as in terms of u_+, u_-. Thus, we obtain

$$\psi_0 = \frac{1}{\sqrt{2}} \left[v_+(1) v_-(2) - v_-(1) v_+(2) \right]$$

One can now describe the measurement of σ_x for each particle in exactly the same way as was done with σ_z, and after the interaction with the measuring apparatus, one obtains

$$\psi = \frac{1}{\sqrt{2}} \left[v_+(1) v_-(2) e^{i\alpha_1} + v_-(1) v_+(2) e^{i\alpha_2} \right]$$

where α_1 and α_2 are separate uncontrollable phase factors.
We conclude that the value of σ_x for each particle is also correlated to that of the other in such a way that the sum of the two is zero. Moreover, it is readily verified that if one had taken the function

$$\psi_1 = \frac{1}{\sqrt{2}} \left(\psi_a + \psi_b \right)$$

then with the substitution, $v_+ = \frac{1}{\sqrt{2}} (u_+ + u_-)$and $v_- = \frac{1}{\sqrt{2}} (u_+ - u_-)$, one would have the wave function

$$\psi_1 = \frac{1}{\sqrt{2}} \left[v_+(1) v_+(2) + v_-(1) v_-(2) \right]$$

This represents a situation in which measurement of σ_x will disclose that both particles have a positive value together, or that both particles have a negative value together. We see therefore that the type of correiation of σ_x which can develop depends on the sign with which $\dot{\psi}_c$ and $\dot{\psi}_d$ are added, and therefore also on the combined angular momentum.

One more significant point arises in connection with this experiment; namely, that the existence of correlations does not inply that the hela vior of either atom is affected in any way at all by what happens to the other,
after the two have ceased to interact. To prove this statement, we first evaluate the mean value of any function $g(d_2)$ of the spin variables of particle No. 2 alone. With the wave function before a measurement took place, we obtain

$$\bar{g}_0 (\boldsymbol{d}_2) = \frac{1}{2} \left(\psi_c^* - \psi_d^* \right) \dot{g} (\boldsymbol{d}_2) \left(\psi_c - \psi_d \right) = \frac{1}{2} \left[\psi_c^* g (\boldsymbol{d}_2) \psi_c + \psi_d^* g (\boldsymbol{d}_2) \psi_d \right]$$

(By virtue of the orthogonality of ψ_c and $g (\boldsymbol{\delta}_2) \psi_d$.) After the spin of the first particle is measured, the average of $g (\mathbf{o}_2)$ becomes
$\bar{g}_f (\boldsymbol{d}_2) = \frac{1}{2} \left(\psi_c^* e^{-i\alpha_c} - \psi_d^* e^{-i\alpha_d} \right) g (\boldsymbol{d}_2) \left(\psi_c e^{i\alpha_c} - \psi_d e^{i\alpha_d} \right)$

$$= \frac{1}{2} \left[\psi_c^* \tilde{y} (\mathcal{J}_2) \psi_c + \psi_d^* \tilde{y} \left(\tilde{J}_2 \right) \psi_d \right]$$

This is the same as what was obtained without a measurement of the spin variables of particle No. 1. The behavior of the two spins is, however, correlated despite the fact that each

behaves in a way that does not depend on what actually happens to the other after interaction has ceased.

18. Physical Description of Origin of Correlations. We have deduced mathematically that in a system of two atoms having a total spin of zero, the spin components of each atom in an arbitrary direction will be correlated, despite the fact that according to our present interpretation of quantum theory these spin components cannot all exist simultaneously in precisely defined forms. We wish to show now that the paradoxical results obtained by ERP in the interpretation of this fact will not be obtained if one avoids making their implicit assumptions (3) and (4); viz., that the world can correctly be analyzed into elements of reality, each of which is a counterpart of a precisely defined mathematical quantity appearing in a complete theory. These assumptions, which are at the root of all classical theory, might perhaps be called the hypothesis that reality is built upon a mathematical plan, for it is required that every element appearing in the real world shall correspond precisely to some term appearing in a complete set of mathematical equations. Although such a hypothesis seems quite natural to us at this time, it is by no means inescapable. † In fact, in quantum theory, one makes a quite different, but equally plausible, hypothesis concerning the funda= mental nature of matter. Here, we assume that the one-to-one correspondence between mathematical theory and well-defined "elements of reality" exists only at the classical level of accuracy. For at the quantum level, the mathematical description provided by the wave function is certainly not in a one-tu-one correspondence with the actual behavior of

† Historically speaking, it is a comparatively new idea, having arisen in connection with the great sucees of mathomatical analysis in mechanics and electrodynamics during the period between the sixteenth and early twentieth centuries (see Chap. 8, Seces. 2 to 10).

the system under description, but only in a statistical correspondence.* Yet, we assert that the wave function (in principle) can provide the most complete possible description of the system that is consistent with the actual siructure of matter. How can we reconcile these two aspects of the wave function? We do so in terms of the assumption that the properties of a given system exist, in general, only in an imprecisely defined form, and that on a more accurate level, they are not really wolldefined properties at all, but instead only potentialities, † which are more definitely realized in interaction with an appropriate classical system, such as a measuring apparatus. For example, consider two noncommuting observables, such as momentum and position of an electron. We say that, in general, neither exists in a given system in a precisely defined form, but that both exist together in a roughly defined form, such that the uncertainty principle is not violated. ‡ Either variable is potentially capable of becoming better defined at the expense of the degree of definition of the other, in interaction with a suitable measuring apparatus. We see then that the properties of position and momentum are not only incompletely defined and opposing potentialities, but also that in a very accurate description, they cannot be regarded as belonging to the electron alone; for the realization of these potentialities depends just as much on the systems with which it interacts as on the electron itself.§ This means that there are actually no precisely defined "elements of reality" belonging to the electron. Thus, we contradict the assumptions (3) and (4) of Einstein, Rosen, and Podolsky.

Quantum-mechanical spin variables must be interpreted in a similar way. Whereas ERP would say that the only existing component of the spin is the one which may happen to be defined precisely by the wave function, we say that, in general, all three components exist simultaneously in roughly defined forms, and that any one component has the potentiality for becoming better defined at the expense of the others if the associated atom interacts with a suitable measuring apparaius. The probability for the development of a definite value of any spin component in a suitable process of measurement is proportional to the square of the amplitude of the coefficient of the part of the wave function corresponding to this component. We must, however, recall that the complete spin wave function for a given atom can be expanded in terms

of the eigenfunctions, $u_+$and u_-, of the spin variables in any direction. Thus $\psi = a_+u_+ + a_-u_-$In such an expansion, the phase relations between $u_+$and u_-help determine the distribution over spin components in other directions. ‖ (Thus, if u_+, u_-represent eigenfunctions of σ_z, then

- See Chap 6, Sere 4.
  † See Chap. 6, Secs. 9 and 13, Chap. 8, Secs. 14 and 15, Chap. 22, Sec. 13.
  ‡ See discussion of complementarity in Chap. 8. Sec. 15.
  § Chap. 6, Sec. 13, Chap. 8, Sec. 16.
  || See Chap. 17, Secs. 6 and 7.
  an cigenfunction of $\bar{u}_x$ is obtained when $\psi - \frac{1}{\sqrt{2}}(\bar{u}_+ \pm u_-)$.)This means that as iong as definite phase relations exist between $u_+$and u_-, one cannot categorize (or classify) the system as having a spin which corresponds either entirely to u_+or entirely to u_-, with respective probabiiities,* $|a_+|^2$ and $|a_-|^2$. Instead, we must say that the system cuts across this method of classification, and in some sense, covers both states at once in a poorly defined way. † Thus, we must give up the classical picture of a precisely defined spin variable associated with each atom, and replace it by our quantum concept of a potentiality, the probability of whose development is given by the wave function. It is only when the wave function is an eigenfunction of a given spin component that the system is certain (in interaction with a suitable apparatus) to develop a predictable value of that spin component.

Now, when we come to our system of two atoms having a total spin of zero, we see from eq. (26) that because the wave function

$$\psi_0 = \frac{1}{\sqrt{2}}(\psi_c - \psi_d)$$

has definite phase relations between ψ_c and ψ_d, the system must cover the states corresponding to ψ_c and ψ_d simultaneously. Thus, for a given atom, no component of the spin of a given variable exists with a precisely defined value, until interaction with a suitable system, such as a measur.ing apparatus, has taken place. But as soon as either atom (say, No. 1) interacts with an apparatus measuring a given component of the spin, definite phase relations between ψ_c and ψ_d are destroyed. This means that the system then acts as if it is either in the state ψ_c or ψ_d. Thus, in every instance in which particle No. 1 develops a definite spin component, in, for example, the z direction, the wave function of particle No. 2 will automatically take such a form that it guarantees the development of the opposite value of σ_z if this particle aiso interacts with an apparatus which measures the same component of the spin. The wave function therefore describes the propagation of correlated potentialities. Because the expansion of the wave function ψ_0 takes the same form when expanded in terms of the eigenfunctions of an arbitrary component of the spin, we conclude that similar correlations will be obtained if the same component of the spin of each atom in any direction is measured. Moreover, because the potentialities for development of a definite spin component are not realized irrevocably until interaction with the apparatus actually takes place, there is no inconsistency in the statement that while the atoms are still in flight, one can rotate the apparatus into an arbitrary

* Chan 6, See. 4, Chap. 22, Sec. 10.
† Chap. 16, Sec. 25, and Chap. 8, Sec. 15.

direction, and thus choose to develop definite and correlated values for any desired spin component of each atom.

Finally, it is perhaps interesting to consider in a new light the fact that the mathematical description provided by the wave function is not in a one-to-one correspondence with the actual behavior of matter. From this fact, we are led to conclude that, contrary to general opinion,

quantum theory is less mathematical in its philosophical basis than is classical theory, for, as we have seen, it does not assume that the world is constructed according to a precisely defined mathematical plan. Instead, we have come to the point of view that the wave function is an abstraction, providing a mathematical reflection of certain aspects of reality, but not a one-to-one mapping. To obtain a description of all aspects of the world, one must, in fact, supplement the mathematical description with a physical interpretation in terms of incompletely defined potentialities.* Moreover, the present form of quantum theory implies that the world cannot be put into a one-to-one correspondence with any conceivable kind of precisely defined mathematical quantities, and that a complete theory will always require concepts that are more general than that of analysis into precisely defined elements. We may probably expect that even the more general types of concepts provided by the present quantum theory will also ultimately be found to provide only a partial reflection of the infinitely complex and subtle structure of the world. As science develops, we may therefore look forward to the appearance of still newer concepts, which are only faintly foreshadowed at present, but there is no strong reason to suppose that these new concepts are likely to lead to a return to the comparatively simple idea of a one-to-one correspondence between the real world and precisely defined mathematical abstractions.

19. Proof that Quantum Theory Is Inconsistent with Hidden Variables. We can now use some of the results of the analysis of the paradox of Einstein, Rosen, and Podolsky to help prove that quantum theory is inconsistent with the assumption of hidden causal variables. (See Chap. 2, Sec. 5 and Chap. 5, Sec. 3.) We first note that the assumption that there are separately existing and precisely defined elements of reality would be at the base of any precise causal description in terms of hidden variables; for without such elements there would be nothing to which a precise causal description could apply. Similarly, as we saw in Chap. 8, Sec. 20, the existence of separate elements requires a precise causal theory of the relationships between these elements for its consistent application. Thus, the analysis of the world into pre-

- See Chap. 23 for a fuller discussion of how the wave function must be supplemented with its interpretation in ierms of potentialities for the production of various classically describable results.

26.3 III.3 A Suggested Interpretation of the Quantum Theory in Terms of "Hidden" Variables, I

The usual interpretation of the quantum theory is self-consistent, but it involves an assumption that cannot be tested experimentally, viz., that the most complete possible specification of an individual system is in terms of a wave function that determines only probable results of actual measurement processes. The only way of investigating the truth of this assumption is by trying to find some other interpretation of the quantum theory in terms of at present "hidden" variables, which in principle deter mine the precise behavior of an individual system, but which are in practice averaged over in measurements of the types that can now be carried out. In this paper and in a subsequent paper, an interpretation of the quantum theory in terms of just such "hidden" variables is suggested. It is shown that as long as the mathematical theory retains its present general form, this suggested interpretation leads to precisely the same results for all physical processes as does the usual interpretation. Nevertheless, the suggested interpretation provides a broader conceptual framework than the usual interpretation, because it makes possible a precise and continuous description of all processes, even at the quantum level. This broader conceptual framework allows more general mathematical formulations of the theory than those allowed by the usual interpretation. Now, the usual mathematical formulation seems to lead to insoluble difficulties when it is extrapolated into the domain of distances of

the order of 10^{-13} cm or less. It is therefore entirely possible that the interpretation suggested here may be needed for the resolution of these difficulties. In any casc, the mere possibility of such an interpretation proves that it is not necessary for us to give up a precise, rational, and objective description of individual systems at a quantum level of accuracy.

26.3.1 1. Introduction

The usual interpretation of the quantum theory is based on an assumption having very far-reaching implications, viz., that the physical state of an individual system is completely specified by a wave function that determines only the probabilities of actual results that can be obtained in a statistical ensemble of similar experiments. This assumption has been the object of severe criticisms, notably on the part of Einstein, who has always believed that, even at the quantum level, there must exist precisely definable elements or dynamical variables determining (as in classical physics) the actual behavior of each individual system, and not merely its probable behavior. Since these elements or variables are not now included in the quantum theory and have not yet been detected experimentally, Einstein has always regarded the present form of the quantum theory as incomplete, although he admits its internal consistency. [1–5]

Most physicists have felt that objections such as those raised by Einstein are not relevant, first, because the present form of the quantum theory with its usual probability interpretation is in excellent agreement with an extremely wide range of experiments, at least in the domain of distances [6] larger than 10^{-13} cm, and, secondly, because no consistent alternative interpretations have as yet been suggested. The purpose of this paper (and of a subsequent paper hereafter denoted by II) is, however, to suggest just such an alternative interpretation. In contrast to the usual interpretation, this alternative interpretation permits us to conceive of each individual system as being in a precisely definable state, whose changes with time are determined by definite laws, analogous to (but not identical with) the classical equations of motion. Quantum-mechanical probabilities are regarded (like their counterparts in classical statistical mechanics) as only a practical necessity and not as a manifestation of an inherent lack of complete determination in the properties of matter at the quantum level. As long as the present general form of Schroedinger's equation is retained, the physical results obtained with our suggested alternative interpretation are precisely the same as those obtained with the usual interpretation. We shall see, however, that our alternative interpretation permits modifications of the mathematical formulation which could not even be described in terms of the usual interpretation. Moreover, the modifications can quite easily be formulated in such a way that their effects are insignificant in the atomic domain, where the present quantum theory is in such good agreement with experiment, but of crucial importance in the domain of dimensions of the order of 10^{-13} cm, where, as we have seen, the present theory is totally inadequate. It is thus entirely possible that some of the modifications describable in terms of our suggested alternative interpretation, but

---

[8]

- Now at Universidade de So Paulo, Faculdade de Filosofia, Ciencias, e Letras, So Paulo, Brasil.

[1] Einstein, Podolsky, and Rosen, Phys. Rev. 47, 777 (1933).

[2] D. Bohm, Quantum Theory (Prentice-Hall, Inc., New York, 1951), see p. 611.

[3] N. Bohr, Phys. Rev. 48, 696 (1935).

[4] W. Furry, Phys. Rev. 49, 393, 476 (1936).

[5] Paul Arthur Schiln, editor, Albert Einstein, PhilosopherScientist (Library of Living Philosophers, Evanston, Illinois, 1949). This book contains a thorough summary of the entire controversy.

[6] At distances of the order of 10^{-13} cm or smaller and for times of the order of this distance divided by the velocity of jight or smaller, present theories become so inadequate that it is generally believed that they are probably not applicable, except perhaps

[8]in a very crude sense. Thus, it is generally expected that in connection with phenomena associated with

not in terms of the usual interpretation, may be needed for a more thorough understanding of phenomena associated with very small distances. We shall not, however, actually develop such modifications in any detail in these papers.

After this article was completed, the author's attention was called to similar proposals for an alternative interpretation of the quantum theory made by de Broglie [7] in 1926, but later given up by him partly as a result of certain criticisms made by Pauli [8] and partly because of additional objections raised by de Broglie [7] himself. † As we shall show in Appendix B of Paper II, however, all of the objections of de Broglie and Pauli could have been met if only de Broglie had carried his ideas to their logical conclusion. The essential new step in doing this is to apply our interpretation in the theory of the measurement process itself as well as in the description of the observed system. Such a development of the theory of measurements is given in Paper II, [9] where it will be shown in detail that our interpretation leads to precisely the same results for all experiments as are obtained with the usual interpretation. The foundation for doing this is laid in Paper I, where we develop the basis of our interpretation, contrast it with the usual interpretation, and apply it to a few simple examples, in order to illustrate the principles involved.

26.3.2 2. The Usual Physical Interpretation of the Quantum Theory

The usual physical interpretation of the quantum theory centers around the uncertainty principle. Now, the uncertainty principle can be derived in two different ways. First, we may start with the assumption already criticized by Einstein, [1] namely, that a wave function that determines only probabilities of actual experimental results nevertheless provides the most complete possible specification of the so-called "quantum state" of an individual system. With the aid of this assumption and with the aid of the de Broglie relation, $\mathbf{p} = \hbar\mathbf{k}$, where $\mathbf{k}$ is the wave number associated with a particular fourier component of the wave function, the

uncertainty principle is readily deduced. [10] From this derivation, we are led to interpret the uncertainty principle as an inherent and irreducible limitation on the precision with which it is correct for us even to conceive of momentum and position as simultaneously defined quantities. For if, as is done in the usual interpretation of the quantum theory, the wave intensity is assumed to determine only the probability of a given position, and if the $\mathbf{k}$ th Fourier component of the wave function is assumed to determine only the probability of a corresponding momentum, $\mathbf{p} = \hbar\mathbf{k}$, then it becomes a contradiction in terms to ask for a state in which momentum and position are simultaneously and precisely defined.

---

this so-called "fundamenial length," a totally new theory will probably be needed. It is hoped that this theory could not only deal precisely with such processes as meson production and scattering of elementary particles, but that it would also systematically predict the masses, charges, spins, etc., of the large number of so-called "elementary" particles that have already been found, as well as those of new particles which might be found in the future.

[87] L. de Broglie, An Introduction to the Study of Wave Mechanics (E. P. Dutton and Company, Inc., New York, 1930), see Chapters 6, 9, and 10. See also Compt. rend. 183, 447 (1926); 184, 273 (1927); 185, 380 (1927).

[8] Reports on the Solvay Congress (Gauthiers-Villars et Cie., Paris, 1928), see p. 280.

† Note added in proof.-Madelung has also proposed a similar interpretation of the quantum theory, but like de Broglie he did not carry this interpretation to a logical conclusion. See E. Madelung, Z. f. Physik 40, 332 (1926), also G. Temple, Introduction to Quantum Theory (London, 1931).

[9] In Paper II, Sec. 9, we also discuss von Neumann's proof [see J. von Neumann, Mathemalische Grundlagen der Quantenmechanik (Verlag, Julius Springer, Berlin, 1932)] that quantum theory cannot be understood in terms of a statistical distribution of "hidden" causal parameters. We shall show that his conclusions do not apply to our interpretation, because he implicitly assumes that the hidden parameters must be associated only with the observed system, whereas, as will become evident in these papers, our interpretation requires that the hidden parameters shall also be associated with the measuring apparatus.

A second possible derivation of the uncertainty principle is based on a theoretical analysis of the processes with the aid of which physically significant quantities such as momentum and position can be measured. In such an analysis, one finds that because the measuring apparatus interacts with the observed system by means of indivisible quanta, there will always be an irreducible disturbance of some observed property of the system. If the precise effects of this disturbance could be predicted or controlled, then one could correct for these effects, and thus one could still in principle obtain simultaneous measurements of momentum and position, having unlimited precision. But if one could do this, then the uncertainty principle would be violated. The uncertainty principle is, as we have seen, however, a necessary consequence of the assumption that the wave function and its probability interpretation provide the most complete possible specification of the state of an individual system. In order to avoid the possibility of a contradiction with this assumption, Bohr [3,5,10,11] and others have suggested an additional assumption, namely, that the process of transfer of a single quantum from observed system to measuring apparatus is inherently unpredictable, uncontrollable, and not subject to a detailed rational analysis or description. With the aid of this assumption, one can show [10] that the same uncertainty principle that is deduced from the wave function and its probability interpretation is also obtained as an inherent and unavoidable limitation on the precision of all possible measurements. Thus, one is able to obtain a set of assumptions, which permit a self-consistent formulation of the usual interpretation of the quantum theory.

The above point of view has been given its most consistent and systematic expression by Bohr, [3,5,10] in terms of the "principle of complementarity." In formulating this principle, Bohr suggests that at the atomic level we must renounce our hitherto successful practice of conceiving of an individual system as a unified and precisely definable whole, all of whose aspects are, in a manner of speaking, simultaneously and

unambiguously accessible to our conceptual gaze. Such a system of concepts, which is sometimes called a "model," need not be restricted to pictures, but may also include, for example, mathematical concepts, as long as these are supposed to be in a precise (i.e., one-to-one) correspondence with the objects that are being described. The principle of complementarity requires us, however, to renounce even mathematical models. Thus, in Bohr's point of view, the wave function is in no sense a conceptual model of an individual system, since it is not in a precise (one-to-one) correspondence with the behavior of this system, but only in a statistical correspondence.

In place of a precisely defined conceptual model, the principle of complementarity states that we are restricted to complementarity pairs of inherently imprecisely defined concepts, such as position and momentum, particle and wave, etc. The maximum degree of precision of definition of either member of such a pair is reciprocally related to that of the opposite member. This need for an inherent lack of complete precision can be understood in two ways. First, it can be regarded as a consequence of the fact that the experimental apparatus needed for a precise measurement of one member of a complementary pair of variables must always be such as to preclude the possibility of a simultaneous and precise measurement of the other member. Secondly, the assumption that an individual system is completely specified by the wave function and its probability interpretation implies a corresponding unavoidable lack of precision in the very conceptual structure, with the aid of which we can think about and describe the behavior of the system.

It is only at the classical level that we can correctly neglect. the inherent lack of precision in all of our conceptual models; for here, the incomplete determination of physical properties implied by the uncertainty principle produces effects that are too small to be of practical significance. Our ability to describe classical systems in terms of precisely definable models is, however, an

[8][10] See reference 2, Chapter 5.

[11] N. Bohr, Atomic Theory and the Description of Nature (Cambridge University Press, London, 1934).

integral part of the usual interpretation of the theory. For without such models, we would have no way to describe, or even to think of, the result of an observation, which is of course always finally carried out at a classical level of accuracy. If the relationships of a given set of classically describable phenomena depend significantly on the essentially quantum-mechanical properties of matter, however, then the principle of complementarity states that no single model is possible which could provide a precise and rational analysis of the connections between these phenomena. In such a case, we are not supposed, for example, to attempt to describe in detail how future phenomena arise out of past phenomena. Instead, we should simply accept without further analysis the fact that future phenomena do in fact somehow manage to be produced, in a way that is, however, necessarily beyond the possibility of a detailed description. The only aim of a
mathematical theory is then to predict the statistical relations, if any, connecting these phenomena.

26.3.3 3. Criticism of the Usual Interpretation of the Quantum Theory

The usual interpretation of the quantum theory can be criticized on many grounds. [5] In this paper, however, we shall stress only the fact that it requires us to give up the possibility of even conceiving precisely what might determine the behavior of an individual system at the quantum level, without providing adequate proof that such a renunciation is necessary. [9] The usual interpretation is admittedly consistent; but the mere demonstration of such consistency does not exclude the possibility of other equally consistent interpretations, which would involve additional elements or parameters permitting a detailed causal and continuous description of all processes, and not requiring us to forego the possibility of conceiving the quantum level in precise terms. From the point of view of the usual interpretation, these additional elements or parameters could be called "hidden" variables. As a matter of fact, whenever we have previously had recourse to statistical theories, we have always ultimately found that the laws governing the individual members of a statistical ensemble could be expressed in terms of just such hidden variables. For example, from the point of view of macroscopic physics, the coordinates and momenta of individual atoms are hidden variables, which in a large scale system manifest themselves only as statistical averages. Perhaps then, our present quantummechanical averages are similarly a manifestation of hidden variables, which have not, however, yet been detected directly.

Now it may be asked why these hidden variables should have so long remained undetected. To answer this question, it is helpful to consider as an analogy the early forms of the atomic theory, in which the existence of atoms was postulated in order to explain certain large-scale effects, such as the laws of chemical combination, the gas laws, etc. On the other hand, these same effects could also be described directly in terms of existing macrophysical concepts (such as pressure, volume, temperature, mass, etc.); and a correct description in these terms did not require any reference to atoms. Ultimately, however, effects were found which contradicted the predictions obtained by extrapolating certain purely macrophysical theories to the domain of the very small, and which could be understood correctly in terms of the assumption that matter is composed of atoms. Similarly, we suggest that if there are hidden variables underlying the present quantum theory, it is quite likely that in the atomic domain, they will lead to effects that can also be described adequately in the terms of the usual quantum-mechanical concepts; while in a domain associated with much smaller dimensions, such as the level associated with the "fundamental length" of the order of 10^{-13} cm, the hidden variables
may lead to completely new effects not consistent with the extrapolation of the present quantum theory down to this level.

If, as is certainly entircly possible, these hidden vari ables are actually needed for a correct description at small distances, we could easily be kept on the wrong track for a long time by restricting ourselves to the usual interpretation of the quantum theory, which excludes such hidden variables as a matter of principle. It is therefore very important for us to investigate our reasons for supposing that the usual physical interpretation is likely to be the correct one. To this end, we shall begin by repeating the two mutually consistent assumptions on which the usual interpretation is based (see Sec. 2) :
(1) The wave function with its probability interpretation determines the most complete possible specification of the state of an individual system.
(2) The process of transfer of a single quantum from observed system to measuring apparatus is inherently unpredictable, uncontrollable, and unanalyzable.

Let us now inquire into the question of whether there are any experiments that could conceivably provide a test for these assumptions. It is often stated in connection with this problem that the mathematical apparatus of the quantum theory and its physical interpretation form a consistent whole and that this combined system of mathematical apparatus and physical interpretation is tested adequately by the extremely wide range of experiments that are in agreement with predictions obtained by using this system. If assumptions (1) and (2) implied a unique mathematical formulation, then such a conclusion would be valid, because experimental predictions could then be found which, if contradicted, would clearly indicate that these assumptions were wrong. Although assumptions (1) and (2) do limit the possible forms of the mathematical theory, they do not limit these forms sufficiently to make possible a unique set of predictions that could in principle permit such an experimental test. Thus, one can contemplate practically arbitrary changes in the Hamiltonian operator, including, for example, the postulation of an unlimited range of new kinds of meson fields each having almost any conceivable rest mass, charge, spin, magnetic moment, etc. And if such postulates should prove to be inadequate, it is conceivable that we may have to introduce nonlocal operators, nonlinear fields, S-matrices, etc. This means that when the theory is found to be inadequate (as now happens, for example, at distances of the order of 10^{-13} cm), it is always possible, and, in fact, usually quite natural, to assume that the theory can be made to agree with experiment by some as yet unknown change in the mathematical formulation alone, not requiring any fundamental changes in the physical interpretation. This means that as long as we accept the usual physical interpretation of the quantum theory, we cannot be led by any conceivable experiment to
give up this interpretation, even if it should happen to be wrong. The usual physical interpretation therefore presents us with a considerable danger of falling into a trap, consisting of a self-closing chain of circular hypotheses, which are in principle unverifiable if true. The only way of avoiding the possibility of such a trap is to study the consequences of postulates that contradict assumptions (1) and (2) at the outset. Thus, we could, for example, postulate that the precise outcome of each individual measurement process is in principle determined by some at present "hidden" elements or variables; and we could then try to find experiments that depended in a unique and reproducible way on the assumed state of these hidden elements or variables. If such predictions are verified, we should then obtain experimental evidence favoring the hypothesis that hidden variables exist. If they are not verified, however, the correctness of the usual interpretation of the quantum theory is not necessarily proved, since it may be necessary instead to alter the specific character of the theory that is supposed to describe the behavior of the assumed hidden variables.

We conclude then that a choice of the present interpretation of the quantum theory involves a real physical limitation on the kinds of theories that we wish to take into consideration. From the arguments given here, however, it would seem that there are no secure experimental or theoretical grounds on which we can base such a choice because this choice follows from bypotheses that cannot conceivably be subjected to an experimental test and because we now

have an alternative interpretation.

26.3.4 4. New Physical Interpretation of Schroedinger's Equation

We shall now give a general description of our suggested physical interpretation of the present mathematical formulation of the quantum theory. We shall carry out a more detailed description in subsequent sections of this paper.

We begin with the one-particle Schroedinger equation, and shall later generalize to an arbitrary number of particles. This wave equation is

$$i\hbar\partial\psi/\partial L = -\left(\hbar^2/2m\right)\nabla^2\psi + V(\mathbf{x})\psi. \tag{1}$$

Now ψ is a complex function, which can be expressed as

$$\psi = R\exp(iS/\hbar), \tag{2}$$

where R and S are real. We readily verify that the equations for R and S are

$$\frac{\partial R}{\partial t} = -\frac{1}{2m}\left[R\nabla^2 S + 2\nabla R\cdot\nabla S\right], \tag{3}$$

$$\frac{\partial S}{\partial t} = -\left[\frac{(\nabla S)^2}{2m} + V(\mathbf{x}) - \frac{\hbar^2}{2m}\frac{\nabla^2 R}{R}\right]. \tag{4}$$

It is convenient to write $P(\mathbf{x}) = R^2(\mathbf{x})$, or $R = P^{\frac{1}{2}}$ where $P(\mathbf{x})$ is the probability density. We then obtain

$$\frac{\partial P}{\partial t} + \nabla\cdot\left(P\frac{VS}{m}\right) = 0 \tag{5}$$

$$\frac{\partial S}{\partial t} + \frac{(\nabla S)^2}{2m} + V(\mathbf{x}) - \frac{\hbar^2}{4m}\left[\frac{\nabla^2 P}{P} - \frac{1}{2}\frac{(\nabla P)^2}{P^2}\right] = 0 \tag{6}$$

Now, in the classical limit ($\hbar \to 0$) the above equations are subject to a very simple interpretation. The function $S(\mathbf{x})$ is a solution of the Hamilton-Jacobi equation. If we consider an ensemble of particle trajectories which are solutions of the equations of motion, then it is a well-known theorem of mechanics that if all of these trajectories are normal to any given surfacc of constant S, then they are normal to all surfaces of constant S, and $\nabla S(\mathbf{x})/m$ will be equal to the velocity vector, $\mathbf{v}(\mathbf{x})$, for any particle passing the point x. Equation (5) can therefore be re-expressed as

$$\partial P/\partial t + \nabla\cdot(P\mathbf{v}) = 0 \tag{7}$$

This equation indicates that it is consistent to regard $P(\mathbf{x})$ as the probability density for particles in our ensemble. For in that case, we can regard $P\mathbf{v}$ as the mean current of particles in this ensemble, and Eq. (7) then simply expresses the conservation of probability.

Let us now see to what extent this interpretation can be given a meaning even when $h \neq 0$. To do this, let us assume that each particle is acted on, not only by a "classical" potential, $V(\mathbf{x})$ but also by a "quantummechanical" potential,

$$U(\mathbf{x}) = \frac{-\hbar^2}{4m}\left[\frac{\nabla^2 P}{P} - \frac{1}{2}\frac{(\nabla P)^2}{P^2}\right] = \frac{-\hbar^2}{2m}\frac{\nabla^2 R}{R} \tag{8}$$

Then Eq. (6) can still be regarded as the HamiltonJacobi equation for our ensemble of particles, $\nabla S(\mathbf{x})/m$ can still be regarded as the particle velocity, and Eq. (5) can still be regarded as describing conservation of probability in our ensemble. Thus, it would seem that we have here the nucleus of an alternative interpretation for Schroedinger's equation.

The first step in developing this interpretation in a more explicit way is to associate with each electron a particle having precisely definable and continuously varying values of position and momentum. The solution of the modified Hamilton-Jacobi equation (4) defines an ensemble of possible trajectories for this particle, which can be obtained from the HamiltonJacobi function, $S(\mathbf{x})$, by integrating the velocity, $\mathbf{v}(\mathbf{x}) = \nabla S(\mathbf{x})/m$. The equation for S implies, however, that the particles moves under the action of a force which is not contircly derivable from the classical potential, $V(x)$, but which also obtains a contribution from the "quantum-mechanical" potential, $U(\mathbf{x}) = (-\hbar^2/2m) \times \nabla^2 R/R$. The function, $R(\mathbf{x})$, is not completely arbitrary, but is partially determined in terms of $S(\mathbf{x})$ by
the differential Eq. (3). Thus R and S can be said to codetermine each other. The most convenient way of obtaining R and S is, in fact, usually to solve Eq. (1) for the Schroedinger wave function, ψ, and then to use the relations,

$$\psi = U + iW = R[\cos(S/\hbar) + i\sin(S/\hbar)],$$
$$R^2 = U^2 + V^2; \quad S = \hbar \tan^{-1}(W/U).$$

Since the force on a particle now depends on a function of the absolute value, $R(\mathbf{x})$, of the wave function, $\psi(\mathbf{x})$, evaluated at the actual location of the particle, we have effectively been led to regard the wave function of an individual electron as a mathematical representation of an objectively real field. This field exerts a force on the particle in a way that is analogous to, but not identical with, the way in which an electromagnetic field exerts a force on a charge, and a meson field exerts a force on a nucleon. In the last analysis, there is, of course, no reason why a particle slould not be acted on by a ψ-field, as well as by an electromagnetic field, a gravitational field, a set of meson fields, and periaps by still other ficlds that have not yet been discovered.

The analogy with the electromagnetic (and other) field goes quite far. For just as the electromagnetic field obeys Maxwell's equations, the ψ-field obeys Schroedinger's equation. In both cases, a complete specification of the fields at a given instant over every point in space determines the values of the fields for all times. In both cases, once we know the field functions, we can calculate force on a particle, so that, if we also know the initial position and momentum of the particle, we can calculate its entire trajectory.

In this connection, it is worth while to recall that the use of the Hamilton-Jacobi equation in solving for the motion of a particle is only a matter of convenience and that, in principle, we can always solve directly by using Newton's laws of motion and the correct boundary conditions. The equation of motion of a particle acted on by the classical potential, $V(\mathbf{x})$, and the "quantummechanical" potential, Eq. (8), is

$$md^2\mathbf{x}/dl^2 = -\nabla\left\{V(\mathbf{x}) - \left(h^2/2m\right)\nabla^2 R/R\right\} \tag{8a}$$

It is in connection with the boundary conditions appearing in the equations of motion that we find the only fundamental difference between the ψ-field and other fields, such as the electromagnetic field. For in order to obtain results that are equivalent to those of the usual interpretation of the quantum theory, we are required to restrict the value of the initial particle momentum to $\mathbf{p} = \nabla S(\mathbf{x})$. From the application of Hamilton-Jacobi theory to Eq. (6), it follows that this restriction is consistent, in the sense that if it holds initially, it will hold for all time. Our suggested new interpretation of the quantum theory implies, however, that this restriction is not inherent in the conceptual structure. We shall see in Sec. 9, for example, that

it is
quite consistent in our interpretation to contemplate modifications in the theory, which permit an arbitrary relation between $\mathbf{p}$ and $\nabla S(\mathbf{x})$. The law of force on the particle can, however, be so chosen that in the atomic domain, $\mathbf{p}$ turns out to be very nearly equal to $\nabla S(\mathbf{x})/m$, while in processes involving very small distances, these two quantities may be very different. In this way, we can improve the analogy between the ψ-field and the electromagnetic field (as well as between quantum mechanics and classical mechanics).

Another important difference between the ψ-field and the electromagnetic field is that, whereas Schroedinger's equation is homogeneous in ψ, Maxwell's equations are inhomogeneous in the electric and magnetic fields. Since inhomogeneities are needed to give rise to radiation, this means that our present equations imply that the ψ-field is not radiated or absorbed, but simply changes its form while its integrated intensity remains constant. This restriction to a homogeneous equation is, however, like the restriction to a homogeneous equation is, however, like the restriction to $\mathbf{p} = \nabla S(\mathbf{x})$, not inherent in the conceptual structure of our new interpretation. Thus, in Sec. 9, we shall show that one can consistently postulate inhomogeneities in the equation governing ψ, which produce important effects only at very small distances, and negligible effects in the atomic domain. If such inhomogeneities are actually present, then the ψ-field will be subject to being emitted and absorbed, but only in connection with processes associated with very small distances. Once the ψ-field has been emitted, however, it will in all atomic processes simply obey Schroedinger's equation as a very good approximation. Nevertheless, at very small distances, the value of the ψ-field would, as in the case of the electromagnetic field, depend to some extent on the actual location of the particle.

Let us now consider the meaning of the assumption of a statistical ensemble of particles with a probability density equal to $P(\mathbf{x}) = R^2(\mathbf{x}) = |\psi(\mathbf{x})|^2$. From Eq. (5), it follows that this assumption is consistent, provided that ψ satisfies Schroedinger's equation, and $\mathbf{v} = \nabla S(\mathbf{x})/m$. This probability density is numerically equal to the probability density of particles obtained in the usual interpretation. In the usual interpretation, however, the need for a probability description is regarded as inherent in the very structure of matter (see Sec. 2), whereas in our interpretation, it arises, as we shall see in Paper II, because from one measurement to the next, we cannot in practice predict or control the precise location of a particle, as a result of corresponding unpredictable and uncontrollable disturbances introduced by the measuring apparatus. Thus, in our interpretation, the use of a statistical ensemble is (as in the case of classical statistical mechanics) only a practical necessity, and not a reflection of an inherent limitation on the precision with which it is correct for us to conceive of the variables defining the state of the system. Moreover, it is clear that if in connection with
very small distances we are ultimately required to give up the special assumptions that ψ satisfies Schroedinger's equation and that $\mathbf{v} = \nabla S(\mathbf{x})/m$, then $|\psi|^2$ will cease to satisfy a conservation equation and will therefore also cease to be able to represent the probability density of particles. Nevertheless, there would still be a true probability density of particles which is conserved. Thus, it would become possible in principle to find experiments in which $|\psi|^2$ could be distinguished from the probability density, and therefore to prove that the usual interpretation, which gives $|\psi|^2$ only a probability interpretation must be inadequate. Moreover, we shall see in Paper II that with the aid of such modifications in the theory, we could in principle measure the particle positions and momenta precisely, and thus violate the uncertainty principle. As long as we restrict ourselves to conditions in which Schroedinger's equation is satisfied, and in which $\mathbf{v} = \nabla S(\mathbf{x})/m$, however, the uncertainty principle will remain an effective practical limitation on the possible precision of measurements. This means that at present, the particle positions and momenta should be regarded as "lidden" variables, since as we shall see in Paper II, we are not now able to obtain experiments that localize them to a region smaller than that in which the intensity of the ψ-field is appreciable. Thus, we cannot yet find clear-cut

experimental proof that the assumption of these variables is necessary, although it is entirely possible that, in the domain of very small distances, new modifications in the theory may have to be introduced, which would permit a proof of the existence of the definite particle position and momentum to be obtained.
We conclude that our suggested interpretation of the quantum theory provides a much broader conceptual framework than that provided by the usual interpretation, for all of the results of the usual interpretation are obtained from our interpretation if we make the following three special assumptions which are mutually consistent:
(1) That the ψ-field satisfies Schroedinger's equation.
(2) That the particle momentum is restricted to $\mathbf{p} = \nabla S(\mathbf{x})$.
(3) That we do not predict or control the precise location of the particle, but have, in practice, a statistical ensemble with probability density $P(\mathrm{x}) = |\psi(\mathrm{x})|^9$. The use of statistics is, however, not inherent in the conceptual structure, but merely a consequence of our ignorance of the precise initial conditions of the particle.

As we shall see in Sec. 9, it is entirely possible that a better theory of phenomena involving distances of the order of 10^{-13} cm or less would require us to go beyond the limitations of these special assumptions. Our principal purpose in this paper (and in Paper II) is to show, however, that if one makes these special assumptions, our interpretation leads in all possible experiments to the same predictions as are obtained from the usual interpretation. [9]

It is now easy to understand why the adoption of the
usual interpretation of the quantum theory would tend to lead us away from the direction of our suggested alternative interpretation. For in a theory involving hidden variables, one would normally expect that the behavior of an individual system should not depend on the statistical ensemble of which it is a member, because this ensemble refers to a series of similar but disconnected experiments carried out under equivalent initial conditions. In our interpretation, however, the "quantum-mechanical" potential, $U(\mathbf{x})$, acting on an individual particle depends on a wave intensity, $P(\mathbf{x})$, that is also numerically equal to a probability density in our ensemble. In the terminology of the usual interpretation of the quantum theory, in which one tacitly assumes that the wave function has only one interpretation; namely, in terms of a probability, our suggested new interpretation would look like a mysterious dependence of the individual on the statistical ensemble of which it is a member. In our interpretation, such a dependence is perfectly rational, because the wave function can consistently be interpreted both as a force and as a probability density. [12]

It is instructive to carry our analogy between the Schroedinger field and other kinds of fields a bit further. To do this, we can derive the wave Eqs. (5) and (6) from a Hamiltonian functional. We begin by writing down the expression for the mean energy as it is expressed in the usual quantum theory:

$$\bar{H} = \int \psi^* \left(-\frac{\hbar^2}{2m}\nabla^2 + V(\mathbf{x}) \right)\psi d\mathbf{x}$$
$$= \int \left\{ \frac{\hbar^2}{2m}|\nabla\psi|^2 + V(\mathbf{x})|\psi|^2 \right\} d\mathbf{x}$$

Writing $\psi = P^{\frac{1}{2}} \exp(iS/h)$, we obtain

$$\bar{H} = \int P(\mathbf{x}) \left\{ \frac{(\nabla S)^2}{2m} + V(\mathbf{x}) + \frac{\hbar^2}{8m}\frac{(\nabla P)^2}{P^2} \right\} d\mathbf{x} \tag{9}$$

We shall now reinterpret $P(\mathbf{x})$ as a field coordinate, defined at each point, $\mathbf{x}$, and we shall tentatively assume that $S(\mathbf{x})$ is the momentum, canonically conjugate to $P(\mathbf{x})$. That such an assumption is appropriate can be verified by finding the Hamiltonian equations of motion for

$P(\mathbf{x})$ and $S(\mathbf{x})$, under the assumption that the Hamiltonian functional is equal to $\bar{H}$ (See Eq. (9)). These equations of motion are

$$\dot{P} = \frac{\delta \bar{H}}{\delta S} = -\frac{1}{m}\nabla \cdot (P \nabla S),$$
$$\dot{S} = -\frac{\delta \bar{H}}{\delta P} = -\left[\frac{(\nabla S)^2}{2m} + V^2(\mathbf{x}) - \frac{\hbar^2}{4m}\left(\frac{\nabla^2 P}{P} - \frac{1}{2}\frac{(\nabla P)^2}{P^2}\right)\right].$$

These are, however, the same as the correct wave Eqs. (5) and (6).

We can now show that the mean particle energy averaged over our ensemble is equal to the usual quantum mechanical mean value of the Hamiltonian, $\bar{H}$. To do this, we note that according to Eqs. (3) and (6), the energy of a particle is

$$E(\mathbf{x}) = -\frac{\partial S(\mathbf{x})}{\partial t} = \left[\frac{(\nabla S)^2}{2m} + V(\mathbf{x}) - \frac{\hbar^2}{2m}\frac{\nabla^2 R}{R}\right]. \tag{10}$$

The mean particle energy is found by averaging $E(\mathbf{x})$ with the weighting function, $P(\mathbf{x})$. We obtain

$$\underset{\substack{\text{average} \\ \langle E\rangle_{\text{ensemble}}}}{\underline{\text{a}}} = \int P(\mathbf{x}) E(\mathbf{x}) d\mathbf{x}$$
$$= \int P(\mathbf{x}) \left[\frac{(\nabla S)^2}{2m} + V(\mathbf{x})\right] d\mathbf{x} - \frac{\hbar^2}{2m}\int R \nabla^2 R d\mathbf{x}$$

A little integration by parts yields

$$\langle E\rangle_{\text{ensemble}} = \int P(\mathbf{x}) \left[\frac{(\nabla S)^2}{2m} + V(\mathbf{x}) + \frac{\hbar^2}{8m}\frac{(\nabla P)^2}{P^2}\right] d\mathbf{x} = \vec{H} \tag{11}$$

26.3.5 5. The Stationary State

We shall now show how the problem of stationary states is to be treated in our interpretation of the quantum theory.

The following seem to be reasonable requirements in our interpretation for a stationary state:

(1) The particle energy should be a constant of the motion.

(2) The quantum-mechanical potential should be independent of time.

(3) The probability density in our statistical ensemble should be independent of time.

It is easily verified that these requirements can be satisfied with the assumption that

$$\psi(\mathbf{x}, t) = \psi_0(\mathbf{x}) \exp(-iEt/h)$$
$$= R_0(\mathbf{x}) \exp[i(\Phi(\mathbf{x}) - Et)/\hbar] \tag{12}$$

From the above, we obtain $S = \Phi(\mathbf{x}) - El$. According to the generalized Hamilton-Jacobi Eq. (4), the particle energy is given by

[812] This consistency is guaranteed by the conservation Eq. (7). The questions of why an arbitrary statistical ensemble tends to decay into an ensemble with a probability density equal to $\psi^*\psi$ will be discussed in Paper II, Sec. 7.

$$\partial S/\partial l = -E.$$

Thus, we verify that the particle energy is a constant of the motion. Moreover, since $P = R^2 = |\psi|^2$, it follows that P (and R) are independent of time. This means that both the probability density in our ensemble and the quantum-mechanical potential are also time independent.

The reader will readily verify that no other form of solution of Schroedinger's equation will satisfy all three of our criteria for a stationary state.

Since ψ is now being regarded as a mathematical representation of an objectively real force field, it follows that (like the electromagnetic field) it should be everywhere finite, continuous, and single valued. These requirements will guarantee in all cases that occur in practice that the allowed values of the energy in a stationary state, and the corresponding eigenfunctions are the same as are cbtained from the usual interpretation of the theory.

In order to show in more detail what a stationary state means in our interpretation, we shall now consider three examples of stationary states.

Case 1: " s " State

The first case that we shall consider is an " s " state. In an " s " state, the wave function is

$$\psi = f(r)\exp[i(\alpha - El)/\hbar], \tag{13}$$

where α is an arbitrary constant and r is the radius taken from the center of the atom. We conclude that the Hamilton-Jacobi function is

$$S = \alpha - Et.$$

The particle velocity is

$$\mathrm{v} = \nabla S = 0.$$

The particle is therefore simply standing still, wherever it may happen to be. How can it do his? The absence of motion is possible because the applied force, $-\nabla V(\mathbf{x})$, is balanced by the "quantum-mechanical" force, ($\hbar^2/2m)\nabla\,(\nabla^2 R/R)$, produced by the Schroedinger ψ-ficld acting on its own particle. There is, however, a statistical ensemble of possible positions of the particle, with a probability density, $P(x) = (f(r))^2$.

Case 2: State with Nonzero Angular Momentum

In a typical state of nonzero angular momentum, we have

$$\psi = f_n^l(r)P_l^m(\cos\theta)\exp[i(\beta - Et + \hbar m\phi)/\hbar], \tag{14}$$

where θ and ϕ are the colatitude and azimuthal polar angles, respectively, $P_l{}^m$ is the associated Legendre polynomial, and β is a constant. The Hamilton-Jacobi function is $S = \beta - El + \hbar m\phi$. From this result it follows that the z component of the angular momentum is equal to hm. To prove this, we write

$$L_z = xp_y - yp_x = x\partial S/\partial y - y\partial S/\partial x = \partial S/\partial\phi = hm. \tag{15}$$

Thus, we obtain a statistical ensemble of trajectories which can have different forms, but all have the same "quantized" value of the z component of the angular momentum.

Case 3: A Scattering Problem

Let us now consider a scattering problem. Because it is comparatively casy to analyze, we shall discuss a hypothetical experiment, in which an electron is incident in the z direction with an initial momentum, p_0, on a system consisting of two slits. [13] After the electron passes through the slit system, its position is measured and recorded, for example, on a phoiographic plate.

Now, in the usual interpretation of the quantum theory, the electron is described by a wave function. The incident part of the wave function is $\psi_0 \sim \exp(ip_0\xi/\ h)$; but when the wave passes through the slit system, it is modified by interference and diffraction effects, so that it will develop a characteristic intensity pattern by the time it reaches the position measuring instrument. The probability that the electron will be detected between $\mathbf{x}$ and $\mathbf{x}+d\mathbf{x}$ is $|\psi(\mathbf{x})|^2 d\mathbf{x}$. If the experiment is repeated many times under equivalent initial conditions, one eventually obtains a patitern of hits on the photographic plate that is very reminiscent of the interference patterns of optics.

In the usual interpretation of the quantum theory, the origin of this interference pattern is very difficult to understand. For there may be certain points where the wave function is zero when both slits are open, but not zero when only one slit is open. How can the opening of a second slit prevent the electron from reaching certain points that it could reach if this slit were closed? If the electron acted completely like a classical particle, this phenomenon could not be explained at all. Clearly, then the wave aspects of the electron must have something to do with the production of the interference pattern. Yet, the electron cannot be identical with its associated wave, because the latter spreads out over a wide region. On the other hand, when the electron's position is measured, it always appears at the detector as if it were a localized particle.

The usual interpretation of the quantum theory not only makes no attempt to provide a single precisely defined conceptual model for the production of the phenomena described above, but it asserts that no such model is even conceivable. Instead of a single precisely defined conceptual model, it provides, as pointed out in Sec. 2, a pair of complementary models, viz., particle and wave, each of which can be made more precise only under conditions which necessitate a reciprocal decrease in the degree of precision of the other. Thus, while the electron goes through the slit system, its position is said to be inherently ambiguous, so that if we wish to obtain an interference pattern, it is meaningless to ask through which slit an individual electron actually passed. Within the domain of space within which the position of the electron has no meaning we can use the wave model and thus describe the subsequent production of interference. If, however, we

tried to define the position of the electron as it passed the slit system more accurately by means of a measurement, the resulting disturbance of its motion produced by the measuring apparatus would destroy the interference pattern. Thus, conditions would be created in which the particle model becomes more precisely defined at the expense of a corresponding decrease in the degree of definition of the wave model. When the position of the electron is measured at the photographic plate, a similar sharpening of the degree of definition of the particle model occurs at the expense of that of the wave model.

In our interpretation of the quantum theory, this experiment is described causally and continuously in terms of a single precisely definable conceptual model. As we have already shown, we must use the same wave function as is used in the usual interpretation; but instead we regard it as a mathematical representation of an objectively real field that determines part of the force acting on the particle. The initial momentum of the particle is obtained from the incident wave function, $\exp(ip_0z/h)$, as $p = \partial s/\partial z = p_0$. We do not in practice, however,

[8][13] This experiment is discussed in some detail in reference 2, Chapter 6, Sec. 2.

control the initial location of the particle, so that although it goes through a definite slit, we cannot predict which slit this will be. The particle is at all times acted on by the "quantum-mechanical" potential, $U = (-\hbar^2/2m)\nabla^2 R/R$. While the particle is incident, this potential vanishes because R is then a constant; but after it passes through the slit system, the particle encounters a quantum-mechanical potential that changes rapidly with position. The subsequent motion of the particle may therefore become quite complicated. Nevertheless, the probability that a particle shall enter a given region, $d\mathbf{x}$, is as in the usual interpretation, equal to $|\psi(\mathbf{x})|^2 d\mathbf{x}$. We therefore deduce that the particle can never reach a point where the wave function vanishes. The reason is that the "quan-tum-mechanical" potential, U, becomes infinite when R becomes zero. If the approach to infinity happens to be through positive values of U, there will be an infinite force repelling the particle away from the origin. If the approach is through negative values of U, the particle will go through this point with infinite speed, and thus spend no time there. In either case, we obtain a simple and precisely definable conceptual model explaining why particles can never be found at points where the wave function vanishes.
If one of the slits is closed, the "quantum-mechanical" potential is correspondingly altered, because the ψ-field is changed, and the particle may then be able to reach certain points which it was unable to reach when both slits were open. The slit is therefore able to affect the motion of the particle only indirectly, through its effect on the Schroedinger ψ-field. Moreover, as we shall see in Paper II, if the position of the electron is measured while it is passing through the slit system, the measuring apparatus will, as in the usual interpretation, create a disturbance that destroys the interference
pattern. In our interpretation, however, the necessity for this destruction is not inherent in the conceptual structure; and as we shall see, the destruction of the interference pattern could in principle be avoided by means of other ways of making measurements, ways which are conceivable but not now actually possible.

26.3.6 6. The Many-body Problem

We shall now extend our interpretation of the quantum theory to the problem of many bodies. We begin with the Schroedinger equation for two particles. (For simplicity, we assume that they have equal masses, but the extension of our treatment to arbitrary masses will be obvious.)

$$ih\frac{\partial\psi}{\partial t} = -\frac{\hbar^2}{2m}\left(\nabla_1^2\psi + \nabla_2^2\psi\right) + V\left(\mathbf{x}_1, \mathbf{x}_2\right)\psi.$$

Writing $\psi = R\left(\mathbf{x}_1, \mathbf{x}_2\right)\exp\left[iS\left(\mathbf{x}_1, \mathbf{x}_2\right)/h\right]$ and $R^2 - P$, we obtain

$$\frac{\partial P}{\partial t} + \frac{1}{m}\left[\nabla_1 \cdot P\nabla_1 S + \nabla_2 \cdot P\nabla_2 S\right] = 0, \tag{16}$$

$$\frac{\partial S}{\partial t} + \frac{\left(\nabla_1 S\right)^2 + \left(\nabla_2 S\right)^2}{2m} + V\left(\mathbf{x}_1, \mathbf{x}_2\right) - \frac{\hbar^2}{2mR}\left[\nabla_1^2 R + \nabla_2^2 R\right] = 0. \tag{17}$$

The above equations are simply a six-dimensional generalization of the similar three-dimensional Eqs. (5) and (6) associated with the one-body problem. In the two-body problem, the system is described therefore by a six-dimensional Schroedinger wave and by a sixdimensional trajectory, specifying the actual location of each of the two particles. The velocity of this trajectory has components, $\nabla_1 S/m$ and $\nabla_2 S/m$, respectively, in each of the three-dimensional surfaces associated with a given particle. $P\left(\mathbf{x}_1, \mathbf{x}_2\right)$ then has a dual interpretation. First, it defines a "quantum-mechanical" potential, acting on each particle

$$U(\mathbf{x}_1, \mathbf{x}_2) = -\left(\hbar^2/2mR\right)\left[\nabla_1^2 R + \nabla_2^2 R\right].$$

This potential introduces an additional effective interaction between particles over and above that due to the classically inferrable potential $V(\mathbf{x})$. Secondly, the function $P(\mathbf{x}_1, \mathbf{x}_2)$ can consistently be regarded as the probability density of representative points ($\mathbf{x}_1, \mathbf{x}_2$) in our six-dimensional ensemble.

The extension to an arbitrary number of particles is straightforward, and we shall quote only the results here. We introduce the wave function, $\psi = R(\mathbf{x}_1, \mathbf{x}_2, \cdots \mathbf{x}_n) \exp\left[iS(\mathbf{x}_1, \mathbf{x}_2 \cdots \mathbf{x}_n)/\hbar\right]$ and define a. $3n$-dimensional trajectory, where n is the number of particles, which describes the behavior of every particle in the system. The velocity of the i th particle is $\mathbf{v}_i = \nabla_i S(\mathbf{x}_1, \mathbf{x}_2 \cdots \mathbf{x}_n)/m$. The function $P(\mathbf{x}_1, \mathbf{x}_2 \cdots \mathbf{x}_n) = R^2$ has two interpretations. First, it defines a "quantum-mechanical" potential

$$U(\mathbf{x}_1, \mathbf{x}_2 \cdots \mathbf{x}_n) = -\frac{n^2}{2mR} \sum_{s=1}^{n} \nabla_s{}^2 R(\mathbf{x}_1, \mathbf{x}_2 \cdots \mathbf{x}_n) \tag{18}$$

Secondly, $P(\mathbf{x}_1, \mathbf{x}_2 \cdots \mathbf{x}_n)$ is equal to the density of representative points ($\mathbf{x}_1, \mathbf{x}_2 \cdots \mathbf{x}_n$) in our $3n$-dimensional ensemble.

We see here that the "effective potential," $U(\mathbf{x}_1, \mathbf{x}_2, \cdots \mathbf{x}_n)$, acting on a particle is equivalent to that produced by a "many-body" force, since the force between any two particles may depend significantly on the location of every other particle in the system. An example of the effects of such a force is given by the exclusion principle. Thus, if the wave function is antisymmetric, we deduce that the "quantum-mechanical" forces will be such as to prevent two particles from ever reaching the same point in space, for in this case, we must have $P = 0$.

26.3.7 7. Transitions between Stationary States. the Franck-hertz Experiment

Our interpretation of the quantum theory describes all processes as basically causal and continuous. How then can it lead to a correct description of processes such as the Franck-Hertz experiment, the photoelectric effect, and the Compton effect, which seem to call most strikingly for an interpretation in terms of discontinuous and incompletely determined transfers of energy and momentum? In this section, we shall answer this question by applying our suggested interpretation of the quantum theory in the analysis of the FranckHertz experiment. Here, we shall see that the apparently discontinuous nature of the process of transfer of energy from the bombarding particle to the atomic electron is brought about by the "quantum-mechanical" potential, $U = (-\hbar^2/2m)\nabla^2 R/R$, which does not necessarily become small when the wave intensity becomes small. Thus, even if the force of interaction between two particles is very weak, so that a correspondingly small disturbance of the Schroedinger wave function is produced by the interaction of these particles, this disturbance is capable of bringing about very large transfers of energy and momentum between the particles in a very short time. This means that if we view only the end results, this process presents the aspect of being discontinuous. Moveover, we shall see that the precise value of the energy transfer is in principle determined by the initial position of each particle and by the initial form of the wave function. Since we cannot in practice predict or control the initial particle positions with complete precision, we are also unable to predict or control the final outcome of such an experiment, and can, in practice, predict only the probability of a given outcome. Because the probability that the particles will enter a region with coordinates, $\mathbf{x}_1, \mathbf{x}_2$, is proportional to $R^2(\mathbf{x}_1, \mathbf{x}_2)$, we conclude that although

a Schroedinger wave of low intensity can bring about large transfers of energy, such a process is (as in the usual interpretation) highly improbable.

In Appendix A of Paper II, we shall see that similar possibilities arise in connection with the interaction of the electromagnetic field with charged matter, so that electromagnetic waves can very rapidly transfer a full quantum of energy (and momentum) to an electron, even after they have spread out and fallen to a very low intensity. In this way, we shall explain the photoelectric effect and the Compton effect. Thus, we are able in our interpretation to understand by means of a causal and continuous model just those propertics of matter and light which seem most convincingly to require the assumption of discontinuity and incomplete determinism.

Before we discuss the process of interaction between two particles, we shall find it convenient to analyze the problem of an isolated single particle that happens to be in a nonstationary state. Because the field function ψ is a solution of Schroedinger's equation, we can linearly suppose stationary-state solutions of this equation and in this way obtain new solutions. As an illustration, let us consider a superposition of two solutions

$$\psi = C_1\psi_1(\mathbf{x})\exp\left(-iE_1t/\hbar\right) + C_2\psi_2(\mathbf{x})\exp\left(-iE_2t/\hbar\right),$$

where C_1, C_2, ψ_1, and ψ_2 are real. Thus we write $\psi_1 = R_1$, $\psi_2 = R_2$, and

$$\psi = \exp\left[-i\left(E_1+E_2\right)t/2\hbar\right]\left\{C_1R_1\exp\left[-i\left(E_1-E_2\right)t/2\hbar\right]\right. \\ \left. +C_2R_2\exp\left[i\left(E_1-E_2\right)t/2\hbar\right]\right\}.$$

Writing $\psi = R\exp(iS/h)$, we obtain

$$R^2 = {C_1}^2{R_1}^2(\mathbf{x}) + {C_2}^2{R_2}^2(\mathbf{x}) \\ + 2C_1C_2R_1(\mathbf{x})R_2(\mathbf{x})\cos\left[\left(F_1-F_2\right)t/2\hbar\right], \tag{19}$$

$$\tan\left\{\frac{S+\left(E_1-E_2\right)t/2}{\hbar}\right\} \\ = \frac{C_2R_2(\mathbf{x})-C_1R_1(\mathbf{x})}{C_2R_2(\mathbf{x})+C_1R_1(\mathbf{x})}\tan\left\{\frac{\left(E_1-E_2\right)t}{2\hbar}\right\}. \tag{20}$$

We see immediately that the particle experiences a "quantum-mechanical" potential, $U(\mathbf{x}) = (-\hbar/2m)\nabla^2R/R$, which fluctuates with angular frequency, $w = \left(E_1 - E_2\right)/\hbar$, and that the energy of this particle, $E = -\partial S/\partial l$, and its momentum $\mathbf{p} = \nabla S$, fluctuate with the same angular frequency. If the particle happens to enter a region of space where R is small, these fluctuations can become quite violent. We see then that, in general, the orbit of a particle in a nonstationary state is very irregular and complicated, resembling Brownian motion more closely than it resembles the smooth track of a planet around the sun.

If the system is isolated, these fluctuations will continue forever. The result is quite reasonable, since as is well known, a system can make a transition from one stationary state to another only if it can exchange en-

ergy with some other system. In order to treat the problem of transition between stationary states, we must therefore introduce another system capable of exchanging energy with the system of interest. In this section, we shall discuss the Franck-Hertz experiment, in which this other system consists of a bombarding particle. For the sake of illustration, let us suppose that we have hydrogen atoms of energy E_0 and wave function, $\psi_0(\mathbf{x})$, which are bombarded by particles that can be scattered inelastically, leaving the atom with energy E_n and wave function, $\psi_n(\mathbf{x})$.

We begin by writing down the initial wave function, $\Psi_1(\mathbf{x}, \mathbf{y}, t)$. The incident particle, whose coordinates are represented by y must be associated with a wave packet, which can be written as

$$f_0(\mathbf{y}, t) = \int e^{i\mathbf{k}\cdot\mathbf{y}} f(\mathbf{k} - \mathbf{k}_0) \exp\left(-i\hbar k^2 t/2m\right) d\mathbf{k} \tag{21}$$

The center of this packet occurs where the phase has an extremum as a function of $\mathbf{k}$, or where $\mathbf{y} = \hbar\mathbf{k}_0 t/m$.
Now, as in the usual interpretation, we begin by writing the incident wave function for the combined system as a product

$$\Psi_i = \psi_0(\mathbf{x}) \exp(-iE_0 l/\hbar) f_0(\mathbf{y}, t) \tag{22}$$

Let us now see how this wave function is to be understood in our interpretation of the theory. As pointed out in Sec. 6, the wave function is to be regarded as a mathematical representation of a six-dimensional but objectively real field, capable of producing forces that act on the particles. We also assume a six-dimensional representative point, described by the coordinates of the two particles, $\mathbf{x}$ and $\mathbf{y}$. We shall now see that when the combined wave function takes the form (22) involving a product of a function of $\mathbf{x}$ and a function of $\mathbf{y}$, the six-dimensional system can correctly be regarded as being made up of two independent three-dimentional subsystems. To prove this, we write
$\psi_0(\mathbf{x}) = R_0(\mathbf{x}) \exp[iS_0(\mathbf{x})/h]$ and

$$f_0(\mathbf{y}, l) = M_0(\mathbf{y}, l) \exp[iN_0(\mathbf{y}, t)/\hbar].$$

We then obtain for the particle velocities

$$d\mathbf{x}/dt = (1/m)\nabla S_0(\mathbf{x}); \quad d\mathbf{y}/dt = (1/m)\nabla N_0(y, t), \tag{23}$$

and for the "quantum-mechanical" potential

$$\begin{aligned} U &= -\frac{\hbar^2 \left\{\left(\nabla_x^2 + \nabla_y^2\right) R(\mathbf{x}, \mathbf{y})\right\}}{2mR(\mathbf{x}, \mathbf{y})} \\ &= \frac{-\hbar^2}{2m}\left\{\frac{\nabla^2 R_0(\mathbf{x})}{R_0(\mathbf{x})} + \frac{\nabla^2 M_0(\mathbf{y}, t)}{M_0(\mathbf{y}, t)}\right\} \end{aligned} \tag{24}$$

Thus, the particle velocities are independent and the "quantum-mechanical" potential reduces to a sum of terms, one involving only $\mathbf{x}$ and the other involving only $\mathbf{y}$. This means that the particles move independ-
ently. Moreover, the probability density, $P = {R_0}^2(\mathbf{x}) \times {M_0}^2(\mathbf{y}, t)$, is a product of a function of $\mathbf{x}$ and a function of $\mathbf{y}$, indicating that the distribution in $\mathbf{x}$ is statistically independent of that in $\mathbf{y}$. We conclude, then, that whenever the wave function can be expressed as a product of two factors, each involving only the coordinates of a single system, then the two systems are completely independent of each other.

As soon as the wave packet in $\mathbf{y}$ space reaches the neighborhood of the atom, the two systems begin to interact. If we solve Schroedinger's equation for the combined system, we obtain a wave function that can be expressed in terms of the following scries:

$$\Psi = \Psi_i + \sum_n \psi_n(\mathbf{x}) \exp(-iE_n l/\hbar) f_n(\mathbf{y}, t), \tag{25}$$

where the $f_n(y, t)$ are the expansion coefficients of the complete set of functions, $\psi_n(\mathbf{x})$. The asymptotic form of the wave function is [14]

$$\Psi = \Psi_i(\mathbf{x},\mathbf{y}) + \sum_n \psi_n(\mathbf{x}) \exp\left(-\frac{iE_n i}{h}\right) \int f(\mathbf{k}-\mathbf{k}_0) \times \frac{\exp\left[ik_n\cdot\mathbf{r} - \left(\hbar k_n^2/2n\right)t\right]}{r} g_n(\theta,\phi,\mathbf{k})d\mathbf{k} \tag{26}$$

where

$$\hbar^2 k_n^2/2m = \left(\hbar^2 k_0^2/2m\right) + E_0 - E_n \tag{27}$$

(conservation of energy).

The additional terms in the above equation represent outgoing wave packets, in which the particle speed, $\hbar k_n/m$, is correlated with the wave function, $\psi_n(\mathbf{x})$, representing the state in which the hydrogen atom is left. The center of the nth packet occurs at

$$r_n = (\hbar k_n/m)\, t. \tag{28}$$

It is clear that because the speed depends on the hydrogen atom quantum number, n, every one of these packets will eventually be separated by distances which are so large that this separation is classically describable.

When the wave function takes the form (25), the two particles system must be described as a single sixdimensional system and not as a sum of two independent three-dimensional subsystems, for at this time, if we try to express the wave function as $\psi(\mathbf{x},\mathbf{y}) = R(\mathbf{x},\mathbf{y}) \times \exp[iS(\mathbf{x},\mathbf{y})/h]$, we find that the resulting expressions for R and S depend on $\mathbf{x}$ and $\mathbf{y}$ in a very complicated way. The particle momenta, $\mathbf{p}_1 = \nabla_2 S(\mathbf{x},\mathbf{y})$ and $\mathbf{p}_2 = \nabla_y S(\mathbf{x},\mathbf{y})$, therefore become inextricably interdependent. The "quantum-mechanical" potential,

$$U = -\frac{h^2}{2mR(\mathbf{x},\mathbf{y})}\left(\nabla_x^2 R + \nabla_y^2 R\right)$$

ceases to be expressible as the sum of a term involving $\mathbf{x}$ and a term involving $\mathbf{y}$. The probability density,

$R^2(\mathbf{x},\mathbf{y})$ can no longer be written as a product of a function of $\mathbf{x}$ and a function of $\mathbf{y}$, from which we conclude that the probability distributions of the two particles are no longer statistically independent. Moreover, the motion of the particle is exceedingly complicated, because the expressions for R and S are somewhat analogous to those obtained in the simpler problem of a nonstationary state of a single particle [see Eqs. (19) and (20)]. In the region where the scattered waves $\psi_n(\mathbf{x})f_n(\mathbf{y},l)$ have an amplitude comparable with that of the incident wave, $\psi_0(\mathbf{x})f_0(\mathbf{y},t)$, the functions R and S, and therefore the "quantum-mechanical" potential and the particle momenta, undergo rapid and violent fluctuations, both as functions of position and of time. Because the quantum-mechanical potential has $R(\mathbf{x},\mathbf{y},t)$ in the denominator, these fluctuations may become very large in this region where R is small. If the particles happen to enter such a region, they may exchange very large quantities of energy and momentum in a very short time, even if the classical potential, $V(\mathbf{x},\mathbf{y})$ is very small. A small value of $V(\mathbf{x},\mathbf{y})$ implies, however, a correspondingly small value of the scattered wave amplitudes, $f_n(\mathbf{y},t)$. Since the fluctuations become large only in the region where the scattered wave amplitude is comparable with the incident wave amplitude and since the probability that the particles shall enter a given region of $\mathbf{x},\mathbf{y}$ space is proportional to $R^2(\mathbf{x},\mathbf{y})$, it is clear that a large transfer of energy is improbable (although still always possible) when $V(x,y)$ is small.

While interaction between the two particles takes place then, their orbits are subject to wild fluctuations. Eventually, however, the behavior of the system quiets down and becomes simple again. For after the wave function takes its asymptotic form (26), and the packets corresponding to different values of n have obtained classically describable separations, we can deduce

[814] N. F. Mott and H. S. W. Massey, The Theory of Atomic Collisions (Clarendon Press, Oxford, 1933).

that because the probability density is $|\psi|^2$, the outgoing particle must enter one of these packets and stay with that packet thereafter (since it does not enter the space between packets in which the probability density is negligibly different from zero). In the calculation of the particle velocities, $\mathrm{V}_1 = \nabla_x S/m$, $\mathrm{V}_2 = \nabla_y S/m$, and of the quantum-mechanical potential, $U = (-\hbar^2/2mR)\,(\nabla_x{}^2 R + \nabla_y{}^2 R\,)$, we can therefore ignore all parts of the wave function other than the one actually containing the outgoing particle. It follows that the system acts as if it had the wave function

$$\Psi_n = \psi_n(\mathbf{x}) \exp\left(\frac{iE_n t}{\hbar}\right) \int f\,(\mathbf{k}-\mathbf{k}_0) \times \frac{\exp\left\{i\left[\mathbf{k}_n\cdot\mathbf{r} - (\hbar {k_n}^2 t/2m)\,t\right]\right\}}{r} g_n(\theta,\phi,\mathbf{k})d\mathbf{k} \qquad (29)$$

where n denotes the packet actually containing the outgoing particle. This means that for all practical purposes the complete wave function (26) of the system may be replaced by Eq. (29), which corresponds to
an atomic electron in its nth quantum state, and to an outgoing particle with a correlated energy, $E_n{}' = \hbar^2 {k_n}^2/2m$. Berause the wave function is a product of a function of $\mathbf{x}$ and a function of $\mathbf{y}$, each system once again acts independently of the other. The wave function can now be renormalized because the multiplication of Ψ_n by a constant changes no physically significant quantity, such as the particle velocity or the "quantummechanical" potential. As shown in Sec. 5, when the electronic wave function is $\psi_n(\mathbf{x})\exp(-iE_n l/h)$, its energy must be E_n. Thus, we have obtained a description of how it comes about that the energy is always transferred in quanta of size $E_n - E_0$.

It should be noted that while the wave packets are still separating, the electron energy is not quantized, but has a continuous range of values, which fluctuate rapidly. It is only the final value of the energy, appearing after the interaction is over that must be quantized. A similar result is obtained in the usual interpretation if one notes that because of the uncertainty principle, the energy of either system can become definite only after enough time has elapsed to complete the scattering process. [15]

In principle, the actual packet entered by the outgoing particle could be predicted if we knew the initial position of both particles and, of course, the initial form of the wave function of the combined system. [16] In practice, however, the particle orbits are very complicated and very sensitively dependent on the precise values of these initial positions. Since we do not at present know how to measure these initial positions precisely, we cannot actually predict the outcome of such an interaction process. The best that we can do is to predict the probability that an outgoing particle enters the nth packet within a given range of solid angle, $d\Omega$, leaving the hydrogen atom in its nth quantum state. In doing this, we use the fact that the probability density in $\mathbf{x},\mathbf{y}$ space is $|\psi(\mathbf{x},\mathbf{y})|^2$ and that as long as we are restricted to the nth packet, we can replace the complete wave function (26) by the wave function (29), corresponding to the packet that actually contains the particle. Now, by definition, we have $\int |\psi_n(\mathbf{x})|^2\,d\mathbf{x} = 1$. The remaining integration of

$$\left| \int f\,(\mathbf{k}-\mathbf{k}_0)\,\frac{\exp\left\{i\left[k_n r - (\hbar k_n^2/2m)\,t\right]\right\}}{r} g_n(\theta,\phi,k)d\mathbf{k} \right|^2$$

over the region of space corresponding to the nth outgoing packet leads, however, to precisely the same probability of scattering as would have been obtained by applying the usual interpretation. We conclude, then, that if ψ satisfies Schroedinger's equation, that if $\mathbf{v} = \nabla S/\mathrm{m}$, and that if the probability density of particles is $P(\mathbf{x},\mathbf{y}) = R^2(\mathbf{x},\mathbf{y})$, we obtain in every respect

[8][15] See reference 2, Chapter 18, Sec. 19.

exactly the same physical predictions for this problem as are obtained when we use the usual interpretation.

There remains only one more problem; namely, to show that if the outgoing packets are subsequently brought together by some arrangement of matter that does not act on the atomic electron, the atomic electron and the scattered particle will continue to act independently. [17] To show that these two particles will continue to act independently, we note that in all practical applications, the outgoing particle soon interacts with some classically describable system. Such a system might consist, for example, of the host of atoms of the gas with which it collides or of the walls of a container. In any case, if the scattering process is ever to be observed, the outgoing particle must interact with a classically describable measuring apparatus. Now all classically describable systems have the property that they contain an enormous number of internal "thermodynamic" degrees of freedom that are inevitably excited when the outgoing particle interacts with the system. The wave function of the outgoing particle is then coupled to that of these internal thermodynamic degrees of freedom, which we represent as $y_1, y_2, \cdots y_s$. To denote this coupling, we write the wave function for the entire system as

$$\Psi = \sum_n \psi_n(\mathbf{x}) \exp\left(-iE_n l/h\right) f_n\left(\mathbf{y}, y_1, y_2 \cdots y_s\right). \tag{30}$$

Now, when the wave function takes this form, the overlapping of different packets in $\mathbf{y}$ space is not enough to produce interference between the different $\psi_n(\mathbf{x})$. To obtain such interference, it is necessary that the packets $f_n\left(\mathbf{y}, y_1, y_2, \cdots y_s\right)$ overlap in every one of the $S+3$ dimensions, $\mathbf{y}, y_1, y_2 \cdots y_s$. The reader will readily convince himself, by considering a typical case such as a collision of the outgoing particle with a metal wall, that it is overwhelmingly improbable that two of the packets $f_n\left(\mathbf{y}_1, y_1, y_2 \cdots y_s\right)$ will overlap with regard to every one of the internal thermodynamic coordinates, $y_1, y_2, \cdots y_s$, even if they are successfully made to overlap in $\mathbf{y}$ space. This is because each packet corresponds to a different particle velocity and to a different time of collision with the metal wall. Because the myriads of internal thermodynamic degrees of freedom are so chaotically complicated, it is very likely that as each of the n packets interacts with them, it will encounter different conditions, which will make the combined wave packet $f_n\left(\mathbf{y}, y_1, \cdots y_s\right)$ enter very different regions of $y_1, y_2 \cdots y_8$ space. Thus, for all practical purposes, we can ignore the possibility that if two of the packets are made to cross in y space, the motion either of the atomic electron or of the outgoing particle will be affected. [18]

26.3.8 8. Penetration of a Barrier

According to classical physics, a particle can never penetrate a potential barrier having a height greater than the particle kinetic energy. In the usual interpretation of the quantum theory, it is said to be able, with a small probability, to "leak" through the barrier. In our interpretation of the quantum theory, however, the potential provided by the Schroedinger ψ-field enables it to "ride" over the barrier, but only a few particles are likely to have trajectories that carry them all the way across without being turned around.

We shall merely sketch in general terms how the above results can be obtained. Since the motion of the particle is strongly affected by its ψ-field, we must first solve for this field with

[16] Note that in the usual interpretation one assumes that nothing determines the precise outcome of an individual scattering process. Instead, one assumes that all descriptions are inherently and unavoidably statistical (see Sec. 2).

[817] See reference 2, Chapter 22, Sec. 11, for a treatment of a similar problem.

[19] It should be noted that exactly the same problem anises in the usual interpretation of the quantum theory for (reference 16), for whenever two packets overlap, then even in the usual interpretation, the system must be regarded as, in some sense, covering the states corresponding to both packets simultaneously. See reference 2, Chapter 6 and Chapter 16, Sec. 25. Once two packets

the aid of "Schroedinger's equation." Initially, we have a wave packet incident on the potential barrier; and because the probability density is equal to $|\psi(x)|^2$, the particle is certain to be somewhere within this wave packet. When the wave packet strikes the repulsive barrier, the ψ-field undergoes rapid changes which can be calculated [19] if desired, but whose precise form does not interest us here. At this time, the "quantum-mechanical" potential, $U = (-\hbar^2/\,2m)\nabla^2 R/R$, undergoes rapid and violent fluctuations, analogous to those described in Sec. 7 in connection with Eqs. (19), (20), and (25). The particle orbit then becomes very complicated and, because the potential is time dependent, very sensitive to the precise initial relationship between the particle position and the center of the wave packet. Ultimately, however, the incident wave packet disappears and is replaced by two packets, one of them a reflected packet and the other a transmitted packet having a much smaller intensity. Because the probability density is $|\psi|^2$, the particle must end up in one of these packets. The other packet can, as shown in Sec. 7, subsequently be ignored. Since the reflected packet is usually so much stronger than the transmitted packet, we conclude that during the time when the packet is inside the barrier, most of the particle orbits must be turned around, as a result of the violent fluctuations in the "quantum-mechanical" potential.

26.3.9 9. Possible Modifications in Mathematical Formiuzation Leading to Experiviental Proof That New Interpretation

We have already seen in a number of cases and in Paper II we shall prove in general, that as long as we have obtained classically describable separations, then, both in the usual interpretation and in our interpretation the probability that there will be significant interference between them is so overwhelmingly small that it may be compared to the probability that a tea kettle placed on a fire will happen to freeze instead of boil. Thus, we may for all practical purposes neglect line possibility of interference between packets corresponding to the different possible energy states in which the hydrogen atom may be left.

[19] See, for example, reference 2, Chapter 11, Sec. 17, and Chapter 12, Sec. 18.

assume that ψ satisfies Schroedinger's equation, that $\mathbf{v} = \nabla S(\mathbf{x})/m$, and that we have a statistical ensemble with a probability density equal to $|\psi(\mathbf{x})|^2$, our interpretation of the quantum theory leads to physical results that are identical with those obtained from the usual interpretation. Evidence indicating the need for adopting our interpretation instead of the usual one could therefore come only from experiments, such as those involving phenomena associated with distances of the order of 10^{-13} cm or less, which are not now adequately understood in terms of the existing theory. In this paper we shall not, however, actually suggest any specific experimental methods of distinguishing between our interpretation and the usual one, but shall confine ourselves to demonstrating that such experiments are conceivable.

Now, there are an infinite number of ways of modifying the mathematical form of the theory that are consistent with our interpretation and not with the usual interpretation. We shall confine ourselves here, however, to suggesting two such modifications, which have already been indicated in Sec. 4, namely, to give up the assumption that $\mathbf{v}$ is necessarily equal to $\nabla S(\mathbf{x})/m$, and to give up the assumption that ψ must necessarily satisfy a homogeneous linear equation of the general type suggested by Schroedinger. As we shall see, giving up either of those first two assumptions will in general also require us to give up the assumption of a statistical ensemble of particles, with a probability density equal to $|\psi(\mathbf{x})|^2$.

We begin by noting that it is consistent with our interpretation to modify the equations of motion of a particle (8a) by adding any conceivable force term to the right-hand side. Let us, for the sake of illustration, consider a force that tends to make the difference, $\mathbf{p} - \nabla S(\mathbf{x})$, decay rapidly with time, with a mean decay time of the order of $\tau = 10^{-13}/c$ seconds, where c is the velocity of light. To achieve this result, we write

$$m\frac{d^2\mathbf{x}}{dt^2} = -\nabla\left\{V(\mathbf{x}) - \frac{\hbar^2}{2m}\frac{\nabla^2 R}{R}\right\} + \mathbf{f}(\mathbf{p} - \nabla S(\mathbf{x})) \tag{31}$$

where $\mathbf{f}(\mathbf{p}-\nabla S(\mathbf{x}))$ is assumed to be a function which vanishes when $\mathbf{p} = \nabla S(\mathbf{x})$ and more generally takes such a form that it implies a force tending to make $\mathbf{p} - \nabla S(\mathbf{x})$ decrease rapidly with the passage of time. It is clear, moreover, that f can be so chosen that it is large only in processes involving very short distances (where $\nabla S(\mathbf{x})$ should be large).

If the correct equations of motion resembled Eq. (31), then the usual interpretation would be applicable only over times much longer than τ, for only after such times have elapsed will the relation $\mathbf{p} = \nabla S(\mathbf{x})$ be a good approximation. Moreover, it is clear that such modifications of the theory cannot even be described in the usual interpretation, because they involve the precisely definable particle variables which are not postulated in the usual interpretation.

Let us now consider a modification that makes the equation governing ψ inhomogeneous. Such a modification is

$$i\hbar\psi/\partial t = H\psi + \xi\left(\mathbf{p} - \nabla S\left(\mathbf{x}_i\right)\right) \tag{32}$$

Here, H is the usual Hamiltonian operator, $\mathbf{x}_i$, represents the actual location of the particle, and ξ is a function that vanishes when $\mathbf{p} = \nabla S\left(\mathbf{x}_i\right)$. Now, if the particle equations are chosen, as in Eq. (31), to makc $\mathbf{p}-\nabla S\left(\mathbf{x}_i\right)$ decay rapidly with time, it follows that in atomic processes, the inhomogeneous term in Eq. (32) will become negligihly small, so that Schroedinger's equation is a good approximation. Nevertheless, in processes involving very short distances and very short times, the inhomogeneities would be important, and the ψ-field would, as in the case of the electromagnetic field, depend to some extent on the actual location of the particle.
It is clear that Eq. (32) is inconsistent with the usual interpretation of the theory. Moreover, we can contemplate further generalizations of Eq. (32), in the direction of introducing nonlinear terms that are large only for processes involving small distances. Since the usual interpretation is based on the hypothesis of linear superposition of "state vectors" in a Hilbert space, it follows that the usual interpretation could not be made consistent with such a nonlinear equation for a one-particle theory. In a many particle theory, opcrators can be introduced, satisfying a nonlinear generalization of Schroedinger's equation; but these must ultimately operate on wave functions that satisfy a linear homogeneous Schroedinger equation.

Finally, we repeat a point already made in Sec. 4, namely, that if the theory is generalized in any of the ways indicated here, the probability density of particles will cease to equal $|\psi(\mathbf{x})|^2$. Thus, experiments would become conceivable that distinguish between $|\psi(\mathbf{x})|^2$ and this probability; and in this way we could obtain an experimental proof that the usual interpretation, which gives $|\psi(\mathbf{x})|^2$ only a probability interpretation, must be inadequate. Moreover, we shall show in Paper II that modifications like those suggested here would permit the particle position and momentum to be measured simultaneously, so that the uncertainty principle could be violated.

26.4 III.3 Suggested Interpretation of the Quantum Theory in Terms of "Hidden" Variables", II

In this paper, we shall show how the theory of measurements is to be understood from the point of view of a physical interpretation of the quantum theory in terms of "hidden" variables, developed in a previous paper. We find that in principle, these "hidden" variables determine the precise results of each individual measurement process. In practice, however, in measurements that we now know how to carry out, the observing apparatus disturbs the observed system in an unpredictable and uncontrollable way, so that the uncertainty principle is obtained as a

practical limitation on the possible precision of measurements. This limitation is not, however, inherent in the conceptual structure of our interpretation. We shall see, for example, that simultaneous measurements of position and momentum having unlimited precision would in principle be possible if, as suggested in the previous paper, the mathematical formulation of the quantum theory needs to be modified at very short distances in certain
ways that are consistent with our interpretation but not with the usual interpretation.

We give a simple explanation of the origin of quantum-mechanical correlations of distant objects in the hypothetical experiment of Einstein, Podolsky, and Rosen, which was suggested by these authors as a criticism of the usual interpretation.

Finally, we show that von Neumann's proof that quantum theory is not consistent with hidden variables does not apply to our interpretation, because the hidden variables contemplated here depend both on the state of the measuring apparatus and the observed system and therefore go beyond certain of von Neumann's assumptions.

In two appendixes, we treat the problem of the electromagnetic field in our interpretation and answer certain additional objections which have arisen in the attempt to give a precise description for an individual system at the quantum level.

26.4.1 10. Summary and Conclusions

The usual interpretation of the quantum theory implies that we must renounce the possibility of describing an individual system in terms of a single precisely defined conceptual model. We have, however, proposed an alternative interpretation which does not imply such a renunciation, but which instead leads us to regard a quantum-mechanical system as a synthesis of a precisely definable particle and a precisely definable ψ-field which exerts a force on this particle. An experimental choice between these two interpretations cannot be made in a domain in which the present mathematical formulation of the quantum theory is a good approximation; but such a choice is conceivable in domains, such as those associated with dimensions of the order of 10^{-13} cm, where the extrapolation of the present theory seems to break down and where our suggested new interpretation can lead to completely different kinds of predictions.

At present, our suggested new interpretation provides a consistent alternative to the usual assumption that no objective and precisely definable description of reality is possible at the quantum level of accuracy. For, in our description, the problem of objective reality at the quantum level is at least in principle not fundamentally different from that at the classical level, although new problems of measurement of the properties of an individual system appear, which can be solved only with the aid of an improvement in the theory, such as the possible modifications in the nuclear domain suggested in Sec. 6. In this connection, we wish to point out that what we can measure depends not only on the type of apparatus that is available, but also on the existing theory, which determines the kind of inference that can
be used to connect the directly observable state of the apparatus with the state of the system of interest. In other words, our epistemology is determined to a large extent by the existing theory. It is therefore not wise to specify the possible forms of future theories in terms of purely epistomological limitations deduced from existing theories.

The development of the usual interpretation of the quantum theory seems to have been guided to a considerable extent by the principle of not postulating the possible existence of entities which cannot now be observed. This principle, which stems from a general philosophical point of view known during the nineteenth century as "positivism" or "empiricism" represents an extraphysical limitation on the possible kinds of theories that we shall choose to take into consideration. [7] The word "extraphysical" is used here advisedly, since we can in no way deduce, either from the experimental data of physics, or from its mathematical formulation, that it will necessarily remain forever impossible for us to observe entities whose existence

cannot now be observed. Now, there is no reason why an extraphysical general principle is necessarily to be avoided, since such principles could conceivably serve as useful working hypotheses. The particular extraphysical principle described above cannot, however, be said to be a good working hypothesis. For the history of scientific research is full of examples in which it was very fruitful indeed to assume that certain objects or elements might be real, long before any procedures were known which would permit them to be observed directly. The atomic theory is just such an example. For the possibility of the actual existence of individual atoms was first postulated in order to explain various macrophysical results which could, however, also be understood directly in terms of macrophysical concepts without the need for assuming the existence of atoms. Certain nineteenthcentury positivists (notably Mach) therefore insisted on purely philosophical grounds that it was incorrect to suppose that individual atoms actually existed, because they had never been observed as such. The atomic theory, they thought, should be regarded only as an interesting way of calculating various observable largescale properties of matter. Nevertheless, evidence for the existence of individual atoms was ultimately discovered by people who took the atomic hypothesis seriously enough to suppose that individual atoms might actually exist, even though no one had yet observed them. We may have here, perhaps, a close analogy to the usual interpretation of the quantum theory, which avoids considering the possibility that the wave function of an individual system may represent objective reality, because we cannot observe it with the aid of existing experiments and theories.

Finally, as an alternative to the positivist hypothesis of assigning reality only to that which we can now observe, we wish to prevent here another hypothesis, which we believe corresponds more closely to conclusions that can be drawn from general experience in actual scientific research. This hypothesis is based on the simple assumption that the world as a whole is objectively real and that, as far as we now know, it can correctly be regarded as having a precisely describable and analyzable structure of unlimited complexity. The pattern of this structure seems to be reflected completely but indirectly at every level, so that from experiments done at the level of size of human beings, it is very probably possible ultimately to draw inferences concerning the properties of the whole structure at all levels. We should never expect to obtain a complete theory of this structure, because there are almost certainly more elements in existence than we possibly can be aware of at any particular stage of scientific development. Any specified element, however, can in principle ultimately be discovered, but never all of them. Of course, we must avoid postulating a new element for each new phenomenon. But an equally serious mistake is to admit into the theory only those elements which can now be observed. For the purpose of a theory is not only to correlate the results of observations that we already know how to make, but also to suggest the need for new kinds of observations and to predict their results. In fact, the better a theory is able to suggest the need for new kinds of observations and to predict their results correctly, the more confidence we have that this theory is likely to be good representation of the actual properties of matter and not simply an empirical system especially chosen in such a way as to correlate a group of already known facts.

26.4.2 1. Introduction

IN a previous paper, [1] to which we shall hereafter refer as I, we have suggested an interpretation of the quantum theory in terms of "hidden" variables. We have shown that although this interpretation provides a conceptual framework that is broader than that of the usual interpretation, it permits of a set of three mutually consistent special assumptions, which lead to the same physical results as are obtained from the usual interpretation of the quantum theory.

[87] A leading nineteenth-century exponent of the positivist point of view was Mach. Modern positivists appear to have retreated from this extreme position, but its reflection still remains in the philosophical point of view implicitly adopted by a large number of modern theoretical physicists,

These three special assumptions are: (1) The ψ-field satisfies Schroedinger's equation. (2) If we write $\psi = R\exp(is/\hbar)$, then the particle momentum is restricted to $\mathbf{p} = \nabla S(\mathbf{x})$. (3) We have a statistical ensemble of particle positions, with a probability density, $P = |\psi(\mathbf{x})|^2$. If the above three special assumptions are not made, then one obtains a more general theory that cannot be made consistent with the usual interpretation. It was suggested in Paper I that such generalizations may actually be needed for an understanding of phenomena associated with distances of the order of 10^{-13} cm or less, but may produce changes of negligible importance in the atomic domain.

In this paper, we shall apply the interpretation of the quantum theory suggested in Paper I to the development of a theory of measurements in order to show that as long as one makes the special assumptions indicated above, one is led to the same predictions for all measurements as are obtained from the usual interpretation. In our interpretation, however, the uncertainty principle is regarded, not as an inherent limitation on the precision with which we can correctly conceive of the simultaneous definition of momentum and position, but rather as a practical limitation on the

precision with which these quantities can simultaneously be measured, arising from unpredictable and uncontrollable disturbances of the observed system by the measuring apparatus. If the theory needs to be generalized in the ways suggested in Paper I, Secs. 4 and 9, however, then these disturbances could in principle either be eliminated, or else be made subject to prediction and control, so that their effects could be corrected for. Our interpretation therefore demonstrates that measurements violating the uncertainty principle are at least conceivable.

26.4.3 Theory

2. QUANTUM THEORY OF MEASUREMENTS

We shall now show how the quantum theory of measurements is to be expressed in terms of our suggested interpretation of the quantum theory. [2]

In general, a measurement of any variable must always be carried out by means of an interaction of the system of interest with a suitable piece of measuring apparatus. The apparatus must be so constructed that any given state of the system of interest will lead to a certain range of states of the apparatus. Thus, the interaction introduces correlations between the state of the observed system and the state of the apparatus. The range of indefiniteness in this correlation may be called the uncertainty, or the error, in the measurement.

Let us now consider an observation designed to measure an arbitrary (hermitian) "observable" Q, associated with an electron. Let $\mathbf{x}$ represent the position of the electron, y that of the significant apparatus coordinate (or coordinates if there are more than one). Now, one can show [2] that it is enough to consider an impulsive measurement, i.e., a measurement utilizing a very strong interaction between apparatus and system

under observation, which lasts for so short a time that the changes of the apparatus and the system under observation that would have taken place in the absence of interaction can be neglected. Thus, at least while the interaction is taking place, we can neglect the parts of the Hamiltonian associated with the apparatus alone and with the observed system alone, and we need retain only the part of the Hamiltonian, H_I, representing the interaction. Moreover, if the Hamiltonian operator is chosen to be a function only of quantities that commute with Q, then

---

[8]

- Now at Universidade de So Paulo, Faculdade de Filosofia, Ciencias e Letras, So Paulo, Brasil.

[i] D. Bohm, Phys. Rev. 84, 106 (1951).

[82] For a treatment of how the theory of measurements can be carried out with the usual interpretation, see D. Bohm, Quantum Theory (Prentice Hall, Inc., New York, 1951), Chapter 22.

the interaction process will produce no uncontrollable changes in the observable, Q, but only in observables that do not commute with Q. In order that the apparatus and the system under observation shall be coupled, however, it is necessary that H_I shall also depend on operators involving y.

For the sake of illustration of the principles involved, we shall consider the following interaction Hamiltonian:

$$H_I - -aQp_v, \tag{1}$$

where a is a suitable constant and p_y is the momentum conjugate to y.

Now, in our interpretation, the system is to be described by a four-dimensional but objectively real wave field that is a function of $\mathbf{x}$ and y and by a corresponding four-dimensional representative point, specified by the coordinates, $\mathbf{x}$, of the electron and the coordinate, y, of the apparatus. Since the motion of the representative point is in part determined by forces produced by the ψ-field acting on both electron and apparatus variables, our first step in solving this problem is to calculate the ψ-field. This is done by solving Schroedinger's equation, with the appropriate boundary conditions on ψ.

Now, during interaction, Schroedinger's equation is approximated by

$$i\hbar\partial\Psi/\partial\iota = -aQp_y\Psi = (ia/\hbar)Q\partial\Psi/\partial y. \tag{2}$$

It is now convenient to expand Ψ in terms of the complete set $\psi_q(\mathbf{x})$ of eigenfunctions of the operator, Q, where q denotes an eigenvalue of Q. For the sake of simplicity, we assume that the spectrum of Q is discrete, although the results are easily generalized to a continuous spectrum. Denoting the expansion coefficients by $f_q(y,t)$, we obtain

$$\Psi(\mathbf{x},y,t) = \sum_q \psi_q(\mathbf{x})f_q(y,t). \tag{3}$$

Noting that $Q\psi_q(\mathbf{x}) = q\psi_q(\mathbf{x})$, we readily verify that Eq. (2) can now be reduced to the following series of equations for $f_q(y,t)$:

$$i\hbar\partial f_q(y,t)/\partial\iota = (ia/\hbar)qf_q(y,t). \tag{4}$$

If the initial value of $f_q(y,t)$ was ${f_q}^0(y)$, we obtain as a solution

$$f_q(y,t) = {f_q}^0\left(y - aqt/\hbar^2\right) \tag{5}$$

and

$$\Psi(\mathbf{x},y,t) = \sum_q \psi_q(\mathbf{x}){f_q}^0\left(y - aql/\hbar^2\right) \tag{6}$$

Now, initially the apparatus and the electron were independent. As shown in Paper I, Sec. 7, in our
interpretation (as in the usual interpretation), independent systems must have wave fields $\Psi(\mathbf{x},y,t)$ that are equal to a product of a function of $\mathbf{x}$ and a function of y. Initially, we therefore have

$$\Psi_0(\mathbf{x},y) = \psi_0(\mathbf{x})g_0(y) = g_0(y)\sum_q c_q\psi_q(\mathbf{x}) \tag{7}$$

where the c_q are the (unknown) expansion coefficients of $\psi_q(\mathbf{x})$, and $g_0(y)$ is the initial wave function of the apparatus coordinate, y. The function $g_0(y)$ will take the form of a packet. For the sake of convenience, we assume that this packet is centered at $y = 0$ and that its width is

Δy. Normally, because the apparatus is classically describable, the definition of this packet is far less precise than that allowed by the limits of precision set by the uncertainty principle.

From Eqs (7) and (3), we shall readily deduce that ${f_q}^0(y) = c_q g_0(y)$. When this value of ${f_q}^0(y)$ is inserted into Eq. (6), we obtain

$$\Psi(\mathbf{x}, y, i) = \sum_q \iota_q \dot{\psi}_q(\mathbf{x}) g_0\left(y - aqi/\hbar^2\right). \tag{8}$$

Equation (8) indicates already that the interaction has introduced a correlation between q and the apparatus coordinate, y. In order to show what this correlation means in our interpretation of the quantum theory, we shall use some arguments that have been developed in more detail in Paper I, Sec. 7, in connection with a similar problem involving the interaction of two particles in a scattering process. First we note that while the electron and the apparatus are interacting, the wave function (8) becomes very complicated, so that if it is expressed as

$$\Psi(\mathbf{x}, y, t) = R(\mathbf{x}, y, t) \exp[iS(\mathbf{x}, y, l)/\hbar]$$

then R and S undergo rapid oscillations both as a function of position and of time. From this we deduce that the "quantum-mechanical" potential,

$$U = \left(-\hbar^2/2mR\right)\left(\nabla_x^2 R + \partial^2 R/\partial y^2\right)$$

undergoes violent fluctuations, especially where R is small, and that the particle momenta, $\mathbf{p} = \nabla_x S(\mathbf{x}, y, t)$ and $p_y = \partial S(\mathbf{x}, y, t)/\partial y$, also undergo corresponding violent and extremely complicated fluctuations. Eventually, however, if the interaction continues long enough, the behavior of the system will become simpler because the packets $g_0\left(y - aqt/\hbar^2\right)$, corresponding to different values of q, will cease to overlap in y space. To prove this, we note that the center of the q th packet in y space is at

$$y = aql/\hbar^2; \quad \text{or} \quad q = \hbar^2 y/al. \tag{9}$$

If we denote the separation of adjacent values of q by δq, we then obtain for the separation of the centers of adjacent packets in y space

$$\delta y = ai\delta q/\tilde{h}^2. \tag{10}$$

It is clear that if the product of the strength of interaction a, and the duration of interaction, t, is large enough, then δy can be made much larger than the
width Δy of the packet. Then packets corresponding to different values of q will cease to overlap in y space and will, in fact, obtain separations large enough to be classically describable.

Because the probability density is equal to $|\Psi|^2$, we deduce that the apparatus variable, y, must finally enter one of the packets and remain with that packet thereafter (since it does not enter the intermediate space between packets in which the probability density is practically zero). Now, the packet entered by the apparatus variable y determines the actual result of the measurement, which the observer will obtain when he looks at the apparatus. The other packets can (as shown in Paper I, Sec. 7) be ignored, because they affect neither the quantum-mechanical potential acting on the particle coordinates $\mathbf{x}$ and y, nor the particle momenta, $\mathbf{p}_x = \nabla_x S$ and $p_y = \partial S/\partial y$. Moreover, the wave function can also be renormalized without affecting any of the above quantities. Thus, for all practical purposes, we can replace the complete wave function, Eq. (8), by a new renormalized wave function

$$\Psi(\mathbf{x}, y) = \dot{\psi}_q(\mathbf{x}) g_0\left(y - aqi/h^2\right) \tag{11}$$

where q now corresponds to the packet actually containing the apparatus variable, y. From this wave function, we can deduce, as shown in Paper I, Sec. 7, that the apparatus and the electron will subsequently behave independently. Moreover, by observing the approximate value of the apparatus coordinate within an error $\Delta y \ll \delta y$, we can deduce with the aid of Eq. (9) that since the electron wave function can for all practical purposes be regarded as $\psi_q(\mathbf{x})$, the observable, Q, must have the definite value, q. However, if the product, "atoq/ $\hbar^2$," appearing in Eqs. (8), (9), (10), and (11), had been less than Δy, then no clear mcasurcment of Q would have been possible, because packets corresponding to different q would have overlapped, and the measurement would not have had the requisite accuracy. [3]

Finally, we note that even if the apparatus packets dre subsequently caused to overlap, none of those conclusions will be altered. For the apparatus variable y will inevitably be coupled to a whole host of internal thermodynamic degrees of freedom, $y_1, y_2, \cdots y_s$, as a result of effects such as friction and brownian motion. As shown in Paper I, Sec. 7, interference between packets corresponding to different values of q would be possible only if the packets overlapped in the space of $y_1, y_2, \cdots y_s$, as well as in y space. Such an overlap, however, is so improbable that for all practical purposes, we can ignore the possibility that it will ever occur.

3. The ROLE OF PROBABILITY IN MEASUREMENTSTHE UNCERTAINTY PRINCIPLE

In principle, the final result of a measurement is determined by the initial form of the wave function of

the combined system, $\Psi^0(\mathbf{x}, y)$, and by the initial position of the electron particle, x_0, and the apparatus variable, y_0. In practice, however, as we have seen, the orbit fluctuates violently while interaction takes place, and is very sensitive to the precise initial values of $\mathbf{x}$ and y, which we can neither predict nor control. All that we can predict in practice is that in an ensemble of similar experiments performed under equivalent initial conditions, the probability density is $|\Psi(\mathbf{x}, y)|^2$. From this information, however, we are able to calculate only the probability that in an individual experiment, the result of a measurement of Q will be a specific number q. To obtain the probability of a given value of q, we need only integrate the above probability density over all $\mathbf{x}$ and over all values of y in the neighborhood of the q th packet. Because the packets do not overlap, the Ψ-field in this region is equal to $c_q \psi_q(\mathbf{x}) g_0 \left(y - aqt/\hbar^2\right)$ [see Eq. (8)]. Since, by definition, $\psi_q(\mathbf{x})$ and $g_0(y)$ are normalized, the total probability that a particle is in the q th packet is

$$P_q = |c_q|^2 . \tag{12}$$

The above is, however, just what is obtained from the usual interpretation. We conclude then that our interpretation is capable of leading in all possible experiments to identical predictions with those obtained from the usual interpretation (provided, or course, that we make the special assumptions indicated in the introduction).

Let us now see what a measurement of the observable, Q, implies with regard to the state of the electron particle and its Ψ-field. First, we note that the process of interaction with an apparatus designed to measure the observable, Q, effectively transforms the electron ψ-field from whatever it was before the measurement took place into an eigenfunction $\psi_q(\mathrm{x})$ of the operator Q. The precise value of q that comes out of this process is as we have seen, not, in general, completely predictable or controllable. If, however, the same measurement is repeated after the ψ-field has been transformed into $\psi_q(\mathbf{x})$, we can then predict that (as in the usual interpretation), the same value of q, and therefore the same wave function, $\psi_q(\mathbf{x})$, will be obtained again. If, however, we measure an observable " P " that does not commute with Q,

[83] A similar requirement is obtained in the usual interpretation. See reference 2, Chapter 22, Sec. 8.

then the results of this measurement are not, in practice, predictable or controllable. For as shown in Eq. (8), the Ψ-field after interaction with the measuring apparatus is now transformed into

$$\Psi(\mathbf{x}, z, l) = \sum_p a_{p,q}\phi_p(\mathbf{x})g_0\left(z - apl/\hbar^2\right) \tag{13}$$

where $\phi_p(\mathbf{x})$ is an eigenfunction of the operator, P, belonging to an eigenvalue, p, and where $a_{p,q}$ is an expansion coefficient defined by

$$\psi_q(\mathbf{x}) = \sum_p u_{p,q}\dot{\phi}_p(\overline{\mathbf{x}}) \tag{14}$$

Since the packets corresponding to different p ultimately become completely separate in z space, we deduce, as in the case of the measurement of Q, that
for all practical purposes, this wave function may be replaced by

$$\Psi = a_{pq}\phi_p(\mathbf{x})g_0\left(z - apl/\hbar^2\right)$$

where p now represents the packet actually entered by the apparatus coordinate, y. As in the case of measurement of Q, we readily show that the precise value of p that comes out of this experiment cannot be predicted or controlled and that the probability of a given value of p is equal to $|a_{pq}|^2$. This is, however, just what is obtained in the usual interpretation of this process.
It is clear that if two "observables," P and Q, do not commute, one cannot carry out a measurement of both simultaneously on the same system. The reason is that each measurement disturbs the system in a way that is incompatible with carrying out the process necessary for the measurement of the other. Thus, a measurement of P requires that wave field, ψ, shall become an eigenfunction of P, while a measurement of Q requires that it shall become an eigenfunction of Q. If P and Q do not commute, then by definition, no ψ-function can be simultaneously an eigenfunction of both. In this way, we understand in our interpretation why measure ments, of complementary quantities, must (as in the usual interpretation) necessarily be limited in their precision by the uncertainty principle.

4. PARTICLE POSITIONS AND MOMENTA AS "HIDDEN VARIABLES"

We have seen that in measurements that can now be carried out, we cannot make precise inferences about the particle position, but can say only that the particle must be somewhere in the region in which $|\psi|$ is appreciable. Similarly, the momentum of a particle that happens to be at the point, $\mathbf{x}$, is given by $\mathbf{p} = \nabla S(\mathbf{x})$, so that since $\mathbf{x}$ is not known, the precise value of $\mathbf{p}$ is also not, in general, inferrable. Hence, as long as we are restricted to making observations of this kind, the precise values of the particle position and momentum must, in general, be regarded as "hidden," since we cannot at present measure them. They are, however, connected with real and already observable properties of matter because (along with the ψ-field) they determine in principle the actual result of each individual measurement. By way of contrast, we recall here that in the usual interpretation of the theory, it is stated that although each measurement admittedly leads to a definite number, nothing determines the actual value of this number. The result of each measurement is assumed to arise somehow in an inherently indescribable way that is not subject to a detailed analysis. Only the statistical results are said to be predictable. In our interpretation, however, we assert that the at present "hidden" precisely definable particle positions and momenta determine the results of each individual measurement process, but in a way whose precise details are so complicated and uncontrollable, and so little known, that one must for all practical purposes

restrict oneself to a statistical description of the connection between the values of these variables and the directly observable results of measurements. Thus, we are unable at present to obtain direct experimental evidence for the existence of precisely definable particle positions and momenta.

5. "OBSERVABLES" OF USUAL INTERPRETATION ARE NOT A COMPLETE DESCRIPTION OF SYSTEM IN OUR INTERPRETATION

We have seen in Sec. 3 that in the measurement of an "observable," Q, we cannot obtain enough information to provide a complete specification of the state of an electron, because we cannot infer the precisely defined values of the particle momentum and position, which are, for example, needed if we wish to make precise predictions about the future behavior of the electron. Moreover, the process of measuring an observable does not provide any unambiguous information about the state that existed before the measurement took place; for in such a measurement, the ψ-field is transformed into an in practice unpredictable and uncontrollable eigenfunction, $\dot{\psi}_q(\mathbf{x})$, of the measured "observable" Q. This means that the measurement of an "observable" is not really a measurement of any physical property belonging to the observed system alone. Instead, the value of an "observable" measures only an incompletely predictable and controllable potentiality belonging just as much to the measuring apparatus as to the observed system itself. [4] At best, such a measurement provides unambiguous information only at a classical level of accuracy, where the disturbance of the ψ-field by the measuring apparatus can be neglected. The usual "observables" are therefore not what we ought to try to measure at a quantum level of accuracy. In Sec. 6, we shall see that it is conceivable that we may be able to carry out new kinds of measurements, providing information not about "observables" having a very ambiguous significance, but rather about physically significant properties of a system, such as the actual values of the particle position and momentum.

As an example of the rather indirect and ambiguous significance of the "observable," we may consider the problem of measuring the momentum of an electron. Now, in the usual interpretation, it is stated that one can always measure the momentum "observable" without changing the value of the momentum. The result is said, for example, to be obtainable with the aid of an impulsive interaction involving only operators which commute with the momentum operator, $\mathbf{p}_x$. To represent such a measurement, we could choose $H_I = -ap_xp_y$ in Eq. (1). In our interpretation, however, we cannot in general conclude that such an interaction will enable us to measure the actual particle momentum without changing its value. In fact, in our interpretation, a measurement of particle momentum that does not change the value of this momentum is possible only if the ψ-field initially takes the special form, $\exp(i\mathbf{p}\cdot\mathbf{x}/\hbar)$. If, however, ψ initially takes its most general possible form,

$$\psi = \sum_p a_1\mathbf{p}\exp(i\mathbf{p}\cdot\mathbf{x}/\hbar), \tag{15}$$

then as we have seen in Secs. 2 and 3, the process of measuring the "observable" p_x will effectively transform the ψ-field of the electron into

$$\exp\left(ip_x/\hbar\right) \tag{16}$$

with a probability $|a_p|^2$ that a given value of $\dot{p}_x$ will be obtained. When the ψ-field is altered in this way, large quantities of momentum can be transferred to the particle by the changing ψ field, even though the interaction Hamiltonian, H_r, commutes with the momentum operator, $\mathbf{p}$.

[84] Even in the usual interpretation, an observation must be regarded as yielding a measure of such a potentiality. See reference 2, Chapter 6, Sec. 9.

As an example, we may consider a stationary state of an atom, of zero angular momentum. As shown in Paper I, Sec. 5, the ψ-field for such a state is real, so that we obtain

$$\mathbf{p} = \nabla S = 0$$

Thus, the particle is at rest. Nevertheless, we see from Eqs. (14) and (15) that if the momentum "observable" is measured, a large value of this "observable" may be obtained if the ψ-field happens to have a large fourier coefficient, a_p, for a high value of $\mathbf{p}$. The reason is that in the process of interaction with the measuring apparatus, the ψ-field is altered in such a way that it can give the electron particle a correspondingly large momentum, thus transforming some of the potential energy of interaction of the particle with its ψ-field into kinetic energy.

A more striking illustration of the points discussed above is afforded by the problem of a "free" particle contained between two impenetrable and perfectly reflecting walls, separated by a distance L. For this case, the spatial part of the ψ-field is

$$\psi = \sin(2\pi nx/L),$$

where n is an integer and the energy of the electron is

$$E = (1/2m)(nh/L)^2.$$

Because the ψ-field is real, we deduce that the particle is at rest.

Now, at first sight, it may seem puzzling that a particle having a high energy should be at rest in the empty space between two walls. Let us recall, however, that the space is not rcally cmpty, but contains an objectively real ψ-field that can act on the particle. Such an action is analogous to (but of course not identical with) the action of an electromagnetic field, which could create non-uniform motion of the particle in this apparently "empty" enclosure. We observe that in our problem, the ψ-field is able to bring the particle to rest and to transform the entire kinetic energy into
potential energy of interaction with the ψ-field. To prove this, we evaluate the "quantum-mechanical potential" for this ψ-field

$$U = \frac{-\hbar^2}{2m}\frac{\nabla^2 R}{R} = \frac{-\hbar^2}{2m}\frac{\nabla^2 \psi}{\psi} = \frac{1}{2m}\left(\frac{nh}{L}\right)^2$$

and note that it is precisely equal to the total energy, E.

Now, as we have seen, any measurement of the momentum "observable" must change the ψ-field in such a way that in general some (and in our case, all) of this potential energy is transformed into kinetic energy. We may use as an illustration of this general result a very simple specific method of measuring the momentum "observable," namely, to remove the confining walls suddenly and then to measure the distance moved by the particle after a fairly long time. We can compute the momentum by dividing this distance by the time of transit. If (as in the usual interpretation of the quantum theory) we assume that the electron is "free," then we conclude that the process of removing the walls should not appreciably change the momentum if we do it fast enough, for the probability that the particle is near a wall when this happens can then in principle be made arbitrarily small. In our interpretation, however, the removal of the walls alters the particle momentum indirectly, because of its effect on the ψ-field, which acts on the particle. Thus, after the walls are removed, two wave packets moving in opposite directions begin to form, and ultimately they become completely separate in space. Because the probability density is $|\psi|^2$, we deduce that the particle must end up in one packet or the other. Moreover, the reader will readily convince himself that the particle momentum will be very close to $\pm nh/L$, the sign depending on which packet the particle actually enters. As in Sec. (2), the packet not containing the particle can subsequently be ignored. In principle, the final

particle momentum is determined by the initial form of the ψ-field and by the initial particle position. Since we do not in practice know the latter, we can at best predict a probability of $\frac{1}{2}$ that the particle ends up in either packet. We conclude then that this measurement of the momentum "observable" leads to the same result as is predicted in the usual interpretation. However, the actual particle momentum existing before the measurement took place is quite different from the numerical value obtained for the momentum "observable," which, in the usual interpretation, is called the "momentum."

6. ON The POSSIBILITY OF MEASUREMENTS OF UNLIMITED PRECISION

We have seen that the so-called "observables" do not measure any very readily interpretable properties of a system. For example, the momentum "observable" has in general no simple relation to the actual particle momentum. It may therefore be fruitful to consider
how we might try to measure properties which, according to our interpretation, are (along with the ψ-field) the physically significant properties of an electron, namely, the actual particle position and momentum. In connection with this problem, we shall show that if, as suggested in Paper I, Secs. 4 and 9, we give up the three mutually consistent special assumptions leading to the same results as those of the usual interpretation of the quantum theory, then in our interpretation, the particle position and momentum can in principle be measured simultaneously with unlimited precision.

Now, for our purposes, it will be adequate to show that precise predictions of the future behavior of a system are in principle possible. In our interpretation, a sufficient condition for precise predictions is as we have seen that we shall be able to prepare a system in a state in which the ψ-field and the initial particle position and momentum are precisely known. We have shown that it is possible, by measuring the "observable," Q, with the aid of methods that are now available, to prepare a state in which the ψ-field is effectively transformed into a known form, $\psi_q(\mathbf{x})$; but we cannot in general predict or control the precise position and momentum of the particle. If we could now measure the position and momentum of the particle without altering the ψ-field, then precise predictions would be possible. However, the results of Secs. 2, 3, and 4 prove that as long as the three special assumptions indicated above are valid, we cannot measure the particle position more accurately without effectively transforming the ψ-function into an incompletely predictable and controllable packet that is much more localized than $\psi_q(\mathbf{x})$. Thus, efforts to obtain more precise definition of the state of the system will be defeated. But it is clear that the difficulty originates in the circumstance that the potential energy of interaction between electron and apparatus, $V(x, y)$, plays two roles. For it not only introduces a direct interaction between the two particles, proportional in strength to $V(x, y)$ itself, but it introduces an indirect interaction between these particles, because this potential also appears in the equation governing the ψ-field. This indirect interaction may involve rapid and violent fluctuations, even when $V(\mathbf{x}, y)$ is small. Thus, we are led to lose control of the effects of this interaction, because no matter how small $V(\mathbf{x}, y)$ is, very large and chaotically complicated disturbances in the particle motion may occur.

If, however, we give up the three special assumptions mentioned previously, then it is not inherent in our conceptual structure that every interaction between particles must inevitably also produce large and uncontrollable changes in the ψ-field. Thus, in Paper I, Eq. (31), we give an example in which we postulate a force acting on a particle that is not necessarily accompanied by a corresponding change in the ψ-field. Equation (31), Paper I, is concerned only with a oneparticle system, but similar assumptions can be made for systems of two or more particles. In the absence of
any specific theory, our interpretation permits an infinite number of kinds of such modifications, which can be chosen to be important at small distances but negligible in the atomic domain. For the sake of illustration, suppose that it should turn out that in certain processes connected

with very small distances, the force acting on the apparatus variable is

$$F_y = ax$$

where a is a constant. Now if " a " is made large enough so that the interaction is impulsive, we can neglect all changes in y that are brought about by the forces that would have been present in the absence of this interaction. Moreover, for the sake of illustration of the principles involved, we are permitted to make the assumption, consistent with our interpretation, that the force on the electron is zero. The equation of motion of y is then

$$\ddot{y} = ax/m.$$

The solution is

$$y - y_0 = \left(axt^2/2m\right) + \dot{y}_0 t$$

where $\dot{y}_0$ is the initial velocity of the apparatus variable and y_0 its initial position. Now, if the product, at^2, is large enough, then $y - y_0$ can be made much larger than the uncertainty in y arising from the uncertainty of y_0, and the uncertainty of $\dot{y}_0$. Thus, $y - y_0$ will be determined primarily by the particle position, x. In this way, it is conceivable that we could obtain a measurement of x that does not significantly change $x, \dot{x}$, or the ψ-function. The particle momentum can then be obtained from the relation, $p = \nabla S(\mathbf{x})$, where $S/\hbar$ is the phase of the ψ-function. Thus, precise predictions would in principle be possible.

7. The ORIGIN OF The STATISTICAL ENSEMBLE IN The QUANTUM THEORY

We shall now see that even if, because of a failure of the three special assumptions mentioned in Secs. 1 and 6, we are able to determine the particle positions and momenta precisely, we shall nevertheless ultimately obtain a statistical ensemble again at the atomic level, with a probability density equal to $|\psi|^2$. The need for such an ensemble arises from the chaotically complicated character of the coupling between the electron and classical systems, such as volumes of gas, walls of containers, pieces of measuring apparatus, etc., with which this particle must inevitably in practice interact. For as we have seen in Sec. 2, and in Paper I, Sec. 7, during the course of such an interaction, the "quantummechanical" potential undergoes violent and rapid fluctuations, which tend to make the particle orbit wander over the whole region in which the ψ-field is appreciable. Moreover, these fluctuations are further complicated by the effects of molecular chaos in the very large number of internal thermodynamic degrees of freedom of these classically describable systems, which are inevitably excited in any interaction process.

Thus, even if the initial particle variables were well defined, we should soon in practice lose all possibility of following the particle motion and would be forced to have recourse to some kind of statistical theory. The only question that remains is to show why the probability density that ultimately comes about should be equal to $|\psi|^2$ and not to some other quantity.

To answer this question, we first note that a statistical ensemble with a probability density $|\psi(\mathbf{x})|^2$ has the property that under the action of forces which prevail at the atomic level, where our three special assumptions are satisfied, it will be preserved by the equations of motion of the particles, once it comcs into existence. There remains only the problem of showing that an arbitrary deviation from this ensemble tends, under the action of the chaotically complicated forces described in the previous paragraph, to decay into an ensemble with a probability density of $|\psi(\mathbf{x})|^2$. This problem is very similar to that of proving Boltzmann's H theorem, which shows in connection with a different but analogous problem that an arbitrary ensemble tends as a result of molecular chaos to decay into an equilibrium Gibbs ensemble. We shall not carry out a

detailed proof here, but we merely suggest that it seems plausible that one could along similar lines prove that in our problem, an arbitrary ensemble tends to decay into an ensemble with a density of $|\psi(x)|^2$. These arguments indicate that in our interpretation, quantum fluctuations and classical fluctuations (such as the Brownian motion) have basically the same origin; viz., the chaotically complicated character of motion at the microscopic level.

8. The HYPOTHETICAL EXPERIMENT OF EINSTEIN, PODOLSKY, AND ROSEN

The hypothetical experiment of Einstein, Podolsky, and Rosen [5] is based on the fact that if we have two particles, the sum of their momenta, $p = p_1 + p_2$, commutes with the difference of their positions, $\xi = x_1 - x_2$. We can therefore define a wave function in which p is zcro, while ξ has a given value, a. Such a wave function is

$$\psi = \delta\left(x_1 - x_2 - a\right). \tag{17}$$

In the usual interpretation of the quantum theory, $p_1 - p_2$ and $x_1 + x_2$ are completely undetermined in a system having the above wave function.

The whole experiment centers on the fact that an observer has a choice of measuring either the momentum or the position of any one of the two particles. Whichever of these quantities he measures, he will be able to infer a definite value of the corresponding variable in the other particle, because of the fact that the above wave function implies correlations between variables belonging to each particle. Thus, if he obtains a position x_1 for the first particle, he can infer a position of

$x_2 = a - x_1$ for the second particle; but he loses all possibility of making any inferences about the momenta of either particle. On the other hand, if he measures the momentum of the first particle and obtains a value of p_1, he can infer a value of $p_2 = -p_1$ for the momentum of the second particle; but he loses all possibility of making any inferences about the position of either particle. Now, Einstein, Podolsky, and Rosen believe that this result is itself probably correct, but they do not belicve that quantum theory as usually interpreted can give a complete description of how these correlations are propagated. Thus, if these were classical particles, we could easily understand the propagation of correlations because each particle would then simply move with a velocity opposite to that of the other. But in the usual interpretation of quantum theory, there is no similar conceptual model showing in detail how the second particle, which is not in any way supposed to interact with the first particle, is nevertheless able to obtain either an uncontrollable disturbance of its position or an uncontrollable disturbance of its momentum depending on what kind of measurement the observer decided to carry out on the first particle. Bohr's point of view is, however, that no such model should be sought and that we should merely accept the fact that these correlations somehow manage to appear. We must note, of course, that the quantum-mechanical description of these processes will always be consistent, even though it gives us no precisely definable means of describing and analyzing the relationships between the classically describable phenomena appearing in various pieces of measuring apparatus.

In our suggested new interpretation of the quantum theory, however, we can describe this experiment in terms of a single precisely definable conceptual model, for we now describe the system in terms of a combination of a six-dimensional wave field and a precisely definable trajectory in a six-dimensional space (see Paper I, Sec. 6). If the wave function is initially equal to Eq. (17), then since the phase vanishes, the particles are both at rest. Their possible positions are, however, described by an ensemble, in which $x_1 - x_2 = a$. Now, if we measure the position of the first particle, we introduce uncontrollable fluctuations in the wave function for

[85] Einstein, Podolsky, and Rosen, Phys. Rev. 47, 777 (1935).

the entire system, which, through the "quantum-mechanical" forces, bring about corresponding uncontrollable fluctuations in the momentum of each particle. Similarly, if we measure the momentum of the first particle, uncontrollable fluctuations in the wave function for the system bring about, through the "quantum-mechanical" forces, corresponding uncontrollable changes in the position of each particle. Thus, the "quantum-mechanical" forces may be said to transmit uncontrollable disturbances instantaneously from one particle to another through the medium of the ψ-field.

What does this transmission of forces at an infinite rate mean? In nonrelativistic theory, it certainly causes
no difficulties. In a relativistic theory, however, the problem is more complicated. We first note that as long as the three special assumptions mentioned in Sec. 2 are valid, our interpretation can give rise to no inconsistencies with relativity, because it leads to precisely the same predictions for all physical processes as are obtained from the usual interpretation (which is known to be consistent with relativity). The reason why no contradictions with relativity arise in our interpretation despite the instantaneous transmission of momentum between particles is that no signal can be carried in this way. For such a transmission of momentum could constitute a signal only if there were some practical means of determining precisely what the second particle would have done if the first particle had not been observed; and as we have seen, this information cannot be obtained as long as the present form of the quantum theory is valid. To obtain such information, we require conditions (such as might perhaps exist in connection with distances of the order of 10^{13} cm) under which the usual form of the quantum theory breaks down (see Sec. 6), so that the positions and momenta of the particles can be determined simultancously and precisely. If such conditions should exist, then there are two ways in which contradictions might be avoided. First, the more general physical laws appropriate to the new domains may be such that they do not permit the transmission of controllable aspects of interparticle forces faster than light. In this way, Lorentz covariance could be preserved. Secondly, it is possible that the application of the usual criteria of Lorentz covariance may not be appropriate when the usual interpretation of quantum theory breaks down. Even in connection with gravitational theory, general relativity indicates that the limitation of speeds to the velocity of light does not necessarily hold universally. If we adopt the spirit of general relativity, which is to seek to make the properties of space dependent on the properties of the matter that moves in this space, then it is quite conceivable that the metric, and therefore the limiting velocity, may depend on the ψ-field as well as on the gravitational tensor $g^{\mu,r}$. In the classical limit, the dependence on the ψ-field could be neglected, and we would get the usual form of covariance. In any case, it can hardly be said that we have a solid experimental basis for requiring the same form of covariance at very short distances that we require at ordinary distances.

To sum up, we may assert that wherever the present form of the quantum theory is correct, our interpretation cannot lead to inconsistencies with relativity. In the domains where the present theory breaks down, there are several possible ways in which our interpretation could continue to treat the problem of covariance consistently. The attempt to maintain a consistent treatment of covariance in this problem might perhaps serve as an important heuristic principle in the search for new physical laws.

9. ON VON NEUMANN'S DEMONGTRATION THAT QUANTUM THEORY IS INCONSISTENT WITH HIDDEN VARIABLES

Von Neumann [6] has studicd the following question: "If the present mathematical formulation of the quantum theory and its usual probability intepretation are assumed to lead to absolutely correct results for every experiment that can ever be done, can quantummechanical probabilities be understood in terms of any conceivable distribution over hidden parameters?" Von Neumann answers this question in the negative. His conclusions are subject, however, to

the criticism that in his proof he has implicitly restricted himself to an excessively narrow class of hidden parameters and in this way has excluded from consideration precisely those types of hidden parameters which have been proposed in this paper.

To demonstrate the above statements, we summarize Von Neumann's proof briefly. This proof (which begins on p. 167 of his book), shows that the usual quantummechanical rules of calculating probabilities imply that there can be no "dispersionless states," i.e., states in which the values of all possible observables are simultaneously determined by physical parameters associated with the observed system. For example, if we consider two noncommuting observables, p and q, then Von Neumann shows that it would be inconsistent with the usual rules of calculating quantum-mechanical probabilities to assume that there were in the observed system a set of hidden parameters which simultaneously determined the results of measurements of position and momentum "observables." With this conclusion, we are in agreement. However, in our suggested new interpretation of the theory, the so-called "observables" are, as we have seen in Sec. 5, not properties belonging to the observed system alone, but instead potentialities whose precise development depends just as much on the observing apparatus as on the observed system. In fact, when we measure the momentum "observable," the final result is determined by hidden parameters in the momentum-measuring device as well as by hidden parameters in the observed electron. Similarly, when we measure the position "observable," the final result is determined in part by hidden parameters in the position-measuring device. Thus, the statistical distribution of "hidden" parameters to be used in calculating averages in a momentum measurement is different from the distribution to be used in calculating averages in a position measurement. Von Neumann's proof (see p. 171 in his book) that no single distribution of hidden parameters could be consistent with the results of the quantum theory is therefore irrelevant here, since in our interpretation of measurements of the type that can now be carried out, the distribution of hidden parameters varies in accordance with the different mutually exclusive experimental

arrangements of matter that must be used in making different kinds of measurements. In this point, we are in agreement with Bohr, who repeatedly stresses the fundamental role of the measuring apparatus as an inseparable part of the observed system. We differ from Bohr, however, in that we have proposed a method by which the role of the apparatus can be analyzed and described in principle in a precise way, whereas Bohr asserts that a precise conception of the details of the measurement process is as a matter of principle unattainable.

Finally, we wish to stress that the conclusions drawn thus far refer only to the measurement of the so-called "observables" carried out by the methods that are now available. If the quantum theory needs to be modified at small distances, then, as suggested in Sec. 6, precise measurements can in principle be made of the actual position and momentum of a particle. Here, it should be noted that Von Neumann's theorem is likewise irrelevant, this time because we are going beyond the assumption of the unlimited validity of the present general form of quantum theory, which plays an integral part in his proof.

26.4.4 Appendices

APPENDIX A. PHOTOELECTRIC AND COMPTON EFFECTS

In this appendix, we shall show how the electromagnetic field is to be described in our new interpretation, with the purpose of making possible a treatment of the photoelectric and Compton effects. For our purposes, it is adequate to restrict ourselves to a gauge in which $\operatorname{div} \mathbf{A} = 0$, and to consider only the transverse part of the electromagnetic field, for in this

[86] J. von Neumann, Mathematische Grundlagen der Quantenmechanik (Verlag. Julius Springer, Berlin, 1932).

gauge, the longitudinal part of the field can be expressed through Poisson's equation entirely in terms of the charge density. The Fourier analysis of the vector potential is then

$$\mathbf{A}(\mathbf{x}) = (4\pi/V)^{\frac{1}{2}} \sum_{\mathbf{k},\mu} \epsilon_{\mathbf{k},\mu} q_{\mathbf{k},\mu} e^{i\mathbf{k}\cdot\mathbf{x}} \tag{A1}$$

with

$$q^*_{k,\mu} = q_{-k,\mu}$$

The $q_{k,\mu}$ are coordinates of the electromagnetic field, associated with oscillations of wave number, $\mathbf{k}$, and polarization direction, μ, where $\varepsilon_{\mathrm{k},\mu}$ is a unit vector normal to $\mathbf{k}$ and μ runs over two indices, corresponding to a pair of orthogonal directions of polarization. V is the volume of the box, which is assumed to be very large.

We also introduce the momenta $\prod_{k,\mu} = \partial {q_{k,\mu}}^*/\partial t$, canonically conjugate [8] to the $q_{k,\mu}$. We have for the transverse part of the electric field

$$\mathfrak{G}(\mathbf{x}) = -\frac{1}{c}\frac{\partial \mathbf{A}(\mathbf{x})}{\partial t} = -\left(\frac{4\pi}{Vc^2}\right)^{\frac{1}{k}} \sum_{\mathbf{k},\mu} \epsilon_{\mathbf{k},\mu} {\Pi_{\mathbf{k},\mu}}^* e^{i\mathbf{k}\cdot\mathbf{x}} \tag{A2}$$

and for the magnetic field

$$\mathfrak{G}(\mathbf{x}) = \nabla \times \mathbf{A} = -(4\pi/V)^{\frac{1}{2}} i \sum_{\mathbf{k},\mu} (\mathbf{k} \times \epsilon_{\mathbf{k},\mu})\, q_{\mathbf{k},\mu} e^{i\mathbf{k}\cdot\mathbf{x}} \tag{A3}$$

The Hamiltonian of the radiation field corresponds to a collection of independent harmonic oscillators, each with angular frequency, $\omega = kc$. This Hamiltonian is

$$H^{(R)} = \sum_{\mathrm{k},\mu} \left(\prod_{\mathrm{k},\mu} \overset{*}{\prod_{\mathrm{k},\mu}} + k^2 c^2 q_{\mathrm{k},\mu} q^*_{\mathrm{k},\mu} \right) \tag{A4}$$

Now, in our interpretation of the quantum theory, the quantity $q_{\mathrm{k},\mu}$ is assumed to refer to the actual value of the $\mathbf{k},\mu$ Fourier component of the vector potential. As in the case of the electron, however, there is present an objectively real superfield that is a function of all the electromagnetic field coordinates $q_{\mathrm{k},\mu}$. Thus, we have

$$\Psi^{(R)} = \Psi^{(R)}\left(\cdots q_{\mathrm{k},\mu} \cdots\right) \tag{A5}$$

Writing $\Psi^{(R)} = R\exp(iS/\hbar)$, we obtain (in analogy with Paper I, Sec. 4)

$$\partial q_{\mathrm{k},\mu}/\partial t = \overset{*}{\prod_{\mathrm{k},\mu}} = \partial s/\partial q^*_{\mathrm{k},\mu} \tag{A6}$$

The function $R\left(\cdots q_{k,\mu} \cdots\right)$ has two interpretations. First, it defines an additional quantum-mechanical term appearing in Maxwell's equations. To see the origin of this term, let us write the generalized Hamil-ton-Jacobi equation of the electromagnetic field, analogous to Paper I, Eq. (4),

$$\frac{\partial s}{\partial t} + \sum_{\mathrm{k},\mu} \frac{\partial s}{\partial q_{\mathrm{k},\mu}} \frac{\partial s}{\partial q^*_{\mathrm{k},\mu}} + \sum_{\mathrm{k},\mu} (kc)^2 q_{\mathrm{k},\mu} q^*_{\mathrm{k},\mu} - \frac{\hbar^2}{2R} \sum_{\mathrm{k},\mu} \frac{\partial^2 R\left(\cdots q_{\mathrm{k},\mu} \cdots\right)}{\partial q_{\mathrm{k},\mu} \partial q^*_{\mathrm{k},\mu}} = 0 \tag{A7}$$

The equation of motion of $q_{k,\mu}$, derived from the Hamiltonian implied by Eq. (A7) becomes

$$\ddot{q}_{\mathrm{k},\mu} + k^2 c^2 q_{\mathrm{k},\mu} = \frac{\partial}{\partial q_{\mathrm{k},\mu}{}^*} \left(\frac{\hbar^2}{2R} \sum_{\mathrm{k}',\mu'} \frac{\partial^2 R}{\partial q_{\mathrm{k}',\mu'} \partial q_{\mathrm{k}',\mu'}{}^*} \right) \tag{A8}$$

Since Maxwell's equations for empty space follow when the right-hand side is zero, we see that the "quantum-mechanical" terms can profoundly modify the behavior of the electromagnetic field. In fact, it is this modification which will contribute to the explanation of the ability of an oscillator, $q_{k,\mu}$, to transfer large quantities of energy and momentum rapidly even when $q_{k,\mu}$ is very small, for when $q_{k,\mu}$ is small, the right-hand side of Eq. (A8) may become very large.

The second interpretation of R is that as in Paper I, Eq. (5), it defines a conserved probability density that each of the $q_{k,\mu}$ has a certain specified value. From this fact, we see that although large transfers of energy and momentum to a radiation oscillator can occur in a short time when R is small, the probability of such a process is (as was also shown in Paper I, Sec. 7) very small.

In the lowest state (when no quanta are present) every oscillator is in the ground state. The super wave fields is then

$$\Psi_0^{(R)} = \exp\left[-\sum_{\mathrm{k},\mu} \left(kcq_{\mathrm{k},\mu} q^*_{\mathrm{k},\mu} + \frac{1}{2} ikct \right) \right]. \tag{A9}$$

If the $\mathbf{k}', \mu'$ oscillator is excited to the nth quantum state, the super wave field is

$$\Psi^{(R)} = h_n \left(q_{\mathbf{k}',\mu'} \right) e^{-ink'ct} \Psi_0^{(R)} \tag{A10}$$

where h_n is the nth hermite polynomial. As shown in Paper I, Sec. 5, the stationary states of such a system correspond to a quantized energy equal to the same value, $E_n = \left(n + \frac{1}{2}\right) \hbar kc$, obtained from the usual interpretation. In nonstationary states, however, Eqs. (A7) and (A8) imply that the energy of each oscillator may fluctuate violently, as was also true of nonstationary states of the hydrogen atom (see Paper I, Sec. 7).

A nonstationary state of particular interest in the photoelectric and Compton effects is a state corresponding to the presence of an electromagnetic wave packet containing a single quantum. The super wave field for such a state is

$$\Psi_P^{(R)} = \sum_{\mathbf{k},\mu} f_\mu \left(\mathbf{k} - \mathbf{k}_0 \right) q_{\mathbf{k},\mu} e^{-ikct} \Psi_0^{(R)} \tag{A11}$$

where $f_\mu \left(\mathbf{k} - \mathbf{k}_0 \right)$ is a function that is large only near $\mathbf{k} = \mathbf{k}_0$ and the first hermite polynomial is represented by $q_{k,\mu}$, to which it is proportional.

To prove that Eq. (A11) represents an electromagnetic wave packet, we can evaluate the difference

$$\langle \Delta W \rangle_{\mathrm{Av}} = \langle W \rangle_{\mathrm{Av}} - \langle W_0 \rangle_{\mathrm{Av}}, \tag{A12}$$

where $\langle W(\mathbf{x}) \rangle_{\mathrm{Av}}$ is the actual mean energy density present (averaged over the ensemble), and $\langle W_0(\mathbf{x}) \rangle_{\mathrm{Av}}$ is the mean energy that would be present even in the ground state, because of zero-point fluctuations. We have

[88] See G. Wentzel, Quantum Theory of Fields (Interscience Publishers, Inc., New York, 1948).

$$\langle W(\mathbf{x})\rangle_{\mathrm{Av}} = \iint\cdots\int \Psi_P^{*(R)}\left(\cdots q_{\mathrm{k},\mu}\cdots\right) \times \frac{\left[\mathscr{E}^2(\mathbf{x})+\mathfrak{S}^2(\mathbf{x})\right]}{8\pi}\Psi_P^{(R)}\left(\cdots q_{\mathrm{k},\mu}\cdots\right) \times\left(\cdots dq_{\mathrm{k},\mu}\cdots\right) \tag{A13}$$

$$\langle W_0(\mathbf{x})\rangle_{\mathrm{Av}} = \iint\cdots\int \Psi_0^{*(R)}\left(\cdots q_{\mathrm{k},\mu}\cdots\right) \times \frac{\left[\mathfrak{F}^2(\mathbf{x})+\mathfrak{S}^2(\mathbf{x})\right]}{8\pi}\Psi_0^{(R)}\left(\cdots q_{\mathrm{k},\mu}\cdots\right) \times\left(\cdots dq_{\mathrm{k},\mu}\cdots\right) \tag{A14}$$

Obtaining $\mathfrak{E}(\mathbf{x})$ from Eq. (A2), $\mathfrak{W}(\mathbf{x})$ from Eq. (A3), ${\Psi_P}^{(R)}$ from Eq. (A10), ${\Psi_0}^{(R)}$ from Eq. (A9), we readily show that

$$\langle \Delta W(\mathbf{x})\rangle_{\mathrm{Av}} = \textstyle\sum_{\mathbf{k},\mu}\sum_{\mathbf{k}',\mu'} f_\mu\left(\mathbf{k}-\mathbf{k}_0\right) f_{\mu'}\left(\mathbf{k}'-\mathbf{k}_0\right) \times e^{i(\mathbf{k}+\mathbf{k}')\cdot\mathbf{x}_{\epsilon_{\mathbf{k},\mu}}\cdot\epsilon_{\mathbf{k}',\mu'}} \tag{A15}$$

This means that the wave packet implies an excess over zero-point energy that is localized within a region in which the packet function, $\boldsymbol{g}(\mathbf{x})$ is appreciable, where

$$\mathbf{g}(\mathbf{x}) = \sum_{\mathbf{k},\mu} f_\mu\left(\mathbf{k}-\mathbf{k}_0\right) e^{i\mathbf{k}\cdot\mathbf{x}}\epsilon_{\mathbf{k},\mu} \tag{A16}$$

We are now ready to treat the photoelectric and Compton effects. The entire treatment is so similar to that of the Franck-Hertz experiment (Paper I, Sec. 7) that we need merely sketch it here. We begin by adding to the radiation Hamiltonian, $H^{(R)}$, the particle Hamiltonian,

$$H^{(P)} = (1/2m)[\mathbf{p}-(e/c)\mathbf{A}(\mathbf{x})]^2 \tag{A17}$$

(We restrict ourselves here to nonrelativistic treatment.) The photoelectric effect corresponds to the transition of a radiation oscillator from an excited state to the ground state, while the atomic electron is ejected, with an energy $E = h\nu - I$, where I is the ionization potential of the atom. The initial super wave field, corresponding to an incident packet containing only one quantum, plus an atom in the ground state is (see Eq. (A11))

$$\Psi_i = \psi_0(\mathbf{x})\exp\left(-iE_0t/\hbar\right)\Psi_0^{(R)}\left(\cdots q_{\mathbf{k},\mu}\cdots\right) \times\sum_{\mathbf{k},\mu} f_\mu\left(\mathbf{k}-\mathbf{k}_0\right) q_{\mathbf{k},\mu}e^{-ikct}. \tag{A18}$$

By solving Schroedinger's equation for the combined system, we obtain an asymptotic wave field analogous to Paper I, Eq. (26), containing terms corresponding to the photoelectric effect. These terms, which must be added to Ψ_i, to yield the complete superfield, are (asymptotically) $\delta\Psi_a = {\Psi_0}^{(R)}\left(\cdots q_{\mathrm{k},\mu}\cdots\right)\sum_{\mathbf{k},\mu} f_\mu\left(\mathbf{k}-\mathbf{k}_0\right)$

$$\times\frac{\exp\left[i\mathbf{k}'\cdot\mathbf{r}-i\hbar\left(k'^2/2m\right)t\right]}{r}g_\mu\left(\theta,\phi,k'\right), \tag{A19}$$

where the energy of the outgoing electron is $E = \hbar^2k^2/2m = \hbar kc + E_0$. The function $g_\mu\left(\theta,\phi,k'\right)$ is the amplitude associated with the ψ-field of the outgoing electron. This quantity

can be calculated from the matrix element of the interaction term, $-(e/c)\mathbf{p}\cdot\mathbf{A}(\mathbf{x})$, by methods that are easily deducible from the usual perturbation theory. [6]

The outgoing electron packet has its center at $r = (\hbar k'/m)\,t$. Eventually, this packet will become completely separated from the initial electron wave function, $\psi_0(\mathbf{x})$. If the electron happens to enter the outgoing packet, the initial wave function can subsequently be ignored. The system then acts for all practical purposes as if its wave field were given by Eq. (A9), from which we conclude that the radiation field is in the ground state, while the electron has been liberated. It is readily shown that, as in the usual interpretation, the probability that the electron appears in the direction θ, ϕ can be calculated from $|g_\mu(\theta, \phi, k')|^2$ (see Paper I, Sec. 7).

To describe the Compton effect, we need only add to the super wave field the term corresponding to the appearance of an outgoing electromagnetic wave, as well as an outgoing electron. This part is asymptotically

$$\begin{aligned}\delta\Psi_b = \Psi_0^{(R)}(\cdots q_{\mathbf{k},\mu}\cdots)\sum_{\mathbf{k}',\mu'} f_\mu(\mathbf{k}-\mathbf{k}_0) \\ \times c_{\mathbf{k}',\mu'}{}^{\mathbf{k},\mu} q_{k',\mu'} g_{\mathbf{k}',\mu'}{}^{\mathbf{k},\mu}(\theta,\phi)\frac{e^{ik''r}}{r} \\ \times \exp\left(-ik'ct - \frac{i\hbar k''^2 t}{2m}\right)\end{aligned} \tag{A20}$$

where

$$\left(\hbar^2 k'^2/2m\right) + \hbar k'c = \hbar kc + E_0$$

The quantity, $c_{\mathbf{k}',\mu'}, \mu$ is proportioned to the matrix element for a transition in which the $\mathbf{k}, \mu$-radiation oscillator falls from the first excited state, to the ground state, while the $\mathbf{k}', \mu'$-oscillator rises from the ground state to the first excited state. This matrix element is determined mainly by the term $(e^2/8mc^2)\,A^2(\mathbf{x})$ in the hamiltonian.

It is easily seen that the outgoing electron packet eventually becomes completely separated both from the initial wave field, $\Psi_i(\mathbf{x}, \cdots q_{\mathrm{k},\mu}\cdots)$, and from the packet for the photoelectric effect, $\delta\Psi_a$ [defined in Eq. (A19)]. If the electron should happen to enter this packet, then the others can be ignored, and the system acts for all practical purposes like an outgoing electron, plus an independent outgoing light quantum. The reader will readily verify that the probability that the light quantum $\mathbf{k}', \mu'$ appears along with an electron with angles θ, ϕ is precisely the same as in the usual interpretation.

APPENDIX B. A DISCUSSION OF INTERPRETATIONS OF The QUANTUM THEORY PROPOSED BY DE BROGLIE AND ROGEN

After this article had been prepared, the author's attention was called to two papers in which an interpretation of the quantum theory similar to that suggested here was proposed, first by L. de Broglie, [9] and later by N . Rosen. [10] In both of these papers, it was suggested that if one writes $\psi = R\exp(is/\hbar)$, then one can regard R^2 as a probability density of particles having a velocity, $\mathbf{v} = \nabla s/m$. De Broglie regarded the ψ-field as an agent "guiding" the particle, and therefore referred to ψ as a "pilot wave." Both of these authors came to the conclusion that this interpretation could not consistently be carried through in those cases in which the field contained a linear combination of stationary state wave functions. As we shall see in this appendix, however, the difficulties encountered by the ahove authors could have heen overcome hy them, if only they had carried their ideas to a logical conclusion.

De Broglie's suggestions met strong objections on the part of Pauli, [11] in connection with the

problem of inelastic scattering of a particle by a rigid rotator. Since this problem is conceptually equivalent to that of inelastic scattering of a particle by a hydrogen atom, which we have already treated in Paper I, Sec. 7, we shall discuss the objections raised by Pauli in terms of the latter example.

Now, according to Pauli's argument, the initial wave function in the scattering problem should be $\Psi = \exp(i\mathbf{p}_0 \cdot \mathbf{y}/\hbar)\,\psi_0(\mathbf{x})$. This corresponds to a stationary state for the combined system, in which the particle momentum is $\mathbf{p}_0$, while the hydrogen atom is in its ground state, with a wave function, $\psi_0(\mathbf{x})$. After interaction between the incident particle and the hydrogen atom, the combined wave function can be represented as

$$\Psi = \sum_n f_n(\mathbf{y})\psi_n(\mathbf{x}) \tag{B1}$$

where $\psi_n(\mathbf{x})$ is the wave function for the nth excited state of the hydrogen atom, and $f_n(\mathbf{y})$ is the associated expansion coefficient. It is casily shown [12] that asymptotically, $f_n(\mathbf{y})$ takes the form of an outgoing wave, $f_n(\mathbf{y}) \sim g_n(\theta,\phi)e^{iknr}/r$, where $(\hbar kn)^2/2m = \left[(\hbar k_0)^2/2m\right] + E_n - E_0$. Now, if we write $\psi = R\exp(iS/\hbar)$, we find that the particle momenta, $p_x = \nabla_x S(\mathbf{x},\mathbf{y})$ and $\mathbf{p}_v = \nabla_y S(\mathbf{x},\mathbf{y})$, fluctuate violently in a way that depends strongly on the position of each particle. Thus, neither atom nor the outgoing particle ever seem to approach a stationary energy. On the other hand, we know from experiment that both the atom and the outgoing particle do eventually obtain definite (but presumably unpredictable) energy values. Pauli therefore concluded that the interpretation proposed by de Broglie was untenable. De Broglie seems to have agreed with the conclusion, since he subsequently gave up his suggested interpretation. [9]

Our answer to Pauli's objection is already contained in Paper I, Sec. 7, as well as in Sec. 2 of this paper. For as is well known, the use of an incident plane wave of infinite extent is an excessive abstraction, not realizable in practice. Actually, both the incident and outgoing parts of the ψ-field will always take the form of bounded packets. Moreover, as shown in Paper I, Sec. 7, all packets corresponding to different values of n will ultimately obtain classically describable separations. The outgoing particle must enter one of these packets, and it will remain with that particular packet thereafter, leaving the hydrogen atom in a definite but correlated stationary state. Thus, Pauli's objection is seen to be based on the use of the excessively abstract model of an infinite plane wave.

Although the above constitutes a complete answer io Pauli's specific objections to our suggested interpretation, we wish here to amplify our discussion somewhat, in order to auticipate certain additional objections that might be made along similar lines. For at this point, one might argue that even though the wave packet is bounded, it can nevertheless in principle be made arbitrarily large in extent by means of a suitable adjustment of initial conditions. Our interpretation predicts that in the region in which incident and outgoing ψ-waves overlap, the momentum of each particle will fluctuate violently, as a result of corresponding fluctuations in the "quantum-mechanical" potential produced by the ψ-field. The question arises, however, as to whether such fluctuations can really be in accord with experimental fact, especially since in principle they could occur when the particles were separated by distances much greater than that over which the "classical" interaction potential, $V(\mathbf{x},\mathbf{y})$, was appreciable.

To show that these fluctuations are not in disagreement with any experimental facts now available, we first point out that even in the usual interpretation the energy of each particle cannot correctly be regarded as definite under the conditions which are assumed here, namely,

[89] L. de Broglie, An Introduction to the Study of Wave Mechanics (E. P. Dutton and Company, Inc., New York, 1930), see Chapters 6, 9, and 10.

[10] N. Rosen, J. Elisha Mitchel Sci. Soc. 61, Nus. 1 and 2 (Augusi, 1945).

[11] Reports on the 1927 Solvay Congress (Gauthiers-Villars et Cie., Paris, 1928), see p. 280.

[12] N. F. Mott and H. S. W. Massey, The Theory of Atomic Collisions (Clarendon Press, Oxford, 1933).

that the incident and outgoing wave packets overlap. For as long as interference between two stationary state wave function is possible, the system acts as if it, in some sense, covered both states simultaneously. [13] In such a situation, the usual interpretation implies that a precisely defined value for the energy of either particle is meaningless. From such a wave function, one can predict only the probability that if the energy is measured, a definite value will be obtained. On the other hand, the very experimental conditions needed for measuring the energy play a key role in making a definite value of the energy possible because the effect of the measuring apparatus is to destroy interference between parts of the wave function corresponding to different values of the energy. [14]

In our interpretation, the overlap of incident and outgoing wave packets signifies not that the precise value of the energy of either particle can be given no meaning, but rather that this value fluctuates violently in an, in practice, unpredictable and uncontrollable way. When the energy of either particle is measured, however, then our interpretation predicts, in agreement with the usual interpretation, that the energy of each particle will become definite and constant, as a result of the effects of the energy-measuring apparatus on the observed system. To show how this happens, let us suppose that the energy of the hydrogen atom is measured by means of an interaction in which the "classical" potential, V, is a function only of the variables associated with the electron in the hydrogen atom and with the apparatus, but is not a function of variables associated with the outgoing particle. Let z be the coordinate of the measuring apparatus. Then as shown in Sec. 2, interaction with an apparatus that measures the energy of the hydrogen atom will transform the Ψ-function (B1), into

$$\Psi = \sum_n f_n(\mathbf{y})\psi_n(\mathbf{x})g_0\left(z - aEnt/\hbar^2\right). \tag{B2}$$

Now, we have seen that if the product at is large enough to make a distinct measurement possible, packets corresponding to different values of n will ultimately obtain classically describable separations in z space. The apparatus variable, z, must enter one of these packets; and, thereafter, all other packets can for practical purposes be ignored. The hydrogen atom is then left in a state having a definite and constant energy, while the outgoing particle has a correspondingly definite but correlated constant value for its energy. Thus, we find that as with the usual interpretation, our interpretation predicts that whenever we measure the energy of either particle by methods that are now available, a definite and constant value will always be obtained. Nevertheless, under conditions in which incident and outgoing wave packets overlap, and in which neither particle interacts with an energymeasuring dcvicc, our interpretation states unambiguously that real fluctuations in the energy of each particle will occur. These fluctuations are moreover, at least in principle, observable (for example, by methods discussed in Sec. 6). Meanwhile, under conditions in which we are limited by present methods of observation, our interpretation leads to predictions that are precisely the same as those obtained from the usual interpretation, so that no experiments supporting the usual interpretation can possibly contradict our interpretation.

In his book, [9] de Broglie raises objections to his own suggested interpretation of the quantum theory, which are very similar to those raised by Pauli. It is therefore not necessary to answer de Broglie's objections in detail here, since the answer is essentially the same as that which has been given to Pauli. We wish, however,

to add one point. De Broglie assumes that not only electrons, but also light quanta, are associated with particles. A consistent application of the interpretation suggested here requires, however, as shown in Appendix A, that light quanta be described as electromagnetic wave packets. The only precisely definable quantities in such a packet are the Fourier components, $q_{\mathbf{k},\mu}$, of

[8][13] Reference 2, Chapter 16, Sec. 25.

[14] Reference 2, Chapter 6, Secs. 3 to 8; Chapter 22, Secs. 8 to 10.

the vector potential and the corresponding canonically conjugate momenta, $\Pi_{k,\mu}$. Such packets have many particle-like properties, including the ability to transfer rapidly a full quantum of energy at great distances. Nevertheless, it would not be consistent to assume the existence of a "photon" particle, associated with cach light quantum.

We shall now discuss Rosen's paper briefly. [10] Rosen gave up his suggested interpretation of the quantum theory, because of difficulties arising in connection with the interpretation of standing waves. In the case of the stationary states of a free particle in a box, which we have already discussed in Sec. 8, our interpretation leads to the conclusion that the particle is standing still. Rosen did not wish to accept this conclusion,

because it seemed to disagree with the statement of the usual interpretation that in such a state the electron is moving with equal probability that the motion is in either direction. To answer Rosen's objections, we need merely point out again that the usual interpretation can give no meaning to the motion of particles in a stationary state; at best, it can only predict the probability that a given result will be obtained, if the velocity is measured. As we saw in Sec. 8, however, our interpretation leads to precisely the same predictions as are obtained from the usual interpretation, for any process which could actually provide us with a measurement of the velocity of the electron. One must remember, however, that the value of the momentum "observable" as it is now "measured" is not necessarily equal to the particle momentum existing before interaction with the measuring apparatus took place.

We conclude that the objections raised by Pauli, de Broglie, and Rosen, to interpretations of the quantum theory similar to that suggested here, can all be answered by carrying every aspect of our suggested interpretation to its logical conclusion.

26.5 III.4 On the Problem of Hidden Variables in Quantum Mechanics*

Abstract

The demonstrations of von Neumann and others, that quantum mechanics does not permit a hidden variable interpretation, are reconsidered. It is shown that their essential axioms are unreasonable. It is urged that in further evalmination of this problem an interesting axiom would be that mutually distant systems are independent of one another.

26.5.1 I. Introduction

To know the quantum mechanical state of a system implies, in general, only statistical restrictions on the results of measurements. It seems interesting to ask if this statistical element be thought of as arising, as in classical statistical mechanics, because the states in question are averages over better defined states for which individually the results would be quite determined. These hypothetical "dispersion free" states would be specified not only by the quantum mechanical state vector but also by additional "hidden variables""hidden" because if states with prescribed values of these variables could actually be prepared, quantum mechanics would be obscrvably inadequate.

Whether this question is indeed interesting has been the subject of debate. [1,2] The present paper does not contribute to that debate. It is addressed to those who do find the question interesting, and more particularly to those among them who believe that [3] "the question concerning the existence of such hidden variables received an early and rather decisive answer in the form of von Neumann's proof on the mathematical impossibility of such variables in quantum theory." An attempt will be made to clarify what von Neumann and his successors actually demonstrated. This will cover, as well as von Neumann's treatment, the recent version of the

argument by Jauch and Piron, [3] and the stronger

result consequent on the work of Gleason. [4] It will be urged that these analyses leave the real question untouched. In fact it will be seen that these demonstrations require from the hypothetical dispersion free states, not only that appropriate ensembles thereof should have all measurable properties of quantum mechanical states, but certain other properties as well. These additional demands appear reasonable when results of measurement are loosely identified with properties of isolated systems. They are seen to be quite unreasonable when one remembers with Bohr "the impossibility of any sharp distinction between the behavior of atomic objects and the interaction with the measuring instruments which serve to define the conditions under which the phenomena appear."

The realization that von Neumann's proof is of limited relevance has been gaining ground since the 1952 work of Bohm. [6] However, it is far from universal. Moreover, the writer has not found in the literature any adequate analysis of what went wrong. [7] Like all a.uthors of noncommissioned reviews, he thinks that he can restate the position with such clarity and simplicity that all previous discussions will be eclipsed.

26.5.2 II. Assumptios, and a Simple Example

The authors of the demonstrations to be reviewed were concerned to assume as little as possible about quantum mechanics. This is valuable for some purposes, but not for ours. We are interested only in the possibility of hidden variables in ordinary quantum me-

chanics and will use freely all the usual notions. Thereby the demonstrations will be substantially shortened.

A quantum mechanical "system" is supposed to have "observables" represented by Hermitian operators in a complex linear vector space. Every "measurement" of an observable yields one of the eigenvalues of the corresponding operator. Observables with commuting operators

---

[8]

• Work supported by U.S. Atomic Energy Commission.

† Permanent address: CERN, Geneva.

[1] The following works contain discussions of and references on the hidden variable problem: L. (de Broglie, Physicien ct Penseur (Albin Michel, Paris, 1953); W. Heisenberg, in Niels Bohr and lite Decelopment of Physics, W. Pauli, Ed. (McGraw-Hill Book Co., Inc., New York, and Pergamon Press, Ltd., London, 1955) ; Observation and Interpretation, S. Körner, Ed. (Academic Press Inc., New York, and Butterworths Scientific Publ, Ltd., London, 1957); N. R. Hansen, The Concept of the Positron (Cambridge University Press, Cambridge, England, 1963). See also the various works by D. Bohm cited later, and Bell and Nauenberg. [8] For the view that the possibility of hidden variables has little interest, see especially the contributions of Rosenfeld to the first and third of these references, of Pauli to the first, the article of Heisenberg, and many passages in Hansen.

[2] A. Einstein, Philosopher Scientist, P. A. Schilp, Ed. (Library of Living Philosophers, Evanston, Ill., 1949). Einstein's "Autobiugraphical Notes" and "Reply" to Critics" suggest that the hidden variable problem has some interest.

[3] J. M. Jauch and C. Piron, Helv. Phys. Acta 36, 827 (1963).

[84] A. M. Gleason, J. Math. & Mech. 6, 885 (1957). I am much indebted to Professor Jauch for drawing my attention to this work.

[5] N. Bohr, in Kef. 2.

[6] D. Bohm, Ihys. Rev. 85, 166, 180 (1952).

[7] In particular the analysis of Bohm [6] seems to lack clarity, or else accuracy. He fully emphasizes the role of the experimental arrangement. However, it seems to be implied (Ref. 6, p. 187) that the circumvention of the theorem requires the association of lidden variables with the apparatus as well as with the system observed. The scheme of Sec. II is a counter example to this. Morcover, it will be seen in Sec. III that if the essential additivity assumption of von Neumann were granted, hidden variables wherever located would not avail. Bohm's further remarks in Ref. 16 (p. 95) and Ref. 17 (p. 358) are also unconvincing. Other critiques of the theorem are cited, and some of them rebutted, by Albertson [J. Albertson, Am. J. Phys. 29, 478 (1961)].

can be measured sinultaneously. [8] A quantum mechanical "state" is represented by a vector in the linear state space. For a state vector ψ the statistical expectation value of an observable with operator O is the normalized inner product $(\psi, O\psi)/(\psi, \psi)$.

The question at issue is whether the quantum mechanical states can be regarded as ensembles of states further specified by additional variables, such that given values of these variables together with the state vector determine precisely the results of individual measurements. These hypothetical well-specified states are said to be "dispersion free."

In the following discussion it will be useful to keep in mind as a simple example a system with a twodimensional state space. Consider for definiteness a spin $-\frac{1}{2}$ particle without translational motion. A quantum mechanical state is represented by a twocomponent state vector, or spinor, ψ. The observables are represented by 2×2 Hermitian matrices

$$\alpha + \beta \cdot \alpha, \tag{1}$$

where α is a real number, β a real vector, and d has for components the Pauli matrices; α is understood to multiply the unit matrix. Measurement of such an observable yields one of the eigenvalues.

$$\alpha \pm |\beta|, \tag{2}$$

with relative probabilities that can be inferred from the expectation value

$$\langle \alpha + \beta \cdot \alpha \rangle = (\psi, [\alpha + \beta \cdot \alpha]\psi).$$

For this system a hidden variable scheme can be supplied as follows: The dispersion free states are specified by a real number λ, in the interval $-\frac{1}{2} \leq \lambda \leq \frac{1}{2}$, as well as the spinor ψ. To describe how λ determines which eigenvalue the measurement gives, we note that by a rotation of coordinates ψ can be brought to the form

$$\psi = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Let $\beta_x, \beta_y, \beta_z$, be the components of β in the new coordinate system. Then measurement of $\alpha + \beta \cdot \alpha$ on the state specified by ψ and λ results with certainty in the eigenvalue

$$\alpha + |\beta| \operatorname{sign}\left(\lambda|\beta| + \frac{1}{2}|\beta_2|\right) \operatorname{sign} X, \tag{3}$$

where

$$\begin{aligned} X = \beta_z \quad & \text{if } \beta_z \neq 0 \\ = \beta_x \quad & \text{if } \beta_z = 0, \beta_x \neq 0 \\ = \beta_y \quad & \text{if } \beta_c = 0, \text{ and } \quad \beta_x = 0 \end{aligned}$$

and

$$\begin{aligned} \operatorname{sign} X = +1 \quad & \text{if } X \geq 0 \\ = -1 \quad & \text{if } X < 0 \end{aligned}$$

[88] Recent papers on the measurement process in quantum mechanics, with further references, are: E. P. Wigner, Am. J. Phys. 31, 6 (1963) ; A. Shimony, ibid. 31, 755 (1963) ; J. M. Jauch, Helv. Phys. Acta 37, 293 (1964); B. d'Espagnat, Conceptions de la physique contemporaine (Hermann & Cie., Paris, 1965); J. S. Bell and M. Nauenberg, in Preludes in Theoretical Physics, In Honor of V. Weisskopf (North-Holland Publishing Company, Amsterdam, 1966).

The quantum mechanical state specified by ψ is obtained by uniform averaging over λ. This gives the expectation value

$\langle \alpha + \beta \cdot \delta \rangle$

$= \int_{-\frac{1}{2}}^{\frac{1}{2}} d\lambda \left\{ \alpha + |\beta| \operatorname{sign} \left(\lambda |\beta| + \frac{1}{2} |\beta_2| \right) \operatorname{sign} . X \right\} = \alpha + \beta_z$

as required.

It should be stressed that no physical significance is attributed here to the parameter λ and that no pretence is made of giving a complete reinterpretation of quantum mechanics. The sole aim is to show that at the level considered by von Neumann such a reinterpretation is not excluded. A complete theory would require for example an account of the behavior of the hidden variables during the measurement process itself. With or without hidden variables the analysis of the measurement process presents peculiar difficulties, [8] and we enter upon it no more than is strictly necessary for our very limited purpose.

26.5.3 III. Von Neumann

Consider now the proof of von Neumann [9] that dispersion free states, and so hidden variables, are impossible. His essential assumption [10] is: Any real linear combination of any two Hermitian operators represents an observable, and the same linear combination of expecta-

tion values is the expectation value of the combination. This is true for quantum mechanical states; it is required hy von Neumann of the hypothetical dispersion free states also. In the two-dimensional example of Sec. II, the expectation value must then be a linear function of α and β. But for a dispersion free state (which has no statistical character) the expectation value of an observable must equal one of its eigenvalues. The eigenvalues (2) are certainly not linear in β. Therefore, dispersion free states are impossible. If the state space has more dimensions, we can always consider a two-dimensional subspace; therefore, the demonstration is quite general.

The essential assumption can be criticized as follows. At first sight the required additivity of expectation values seems very reasonable, and it is rather the nonadditivity of allowed values (eigenvalues) which requires explanation. Of course the explanation is well known: A measurement of a sum of noncommuting observables cannot be made by combining trivially the results of separate observations on the two terms-it requires a quite distinct experiment. For example the measurement of σ_x for a magnetic particle might be made with a suitably oriented Stern Gerlach magnet. The measurement of σ_y would require a different orientation, and of ($\sigma_x + \sigma_y$) a third and different orientation. But this explanation of the nonadditivity of allowed values also establishes the nontriviality of the additivity of expectation values. The latter is a quite peculiar property of quantum mechanical states, not to be expected a priori. There is no reason to demand it individually of the hypothetical dispersion free states, whose function it is to reproduce the measurable peculiarities of quantum mechanics when averaged over.

In the trivial example of Scc. II the dispersion free states (specified λ) have additive expectation values only for commuting operators. Nevertheless, they give logically consistent and precise predictions for the results of all possible measurements, which when averaged over λ are fully equivalent to the quantum mechanical predictions. In fact, for this trivial example, the hidden variable question as posed informally by von Neumann [11] in his book is answered in the affirmative.

---

[89] J. von Neumann, Mathematische Gruindlagen der Quantenmechanik (Julius Springer-Verlag, Berlin, 1932) [English transl.: Princeton University Press, Princet on, N.J., 1955]. All page numbers quoted are those of the English edition. The problem is posed in the preface, and on p. 209. The formal proof occupies essentially pp. 305-324 and is followed by several pages of com mentary. A self-contained exposition of the proof has been presented by J. Albertson (see Ref. 7).

[10] This is contained in von Neumann's B' (p. 311), 1 (p. 313), and 11 (p. 314).

Thus the formal proof of von Neumann does not justify his informal conclusion [12] : "It is therefore not, as is often assumed, a question of reinterpretation of quantum mechanics-the present system of quantum mechanics would have to be objectively false in order that another description of the elementary process than the statistical one be possible." It was not the objective measurable predictions of quantum mechanics which ruled out hidden variables. It was the arbitrary assumption of a particular (and impossible) relation between the results of incompatible measurements

either of which might be made on a given occasion but only one of which can in fact be made.

26.5.4 iV. Jauch and Piron

A new version of the argument has been given by Jauch and Piron. [3] Like von Neumann they are interested in generalized forms of quantum mechanics and do not assume the usual connection of quantum mechanical expectation values with state vectors and operators. We assume the latter and shorten the argument, for we are concerned here only with possible interpretations of ordinary quantum mechanics.

Consider only observables represented by projection operators. The eigenvalues of projection operators are 0 and 1 . Their expectation values are equal to the probabilities that 1 rather than 0 is the result of measurement. For any two projection operators, a and b, a third $(a \cap b)$ is defined as the projection on to the intersection of the corresponding subspaces. The essential axioms of Jauch and Piron are the following:
(A) Expectation values of commuting projection operators are additive.
(B) If, for some state and two projections a and b,

$$\langle a \rangle = \langle b \rangle = 1,$$

then for that state

$$\langle a \cap b \rangle = 1.$$

Jauch and Piron are led to this last axiom (4° in their numbering) by an analogy with the calculus of propositions in ordinary logic. The projections are to some extent analogous to logical propositions, with the allowed value 1 corresponding to "truth" and 0 to "falsehood," and the construction ($a \cap b$) to (a "and" b) In logic we have, of course, if a is true and b is true then (a and b) is true. The axiom has this same structure.
Now we can quickly rule out dispersion free states by considering a 2 -dimensional subspace. In that the projection operators are the zero, the unit operator, and those of the form

$$\frac{1}{2} + \frac{1}{2}\hat{\boldsymbol{\alpha}} \cdot \boldsymbol{\delta},$$

where $\hat{\alpha}$ is a unit vector. In a dispersion free state the expectation value of an operator must be one of its eigenvalues, 0 or 1 for projections. Since from A

$$\left\langle \frac{1}{2} + \frac{1}{2}\hat{\boldsymbol{\alpha}} \cdot \boldsymbol{\delta} \right\rangle + \left\langle \frac{1}{2} - \frac{1}{2}\hat{\boldsymbol{\alpha}} \cdot \boldsymbol{\delta} \right\rangle = \mathbf{1},$$

we have that for a dispersion free state either

$$\left\langle \frac{1}{2} + \frac{1}{2}\hat{\boldsymbol{\alpha}} \cdot \boldsymbol{\delta} \right\rangle = 1 \quad \text{or} \quad \left\langle \frac{1}{2} - \frac{1}{2}\hat{\boldsymbol{\alpha}} \cdot \boldsymbol{\delta} \right\rangle = 1.$$

[811] Reference 9, p. 209.
[12] Reference 9, p. 325.

Let $\boldsymbol{\alpha}$ and $\hat{\boldsymbol{\beta}}$ be any noncollinear unit vectors and

$$a = \frac{1}{2} \pm \frac{1}{2}\hat{\boldsymbol{\alpha}} \cdot \boldsymbol{\delta}, \quad b = \frac{1}{2} \pm \frac{1}{2}\hat{\boldsymbol{\beta}} \cdot \cdot \boldsymbol{\delta},$$

with the signs chosen so that $\langle a \rangle = \langle b \rangle = 1$. Then B requires

$$\langle a \cap b \rangle = 1.$$

But with $\hat{\alpha}$ and $\hat{\beta}$ noncollinear, one readily sees that

$$a \cap b = 0$$

so that

$$\langle a \cap b \rangle = 0.$$

So there can be no dispersion free states.
The objection to this is the same as before. We are not dealing in B with logical propositions, but with measurements involving, for example, differently oriented magnets. The axiom holds for quantum mechanical states. [13] But it is a quite peculiar property of them, in no way a necessity of thought. Only the quantum mechanical averages over the dispersion free states need reproduce this property, as in the example of Sec. II.

26.5.5 V. Gleason

The remarkable mathematical work of Gleason [4] was not explicitly addressed to the hidden variable problem. It was directed to reducing the axiomatic basis of quantum mechanics. However, as it apparently enables von Neumann's result to be obtained without objectionable assumptions about noncommuting operators, we must clearly consider it. The relevant corollary of Gleason's work is that, if the dimensionality of the state space is greater than two, the additivity requirement for expectation values of commuting operators cannot be met by dispersion free states. This will now be proved, and then its significance discussed. It should be stressed that Gleason obtained more than this, by a lengthier argument, but this is all that is essential here.

It suffices to consider projection operators. Let $P(\Phi)$ be the projector on to the Hilbert space vector Φ, i.e., acting on any vector ψ

$$P(\Phi)\psi = (\Phi, \Phi)^{-1}(\Phi, \psi)\Phi$$

If a set Φ_i are complete and orthogonal,

$$\sum_i P\left(\Phi_i\right) = 1.$$

Since the $P\left(\Phi_i\right)$ conmute, by hypothesis then

$$\sum_i \langle P\left(\Phi_i\right) \rangle = 1. \tag{4}$$

Since the expectation value of a projector is nonnegative (each measurement yields one of the allowed values 0 or 1), and since any two orthogonal vectors can be regarded as members of a complete set, we have:

(A) If with some vector Φ, $\langle P(\Phi)\rangle = 1$ for a given state, then for that state $\langle P(\psi)\rangle = 0$ for any ψ orthogonal on Φ.

If ψ_1 and ψ_2 are another orthogonal basis for the subspace spanned by some vectors Φ_1 and Φ_2, then from (4)

$$\langle P(\psi_1)\rangle + \langle P(\psi_2)\rangle = 1 - \sum_{i\neq 1, i\neq 2} \langle P(\Phi_i)\rangle$$

or

$$\langle P(\psi_1)\rangle + \langle P(\psi_2)\rangle = \langle P(\Phi_1)\rangle + \langle P(\Phi_2)\rangle$$

Since ψ_1 may be any combination of Φ_1 and Φ_2, we have:
(B) If for a given state

$$\langle P(\Phi_1)\rangle = \langle P(\Phi_2)\rangle = 0$$

for some pair of orthogonal vectors, then

$$\langle P(\alpha\Phi_1 + \beta\Phi_2)\rangle = 0$$

for all α and β.
(A) and (B) will now be used repeatedly to establish the following. Let Φ and ψ be some vectors such that for a given state

$$\langle P(\psi)\rangle = 1, \tag{5}$$
$$\langle P(\Phi)\rangle = 0. \tag{6}$$

Then Φ and ψ cannot be arbitrarily close; in fact

$$|\Phi - \psi| > \frac{1}{2}|\psi|. \tag{7}$$

To see this let us normalize ψ and write Φ in the form

$$\Phi = \psi + \epsilon\psi'$$

where ψ' is orthogonal to ψ and normalized and ϵ is a real number. Let ψ'' be a normalized vector orthogonal to both ψ and ψ' (it is here that we need three dimensions at least) and so to Φ. By (A) and (5),

$$\langle P(\psi')\rangle - 0, \quad \langle P(\psi'')\rangle - 0.$$

Then by (B) and (6),

$$\left\langle P\left(\Phi + \gamma^{-1}\epsilon\psi''\right)\right\rangle = 0$$

where γ is any real number, and also by (B),

$$\langle P(-\epsilon\psi' + \gamma\epsilon\psi'')\rangle = 0.$$

The vector arguments in the last two formulas are orthogonal; so we may add them, again using (B):

[813] In the two-dimensional case $\langle a\rangle = \langle b\rangle = 1$ (for some quantum mechanical state) is possible only if the two projectors are identical ($\hat{\alpha} = \hat{\beta}$). Then $a \cap b = a = b$ and $\langle a \cap b\rangle = \langle a\rangle = \langle b\rangle = 1$.

$$\left\langle P\left(\psi+\epsilon\left(\gamma+\gamma^{-1}\right)\psi''\right)\right\rangle=0$$

Now if ϵ is less than $\frac{1}{2}$, there are real γ such that

$$\epsilon\left(\gamma+\gamma^{-1}\right)=\pm 1.$$

Thercfore,

$$\langle P\left(\psi+\psi''\right)\rangle=\langle P\left(\psi-\psi''\right)\rangle=0$$

The vectors $\psi\pm\psi''$ are orthogonal; adding them and again using (B),

$$\langle P(\psi)\rangle=0$$

This contradicts the assumption (5). Therefore,

$$\epsilon>\frac{1}{2},$$

as announced in (%).

Consider now the possibility of dispersion free states. For such states each projector has expectation value either 0 or 1 . It is clear from (4) that both values must occur, and since there are no other values possible, there must be arbitrarily close pairs ψ,Φ with different expectation values 0 and 1 , respectively. But we saw above such pairs could not be arbitrarily close. Therefore, there are no dispersion free states.

That so much follows from such apparently innocent assumptions leads us to question their innocence. Are the requirements imposed, which are satisfied by quantum mechanical states, reasonable requirements on the dispersion free states? Indeed they are not. Consider the statement (B). The operator $P\left(\alpha\Phi_1+\beta\Phi_2\right)$ commutes with $P\left(\Phi_1\right)$ and $P\left(\Phi_2\right)$ only if either α or β is zero. Thus in general measurement of $P\left(\alpha\Phi_1+\beta\Phi_2\right)$ requires a quite distinct experimental arrangement. We can therefore reject (B) on the grounds already used: it relates in a nontrivial way the results of experiments which cannot be performed simultaneously; the dispersion free states need not have this property, it will suffice if the quantum mechanical averages over them do. How did it come about that (B) was a consequence of assumptions in which only commuting operators were explicitly mentioned? The danger in fact was not in the explicit but in the implicit assumptions. It was tacitly assumed that measurement of an observable must yield the same value independently of what other measurements may be made simultaneously. Thus as well as $P\left(\Phi_3\right)$ say, one might measure either $P\left(\Phi_2\right)$ or $P\left(\psi_2\right)$, where Φ_2 and ψ_2 are orthogonal to Φ_3 but not to one another. These different possibilities require different experimental arrangements; there is no a priori reason to believe that the results for $P\left(\Phi_3\right)$ should be the same. The result of an observation may reasonably depend not only on the state of the system (including hidden variables) but also on the complete disposition of the apparatus; see again the quotation from Bohr at the end of Sec. I.

To illustrate these remarks, we construct a very artificial but simple hidden variable decomposition. If we regard all observables as functions of commuting projectors, it will suffice to consider measurements of the latter. Let $P_1,P_2,\cdots$ be the set of projectors measured by a given apparatus, and for a given quantum mechanical state let their expectation values be $\lambda_1,\lambda_2-\lambda_1,\lambda_3-\lambda_2,\cdots$. As hidden variable we take a real number $0<\lambda\leq 1$; we specify that measurement on a state with given λ yields the value 1 for P_n if $\lambda_n.1<\lambda\leq\lambda_n$, and zero otherwise. The quantum mechanical state is obtained by uniform averaging over λ. There is no contradiction with Gleason's corollary, because the result for a given P_n depends also on the choice of the others. Of course it would be silly to let the result be affected by a mere permutation of the other P 's, so we specify that the same order is taken (however defined) when the

P 's are in fact the same set. Reflection will deepen the initial impression of artificiality here. However, the example suffices to show that the implicit assumption of the impossibility proof was essential to its conclusion. A more serious hidden variable decomposition will be taken up in Sec. VI. [14]

26.5.6 VI. Locality and Separability

Up till now we have been resisting arbitrary demands upon the hypothetical dispersion free states. However, as well as reproducing quantum mechanics on averaging, there are features which can reasonably be desired in a hidden variable scheme. The hidden variables should surely have some spacial significance and should evolve in time according to prescribed laws. These are prejudices, but it is just this possibility of interpolating some (preferably causal) space-time picture, between preparation of and measurements on states, that makes the quest for hidden variables interesting to the unsophisticated. [2] The ideas of space, time, and causality are not prominent in the kind of discussion we have been considering above. To the writer's knowledge the most successful attempt in that direction is the 1952 scheme of Bohm for elementary wave mechanics. By way of conclusion, this will be sketched briefly, and a curious feature of it stressed.

Consider for example a system of two spin $-\frac{1}{2}$ particles. The quantum mechanical state is represented by a wave function,

$$\psi_{ij}\left(\mathbf{r}_1, \mathbf{r}_2\right),$$

where i and j are spin indices which will be suppressed. This is governed by the Schrödinger equation,

$$\begin{aligned}\partial\psi/\partial t = -i\left(-\left(\partial^2/\partial\mathbf{r}_1^2\right) - \left(\partial^2/\partial\mathbf{r}_2^2\right) + V\left(\mathbf{r}_1 - \mathbf{r}_2\right)\right. \\ \left. + a\boldsymbol{d}_1 \cdot \mathbf{H}\left(\mathbf{r}_1\right) + b\boldsymbol{d}_2 \cdot \mathbf{H}\left(\mathbf{r}_2\right)\right)\psi \end{aligned} \tag{8}$$

where V is the interparticle potential. For simplicity we have taken neutral particles with magnetic moments, and an external magnetic field $\mathbf{H}$ has been allowed to represent spin analyzing magnets. The hidden variables are then two vectors $\mathbf{X}_1$ and $\mathbf{X}_2$, which give directly the results of position measurements. Other measurements are reduced ultimately to position measurements. [15] For example, measurement of a spin component means observing whether the particle emerges with an upward or downward deflection from a Stern-

Gerlach magnet. The variables $\mathbf{X}_1$ and $\mathbf{X}_2$ are supposed to be distributed in configuration space with the probability density,

$$\rho\left(\mathbf{X}_1, \mathbf{X}_2\right) = \sum_{ij} \left|\psi_{ij}\left(\mathbf{X}_1, \mathbf{X}_2\right)\right|_i,$$

appropriate to the quantum mechanical state. Consistently, with this $\mathbf{X}_1$ and $\mathbf{X}_2$ are supposed to vary with time according to

[8][14] The simplest example for illustrating the discussion of Sec. V would then be a particle of spin 1 , postulating a sufficient variety of spin-external-field interactions to permit arbitrary complete sets of spin states to be spacially separated.

[15] There are clearly enough measurements to he interesting that can be made in this way. We will not consider whether there are others.

$$d\mathbf{X}_1/dt = \rho\left(\mathbf{X}_1, \mathbf{X}_2\right)^1 \operatorname{Im} \sum_{ij} \psi_{ij}{}^* \left(\mathbf{X}_1, \mathbf{X}_2\right) \left(\partial/\partial \mathbf{X}_1\right) \psi_{ij} \left(\mathbf{X}_1, \mathbf{X}_2\right)$$
$$d\mathbf{X}_2/dt = \rho\left(\mathbf{X}_1, \mathbf{X}_2\right)^{-1} \operatorname{Im} \sum_{ij} \psi_{ij}{}^* \left(\mathbf{X}_1, \mathbf{X}_2\right) \left(\partial/\partial \mathbf{X}_2\right) \psi_{ij} \left(\mathbf{X}_1, \mathbf{X}_2\right) \tag{9}$$

The curious feature is that the trajectory equations (9) for the hidden variables have in general a grossly nonlocal character. If the wave function is factorable before the analyzing fields become effective (the particles being far apart),

$$\psi_{ij}\left(\mathbf{X}_1, \mathbf{X}_2\right) = \Phi_i\left(\mathbf{X}_1\right) \chi_i\left(\mathbf{X}_2\right),$$

this factorability will be preserved. Equations (8) then reduce to

$$d\mathbf{X}_1/dt = \left[\sum_i \Phi_1^*\left(\mathbf{X}_1\right) \Phi_1\left(X_1\right)\right]' \times \operatorname{Im} \sum_i \Phi_t^*\left(\mathbf{X}_1\right) \left(\partial'/\partial \mathbf{X}_1\right) \Phi_1\left(X_1\right)$$
$$d\mathbf{X}_2/dt = \left[\sum_j \chi_j^*\left(\mathbf{X}_2\right) \chi_j\left(X_2\right)\right]^{-1} \times \operatorname{Im} \sum_j \chi_j^*\left(\mathbf{X}_2\right) \left(\partial/\partial \mathbf{X}_2\right) \chi\left(Y_2\right)$$

The Schrödinger equation (8) also separates, and the trajectories of $\mathbf{X}_1$ and $\mathbf{X}_2$ are determined separately by equations involving $\mathbf{H}\left(\mathbf{X}_1\right)$ and $\mathbf{H}\left(\mathbf{X}_2\right)$, respectively. However, in general, the wave function is not factorable. The trajectory of 1 then depends in a complicated way on the trajectory and wave function of 2 , and so on the
analyzing fields acting on 2-however remote these may be from particle 1. So in this theory an explicit causal mechanism exists whereby the disposition of one piece of apparatus affects the results obtained with a distant piece. In fact the Einstein-PodolskyRosen paradox is resolved in the way which Einstein would have liked least (Ref. 2, p. 85).

More generally, the hidden variable account of a given system becomes entirely different when we remember that it has undoubtedly interacted with numerous other systems in the past and that the total wave function will certainly not be factorable. The same effect complicates the hidden variable account of the theory of measurement, when it is desired to include part of the "apparatus" in the system.

Bohm of course was well aware [6,16···18] of these fealures of his scheme, and has given them much attention. However, it must be stressed that, to the present writer's knowledge, there is no proof that any hidden variable account of quantum mechanics must have this extraordinary character. [19] It would therefore be interesting, perhaps, [1] to pursue some further "impossibility proofs," replacing the arbitrary axioms objected to above by some condition of locality, or of separability of distant systems.

26.5.7 Acknowledgments

The first ideas of this paper were conceived in 1952. I warmly thank Dr. F. Mandl for intensive discussion at that time. I am indebted to many others since then, and latterly, and very especially, to Professor J. M. Jauch.

[8 16] D. Bohm, Causality and Chance in Modern Physics (I). Van Nostrand Co., Inc., Princeton, N.J., 1957).
[17] D. Bohm, in Quanlum Theory, I). R. Bates, Ed. (Academic Press Inc., New York, 1962).

26.6 III.5 On the Einstein Podolsky Rosen Paradox*

26.6.1 1. Introduction

The paradox of Einstein, Podolsky and Rosen [1] was advanced as an argument that quantum mechanics could not be a complete theory but should be supplemented by additional variables. These additional variables were to restore to the theory causality and locality [2]. In this note that idea will be formulated mathematically and shown to be incompatible with the statistical predictions of quantum mechanics. It is the requirement of locality, or more precisely that the result of a measurement on one system he unaffected by operations on a distant system with which it has interacted in the past, that creates the essential difficulty. There have been attempts [3] to show that even without such a separability or locality requirement no "hidden variable" interpretation of quantum mochanics is possible. These attempts have heen examined elsewhere [4] and found wanting. Moreover, a hidden variable interpretation of elementary quantum theory [5] has been explicitly constructed. That particular interpretation has indeed a grossly nonlocal structure. This is characteristic, according to the result to be proved here, of any such theory which reproduces exactly the quantum mechanical predictions.

26.6.2 II. Formulation

With the example advocated by Bohm and Aharonov [6]. the EPR argument is the following. Consider a pair of spin one-half particles formed somehow in the singlet spin state and moving freely in opposite directions. Measurements can be made, say by Stern-Gerlach magnets, on selected components of the spins $\vec{\sigma}_1$ and $\vec{\sigma}_2$. If measurement of the component $\vec{\sigma}_1 \cdot \vec{a}$, where $\vec{a}$ is some unit vector, yields the value $+1$ then, according to quantum mechanics, measurement of $\vec{\sigma}_2 \cdot \vec{a}$ must yield the value -1 and vice versa. Now we make the hypothesis [2], and it seems one at least worth considering, that if the two measurements are made at places remote from one another the orientation of one magnet does not influence the result obtained with the other. Since we can predict in advance the result of measuring any chosen component of $\vec{\sigma}_2$, by previously measuring the same component of $\vec{\sigma}_1$, it follows that the result of any such measurement must actually be predetermined. Since the initial quantum mechanical wave function does not determine the result of an individual measurement, this predetermination implies the possibility of a more complete specification of the state.

Let this more complete specification be effected by means of parameters λ. It is a matter of indifference in the following whether λ denotes a single variable or a set, or even a set of functions, and whether the variables are discrete or continuous. However, we write as if λ were a single continuous parameter. The result A of measuring $\vec{\sigma}_1 \cdot \vec{a}$ is then determined by $\vec{a}$ and λ, and the result B of measuring $\vec{\sigma}_2 \cdot \vec{b}$ in the same instance is determined by $\vec{b}$ and λ, and

$$A(\vec{a}, \lambda) = \pm 1, \vec{B}(\vec{b}, \lambda) = \pm 1. \tag{1}$$

The vital assumption [2] is that the result B for particle 2 does not depend on the setting $\vec{a}$, of the magnet for particie 1 , nor A on $\vec{D}$.

If $\rho(\lambda)$ is the probability distribution of λ then the expectation value of the product of the two components $\vec{\sigma}_1 \cdot \vec{a}$ and $\vec{\sigma}_2 \cdot \vec{b}$ is

$$P(\vec{a}, \vec{b}) = \int d\lambda \rho(\lambda) A(\vec{a}, \lambda) B(\vec{b}, \lambda) \tag{2}$$

[18] D. Bohm and Y. Aharonov, Phys. Rev. 108, 1070 (1957).

[19] Since the completion of this paper such a proof has been found [J. S. Beil, Physics 1, 195 (1965)].

[8]*Work supported in part by the U.S. Atomic Energy Commission

† On leave of absence from SLAC and CERN

This should equal the quantum mechanical expectation value, which for the singlet state is

$$\left\langle \ \vec{\sigma}_1 \cdot \vec{a} \quad \vec{\sigma}_2 \cdot \vec{b} \ \right\rangle = -\vec{a} \cdot \vec{b}. \tag{3}$$

But it will be shown that this is not possible.
Some might prefer a formulation in which the hidden variables fall into two sets, with A dependent on one and B on the other; this possibility is contained in the above, since λ stands for any number of variables and the dependences thereon of A and B are unrestricted. In a complete physical theory of the type envisaged by Einstein, the hidden variables would have dynamical significance and laws of motion; our λ can then be thought of as initial values of these variables at some suitable instant.

26.6.3 iii. Illustration

The proof of the main result is quite simple. Before giving it, however, a number of illustrations may serve to put it in perspective.

Firstly, there is no difficulty in giving a hidden variable account of spin measurements on a single particle. Suppose we have a spin half particle in a pure spin state with polarization denoted by a unit vector $\vec{p}$. Let the hidden variable be (for example) a unit vector $\vec{\lambda}$ with uniform probability distribution over the hemisphere $\vec{\lambda} \cdot \vec{p} > 0$. Specify that the result of measurement of a component $\vec{\sigma} \cdot \vec{a}$ is

$$\text{sign}\, \vec{\lambda} \cdot \vec{a}' \tag{4}$$

where $\vec{a}'$ is a unit vector depending on $\vec{a}$ and $\vec{p}$ in a way to be specified, and the sign function is +1 or -1 according to the sign of its argument. Actually this leaves the result undetermined when $\lambda \cdot a' = 0$, but as the probability of this is zero we will not make special prescriptions for it. Averaging over $\vec{\lambda}$ the expectation value is

$$\langle \vec{\sigma} \cdot \vec{a} \rangle = 1 - 2\theta'/\pi, \tag{5}$$

where θ' is the angle between $\vec{a}'$ and $\vec{p}$. Suppose then that $\vec{a}'$ is obtained from $\vec{a}$ by rotation towards $\vec{p}$ until

$$1 - \frac{2\theta'}{\pi} = \cos\theta \tag{6}$$

where θ is the angle between $\vec{a}$ and $\vec{p}$. Then we have the desired result

$$\langle \vec{\sigma} \cdot \vec{a} \rangle = \cos\theta \tag{7}$$

So in this simple case there is no difficulty in the view that the result of every measurement is determined by the value of an extra variable, and that the statistical features of quantum mechanics arise because the . value of this variable is unknown in individual instances.

Secondly, there is no difficulty in reproducing, in the form (2), the only features of (3) commonly used in verbal discussions of this problem:

$$\left.\begin{array}{l} P(\vec{a}, \vec{a}) = -P(\vec{a}, -\vec{a}) = -1 \\ P(\vec{a}, \vec{b}) = 0 \text{ if } \vec{a} \cdot \vec{b} = 0 \end{array}\right\} \tag{8}$$

For example, let λ now be unit vector $\vec{\lambda}$, with uniform probability distribution over all directions, and take

$$\left.\begin{aligned} A(\vec{a},\vec{\lambda}) &= \operatorname{sign}\vec{a}\cdot\vec{\lambda} \\ B(a,b) &= -\operatorname{sign}\vec{b}\cdot\vec{\lambda} \end{aligned}\right\} \tag{9}$$

This gives

$$P(\vec{a},\vec{b}) = -1 + \frac{2}{\pi}\theta, \tag{10}$$

where θ is the angle between a and b, and (10) has the properties (8). For comparison, consider the result of a modified theory [6] in which the pure singlet state is replaced in the course of time by an isotropic mixture of product states; this gives the correlation function

$$-\frac{1}{3}\dot{a}\cdot\vec{b} \tag{11}$$

It is probably less easy, experimentally, to distinguish (10) from (3), than (11) from (3). Unlike (3), the function (10) is not stationary at the minimum value -1 (at $\theta = 0$). It will be seen that this is characteristic of functions of type (2).

Thirdly, and finally, there is no difficulty in reproducing the quantum mechanical correlation (3) if the results A and B in (2) are allowed to depend on $\vec{b}$ and $\vec{a}$ respectively as well as on $\vec{a}$ and $\vec{b}$. For example, replace $\vec{a}$ in (9) by $\vec{a}'$, obtained from $\vec{a}$ by rotation towards $\vec{b}$ until

$$1 - \frac{2}{\pi}\theta' = \cos\theta,$$

where θ' is the angle between $\vec{a}'$ and $\vec{b}$. However, for given values of the hidden variables, the results of measurements with one magnet now depend on the setting of the distant magnet, which is just what we would wish to avoid.

26.6.4 IV. Contradiction

The main result will now be proved. Because ρ is a normalized probability distribution,

$$\int d\lambda\rho(\lambda) = 1, \tag{12}$$

and because of the properties (1), P in (2) cannot be less than -1 . It can reach -1 at $\vec{a} = \vec{b}$ only if

$$A(\vec{a},\lambda) = -B(\vec{a},\lambda) \tag{13}$$

except at a set of points λ of zero probability. Assuming this, (2) can be rewritten

$$P(\vec{a},\vec{b}) = -\int d\lambda\rho(\lambda)A(\vec{a},\lambda)A(\vec{b},\lambda). \tag{14}$$

It follows that $\vec{c}$ is another unit vector

$$\begin{aligned} P(\vec{a},\vec{b}) - P(\vec{a},\vec{c}) &= -\int d\lambda\rho(\lambda)[A(\vec{a},\lambda)A(\vec{b},\lambda) - A(\vec{a},\lambda)A(\vec{c},\lambda)] \\ &= \int d\lambda\rho(\lambda)A(\vec{a},\lambda)A(\vec{b},\lambda)[A(\vec{b},\lambda)A(\vec{c},\lambda) - 1] \end{aligned}$$

using (1), whence

$$|P(\vec{a},\vec{b}) - P(\vec{a},\vec{c})| \leq \int d\lambda\rho(\lambda)[1 - A(\vec{b},\lambda)A(\vec{c},\lambda)]$$

The second term on the right is $P(\vec{b},\vec{c})$, whence

$$1 + P(\vec{b},\vec{c}) \geq |P(\vec{a},\vec{b}) - P(\vec{a},\vec{c})| \tag{15}$$

Unless P is constant, the right hand side is in general of order $|\vec{b}-\vec{c}|$ for small $|\vec{b}-\vec{c}|$. Thus $P(\vec{b},\vec{c})$ cannot be stationary at the minimum value (-1 at $\vec{b}=\vec{c}$) and cannot equal the quantum mechanical value (3).

Nor can the quantum mechanical correlation (3) be arbitrarily closely approximated by the form (2). The formal proof of this may be set out as follows. We would not worry about failure of the approximation at isolated points, so let us consider instead of (2) and (3) the functions

$$\vec{P}(\vec{a},\vec{b}) \text{ and } -\vec{a}\cdot\vec{b}$$

where the bar denotes independent averaging of $P\left(\vec{a}',\vec{b}'\right)$ and $-\vec{a}'\cdot\vec{b}'$ over vectors $\vec{a}'$ and $\vec{b}'$ within specified small angles of $\vec{a}$ and $\vec{b}$. Suppose that for all $\vec{a}$ and $\vec{b}$ the difference is bounded by ϵ :

$$|\vec{P}(\vec{a},\vec{b}) + \vec{a}\cdot\vec{b}| \leq \epsilon \tag{16}$$

Then it will be shown that ϵ cannot be made arbitrarily small.
Suppose that for all a and b

$$|\vec{a}\cdot\vec{b} - \vec{a}\cdot\vec{b}| \leq \delta \tag{17}$$

Then from (16)

$$|\ \vec{\vec{P}}\ (\vec{\vec{a}},\vec{b}) + \vec{\vec{a}}\cdot\vec{b}| \leq \epsilon + \delta \tag{18}$$

From (2)

$$\bar{P}(\vec{a},\vec{b}) = \int d\lambda \rho(\lambda)\bar{A}(\vec{a},\lambda)\bar{B}(\vec{b},\lambda) \tag{19}$$

where

$$|\bar{A}(\vec{a},\lambda)| \leq 1 \text{ and } |\bar{B}(\vec{b},\lambda)| \leq 1 \tag{20}$$

From (18) and (19), with $\vec{a}=\vec{b}$,

$$d\lambda\rho(\lambda)[\vec{A}(\vec{b},\lambda)\vec{B}(\vec{b},\lambda)+1] \leq \epsilon+\delta \tag{21}$$

From (19)

$$\begin{aligned}\vec{P}(\vec{a},\vec{b}) - \vec{P}(\vec{a},\vec{c}) &= \int d\lambda\rho(\lambda)[\vec{A}(\vec{a},\lambda)\vec{B}(\vec{b},\lambda) - \vec{A}(\vec{a},\lambda)\vec{B}(\vec{c},\lambda)] \\ &= \int d\lambda\rho(\lambda)\vec{A}(\vec{a},\lambda)\vec{B}(\vec{b},\lambda)[1+\vec{A}(\vec{b},\lambda)\vec{B}(\vec{c},\lambda)] \\ &\quad - \int d\lambda\rho(\lambda)\vec{A}(\vec{a},\lambda)\vec{B}(\vec{c},\lambda)[1+\vec{A}(\vec{b},\lambda)\vec{B}(\vec{b},\lambda)]\end{aligned}$$

Using (20) then

$$\begin{aligned}|\bar{P}(\vec{a},\vec{b}) - \bar{P}(\vec{a},\vec{c})| < &\int d\lambda\alpha(\lambda)[1+\bar{A}(\vec{b},\lambda)\bar{B}(\vec{c},\lambda)] \\ &+ \int d\lambda\rho(\lambda)[1+\bar{A}(\vec{b},\lambda)\bar{B}(\vec{b},\lambda)]\end{aligned}$$

Then using (19) and 21)

$$|\bar{P}(\vec{a},\vec{b}) - \bar{P}(\vec{a},\overrightarrow{c})| \leq 1 + \bar{P}(\vec{b},\overrightarrow{c}) + \epsilon + \delta$$

Finally, using (18),

$$|\vec{a}\cdot\vec{c} - \vec{a}\cdot\vec{b}| - 2(\epsilon+\delta) \leq 1 - \vec{b}\cdot\vec{c} + 2(\epsilon+\delta)$$

oi

$$4(\epsilon+\delta) \geq |\vec{a}\cdot\vec{c} - \vec{a}\cdot\vec{b}| + \vec{b}\cdot\vec{c} - 1 \tag{22}$$

Take for example $\vec{a}\cdot\vec{c} = 0, \vec{a}\cdot\vec{b} = \vec{b}\cdot\vec{c} = 1/\sqrt{2}$ Then

$$4(\epsilon+\delta) \geq \sqrt{2} - 1$$

Therefore, for small finite δ, ϵ cannot be arbitrarily small.
Thus, the quantum mechanical expectation value cannot be represented, either accurately or arbitrarily closely, in the form (2).

26.6.5 V. Generalization

The example considered above has the advantage that it requires little imagination to envisage the measurements involved actually being made. In a more formal way, assuming [7] that any Hermitian operator with a complete set of eigenstates is an "observable", the result is easily extended to other systems. If the two systems have state spaces of dimensionality greater than 2 we can always consider two dimensional subspaces and define, in their direct product, operators $\vec{u}_1$ and $\vec{\sigma}_2$ formally analogous to those used above and which are zero for states outside the product subspace. Then for at least one quantum mechanical state, the "singlet" state in the combined subspaces, the statistical predictions of quantum mechanics are incompatible with separable predetermination.

26.6.6 VI. Conclusion

In a theory in which parameters are added to quantum mechanics to determine the results of individual measurements, without changing the statistical predictions, there must be a mechanism whereby the setting of one measuring device can influence the reading of another instrument, however remote. Moreover, the signal involved must propagate instantaneously, so that such a theory could not be Lorentz invariant.

Of course, the situation is different if the quantum mechanical predictions are of limited validity. Conceivably they might apply only to experiments in which the settings of the instruments are made sufficiently in advance to allow them to reach some mutual rapport by exchange of signals with velocity less than or equal to that of light. In that connection, experiments of the type proposed by Bohm and Aharonov [6], in which the settings are changed during the flight of the particles, are crucial.

I am indebted to Drs. M. Bander and J. K. Perting for very useful discussions of this problem. The first draft of the paper was written during a stay at Brandeis University; I am indebted to colleagues there and at the University of Wisconsin for their interest and hospitality.

References

1. A. EINSTEIN, N. ROSEN and B. PODOLSKY, Phys. Rev. 47, 777 (1935); see also N. BOHR, Ibid. 48, 696 (1935), W. H. FURRY, ibid. 49, 393 and 476 (1936), and D. R. iNGLis, Rev. Mod. Phys. 33, 1 (1961).

2. "But on one supposition we should, in my opinion, absolutely hold fast: the real factual situation of the system S_2 is independent of what is done with the system S_1, which is spatially separated from the former." A. EINSTEIN in Albert Einstein, Philosopher Scientist, (Edited by P. A. SCHILP) p. 85, Library of Living Philosophers, Evanston, Illinois (1949).

3. J. VON NEUMANN, Mathematishe Grundlagen der Quanten-mechanik. Verlag Julius-Springer, Berlin (1932), [English translation: Princeton University Press (1955)]; J. M. JAUCH and C. PIRON, Helv. Phys. Acta 36, 827 (1963).

4. J. S. BELL, to be published.

5. D. BOHM, Phys. Rev. 85, 166 and 180 (1952).

6. D. BOHM and Y. AHARONOV, Phys. Rev. 108, 1070 (1957).

7. P. A. M. DiRAC, The Frincipies of Quanium Mechanics (3rd Ed.) p. 37. The Clarendon Press, Oxford (1947).

26.7 III.6 Proposed Experiment to Test Local Hidden-variable Theories by Clauser, Horne, Shimony, Holt

Abstract

A theorem of Bell, proving that certain predictions of quantum mechanics are inconsistent with the entire family of local hidden-variable theories, is generalized so as to apply to realizable experiments. A proposed extension of the experiment of Kocher and Commins, on the polarization correlation of a pair of optical photons, will provide a decisive test between quantum mechanics and local hidden-variable theories.

Einstein, Podolsky, and Rosen (EPR) in a classic paper [1] presented a paradox which led them to infer that quantum mechanics is not a complete theory. They concluded that the quantum mechanical description of a physical system should be supplemented by postulating the existence of "hidden variables," the specification of which would predetermine the result of measuring any observable of the system. They believed the predictions of quantum mechanics to be correct, but only as consequences of statistical distributions of the hidden variables. Bohr [2] argued in reply that no paradox can be derived from the assumption of completeness if one recognizes that quantum mechanics concerns only the interaction of microsystems with experimental apparatus and not their intrinsic character.

There is an extensive literature purporting to prove the inconsistency of hidden-variable theories with the statistical predictions of quantum mechanics. These proofs, though mathematically valid, rest upon physically unrealistic postulates. [3] Bell [4] succeeded in replacing these postulates by a physically reasonable condition of locality. He showed that in a Gedankenexperiment of Bohm [5] (a variant of that of EPR) no local hidden-variable theory can reproduce all of the statistical predictions of quantum mechanics. This result is somewhat ironical in view of Einstein's convictions [6] that quantum mechanical predictions concerning spatially separated systems are incompatible with his conditions for locality unless hidden variables exist.

Bell's theorem has profound implications in that it points to a decisive experimental test of the entire family of local hidden-variable theories. The aim of this paper is to propose explicitly such an
experiment. For this purpose, we first present a generalization of Bell's theorem which applies to realizable experiments. Second, we indicate that neither of the experimental realizations [7] of Bohm's Gedankenexperiment has produced evidence against local hidden-variable theories, even though the results of both are compatible with quantum mechanical predictions. Third, we show that a simple extension of one of these experiments can provide a decisive test.

Generalization of Bell's theorem. - Consider an ensemble of correlated pairs of particles moving so that one enters apparatus I_a and the other apparatus II_b, where a and b are adjustable apparatus parameters. In each apparatus a particle must select one of two channels labeled +1 and -1 . Let the results of these selections be represented by $A(a)$ and $B(b)$, each of which equals ± 1 according as the first or second channel is selected.
Suppose now that a statistical correlation of $A(a)$ and $B(b)$ is due to information carried by and localized within each particle, and that at some time in the past the particles constituting one pair were in contact and communication regarding this information. The information, which emphatically is not quantum mechanical, is part of the content of a set of hidden variables, denoted collectively by λ. The results of the two selections are then to be deterministic functions $A(a,\lambda)$ and $B(b,\lambda)$. Locality reasonably requires $A(a,\lambda)$ to be independent of the parameter b and $B(b,\lambda)$ to be likewise independent of a, since the two selections may occur at an arbitrarily great distance from each other. Finally, since the pair of particles is generally emitted by a source in a manner physically independent of the adjustable parameters a and b, we assume that the normalized probability distribution $\rho(\lambda)$ characterizing the ensemble is independent of a and b.
Defining the correlation function $P(a,b) \equiv \int_\Gamma A(a,\lambda)B(b,\lambda)\rho(\lambda)d\lambda$, where Γ is the total λ space, we have

$$|P(a,b)-P(a,c)| \leqslant \int_\Gamma |A(a,\lambda)B(b,\lambda)-A(a,\lambda)B(c,\lambda)|\rho(\lambda)d\lambda = \int_\Gamma |A(a,\lambda)B(b,\lambda)|[1-B(b,\lambda)B(c,\lambda)]\rho($$
$$= \int_\Gamma [1-B(b,\lambda)B(c,\lambda)]\rho(\lambda)d\lambda = 1-\int_\Gamma B(b,\lambda)B(c,\lambda)\rho(\lambda)d\lambda$$

Suppose that for some b' and b we have $P(b',b) = 1-\delta$, where $0 \leqslant \delta \leqslant 1$. Experimentally interesting cases will have δ close to but not equal to zero. Here we avoid Bell's experimentally unrealistic restriction that for some pair of parameters b' and b there is perfect correlation (i.e., $\delta = 0$). Dividing Γ into two regions $\Gamma_+$and Γ_-such that $\Gamma_\pm = \{\lambda \mid A(b',\lambda) = \pm B(b,\lambda)\}$, we have $\int_{\Gamma_-}\rho(\lambda)d\lambda = \frac{1}{2}\delta$. Hence,

$$\int_\Gamma B(b,\lambda)B(c,\lambda)\rho(\lambda)d\lambda = \int_\Gamma A(b',\lambda)B(c,\lambda)\rho(\lambda)d\lambda - 2\int_{\Gamma_-} A(b',\lambda)B(c,\lambda)\rho(\lambda)d\lambda$$
$$\geqslant P(b',c) - 2\int_{\Gamma_-} |A(b$$

and therefore

$$|P(a,b)-P(a,c)| \leqslant 2 - P(b',b) - P(b',c) \tag{1a}$$

In the experiment proposed below $P(a,b)$ depends only on the parameter difference $b-a$. Defining $\alpha \equiv b-a$, $\beta \equiv c-b$, and $\gamma \equiv b-b'$, we have

$$|P(\alpha)-P(\alpha+\beta)| \leqslant 2 - P(\gamma) - P(\beta+\gamma). \tag{1b}$$

In principle entire measuring devices, each consisting of a filter followed by a detector, could be used for I_a and II_b, and the values ± 1 of $A(a)$ and $B(b)$ would denote detection or nondetection of the particles. Inequalities (1) would then apply directly to experimental counting rates. Unfortunately, if the particles are optical photons (as in the experiment proposed below) no practical tests of (1) can presently be performed in this way, because available photoelectric efficiencies are rather small. We shall therefore henceforth interpret $A(a) = \pm 1$ and $B(b) = \pm 1$ to mean emergence or nonemergence of the photons from the respective filters. Also the filters will be taken to be linear polarization filters, and a and b will represent their orientations. It will be convenient to introduce an exceptional value ∞ of the parameter a (and likewise of b) to represent the removal of a polarizer; clearly, $A(\infty)$ and $B(\infty)$ necessarily equal $+1$. Since $P(a, b)$ is an emergence correlation function, in order to derive an experimental prediction from (1) an additional assumption [8] must be made: that if a pair of photons emerges from I_a, I_b the probability of their joint detection is independent of a and b. Then if the flux into I_a, II_b is a constant independent of a and b, the rate of coincidence detection $R(a, b)$ will be proportional to $w\left[A(a)_+, B(b)_+\right]$, where $w\left[A(a)_+, B(b)_+\right]$is the probability that $A(a) = \pm 1$ and $B(b) = \pm 1$. Letting $R_0 = R(\infty,$
$\infty), R_1(a) = R(a, \infty)$, and $R_2(b) = R(\infty, b)$, making use of the evident formulas

$$P(a, b) = w\left[A(a)_+, B(b)_+\right] - w\left[A(a)_+, B(b)_-\right] - w\left[A(a)_-, B(b)_+\right] + w\left[A(a)_-, B(b)_-\right]$$

and

$$w\left[A(a)_+, B(\infty)_+\right] = w\left[A(a)_+, B(b)_+\right] + w\left[A(a)_+, B(b)_-\right]$$

and of similar formulas for $w\left[A(\infty)_+, B(b)_+\right]$and $w\left[A(\infty)_+, B(\infty)_+\right]$, we obtain

$$\boldsymbol{P}(a, b) = \frac{4R(a, b)}{\boldsymbol{R}_0} - \frac{2\boldsymbol{R}_1(a)}{\boldsymbol{R}_0} - \frac{2\boldsymbol{R}_2(b)}{\boldsymbol{R}_0} + \mathbf{1}.$$

We can now express (1) in terms of experimental quantities, namely coincidence rates with both polarizers in, and with one and then the other removed. If $\boldsymbol{R}_1(a)$ and $\boldsymbol{R}_2(b)$ are found experimentally to be constants R_1 and R_2, the result is

$$|K(a, b) - R(a, c)| + K\left(b', b\right) + K\left(b', c\right) - R_1 - R_2 \leqslant 0. \tag{2a}$$

In the special case in which $P(a, b) = P(a - b)$, (2a) becomes

$$|\boldsymbol{R}(\alpha) - \boldsymbol{R}(\alpha + \beta)| + \boldsymbol{R}(\gamma) + K(\beta + \gamma) - R_1 - R_2 \leqslant 0. \tag{2b}$$

Existing experimental results. - Bohm's Gedankenexperiment, involving correlated spin-$\frac{1}{2}$ particles, has not been performed, nor does it appear to be easily realizable. Two related experiments have been performed on polarization correlation of photons. Wu and Shaknov (WS) [7] examined polarization correlation of $0.5-\mathrm{MeV}\gamma$ rays emitted during positronium annihilation. [9] Although the polarization state of the pair is suitable for our purposes, their high energy requires the use of Compton polarimeters. Thus, instead of directly examining the polarization correlation, WS examined the polariza-tion-dependent joint distribution for Compton scattering of the pair. Inequality (2) cannot be immediately applied to such a scattering experiment because neither photon is forced to make a binary decision. However, a suitable binary result may be imposed by partitioning the scattering sphere into two arbitrary regions, denoted, respectively, by ± 1, and by letting the adjustable parameter a (or b) designate the particular mode of partitioning. But as one can see [10] by examining the joint scattering distribution, [11] no such partitioning can yield a correlation in violation of (2). The essential difficulty is

that the direction of Compton scattering of a photon is a statistically weak index of its iinear polarization.

The other experiment, that of Kocher and Commins (KC), [7] involved polarization correlation of photon pairs emitted in the $6^1S_0 \to 4^1P_1 \to 4^1S_0$ cascade of calcium. Since the two photons are in the visible, filters of the Polaroid type could be used. The photons impinged normally upon a pair of these polarizers whose planes were parallel, and the polarization correlation was measured with standard coincidence techniques. With this arrangement inequality (2b) is applicable upon assumption of a local hid-den-variable theory. However, the data obtained by KC do not suffice to test (2b), because their polarizers were not highly efficient and were placed only in the relative orientations 0° and 90°.

Proposed experiment. - A decisive test can be obtained by modifying the KC experiment to include observations at two appropriate relative orientations of the polarizers, and also with one and then the other removed. For realizable apparatus, quantum mechanics predicts violation of inequality (2b).

Define ${\epsilon_M}^i$ as the efficiency of the polarizer $i(i = \mathrm{I}, \mathrm{II})$ for light polarized parallel to the polarizer axis and ${\epsilon_m}^i$ as that for light perpendicularly polarized. Consider a point source and filter-detector assemblies, each of which gathers the photons emitted into a cone of half-angle θ. Then for a $J = 0 - J = 1 - J = 0$ electric-dipole cascade (0-1-0) the quantum mechanical predictions for the counting rates are [10]

$$R(\varphi)/R_0 = \frac{1}{4}\left(\epsilon_M^{\mathrm{I}} + \epsilon_m^{\mathrm{I}}\right)\left(\epsilon_M^{\mathrm{I}} + \epsilon_m^{\mathrm{I}}\right) + \frac{1}{4}\left(\epsilon_M^{\mathrm{I}} - \epsilon_m^{\mathrm{I}}\right)\left(\epsilon_M^{\mathrm{I}} - \epsilon_m^{\mathrm{I}}\right) F_1(\theta)\cos 2\varphi$$

$$R_1/R_0 = \frac{1}{2}\left(\epsilon_M^{\mathrm{I}} + \epsilon_m^{\mathrm{I}}\right), \quad R_2/R_0 = \frac{1}{2}\left(\epsilon_M^{\mathrm{I}} + \epsilon_m^{\mathrm{I}}\right). \tag{3}$$

Here φ is the angle between the polarizer axes,

$$F_1(\theta) = 2G_1^2(\theta)\left[G_2^2(\theta) + \frac{1}{2}G_3^2(\theta)\right]^{-1},$$

and

$$G_1(\theta) = \frac{1}{4}\left(\frac{4}{3} - \cos\theta + \sin^2\theta - \frac{1}{3}\cos^3\theta\right), \quad G_2(\theta) = \frac{2}{3} - \frac{1}{3}\left(\sin^2\theta + 2\right)\cos\theta, \quad G_3(\theta) = \frac{4}{3} - \cos\theta - \frac{1}{3}\cos^3\theta$$

The predictions for a $0 - 1 - 1$ electric-dipole cascade (and for a 1-1-0, provided the initial statistical state of the atom is isotropic) are obtained from (3) upon replacing $F_1(\theta)$ with $-F_2(\theta)$ where

$$F_2(\theta) = 2G_1^2(\theta)\left[2G_2(\theta)G_3(\theta) + \frac{1}{2}G_3^2(\theta)\right]^{-1}$$

For sufficiently efficient polarizers one easily sees that there exist sets of relative orientations for which the quantum mechanical counting rates violate Inequality (2b). The greatest violation always occurs at $\alpha = 22.5°, \beta = 45°$, and $\gamma = 157.5°$ for the $0 - 1 - 0$ cascade and at $\alpha = 67.5°, \beta = 135°$, and $\gamma = 112.5°$ for the 0-1-1 cascade. Note that in each case the four angles $\alpha, \alpha + \beta, \gamma$, and $\beta + \gamma$ which occur in Inequality (2b) characterize only two distinct relative orientations of the polarizers, namely 22.5° and 67.5°.

In an actual experiment $F_j(\theta)$ is less than 1 , because of finite half-angle θ, and ϵ_M is never unity. Assuming the use of calcite polarizers (for which $\epsilon_m \approx 10^{-5}$), taking ${\epsilon_M}^1 = {\epsilon_M}^{\Pi} = \epsilon_M$ for

simplicity, and using the above choices for α, β, and γ, we find that for either type of cascade, the condition for violation of Inequality (2b) is

$$\sqrt{2}F_j(\theta) + 1 > 2/\epsilon_M. \tag{4}$$

This is the essential requirement on the design of a decisive experiment. For given $F_j(\theta)$, (4)

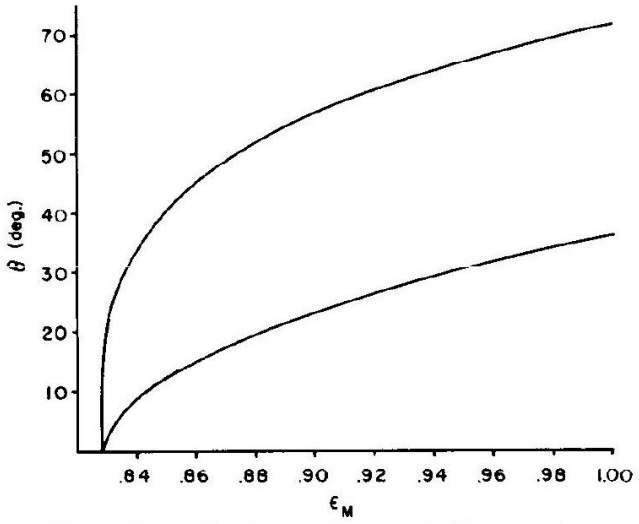


FIG. 1. Upper limits on detector half-angle θ as a function of polarizer efficiency ϵ_M. To test for hiddenvariable theories, the experiment must be performed in the region below the appropriate curve-the upper curve for a $0-1-0$ cascade, the lower for a $0-1-1$.}

implies a lower limit on ϵ_M, and vice versa. Since both $F_1(\theta)$ and $F_2(\theta)$ are monotonically decreasing functions, a lower limit on $F_j(\theta)$ implies an upper limit on θ. Condition (4) and numerical evaluation of $F_1(\theta)$ and $F_2(\theta)$ lead to the curves shown in Fig. 1, from which one can directly read combinations of θ and ϵ_M suitable for a decisive experiment. The experiment can be performed with uncoated calcite polarizers ($\epsilon_M \approx 0.92$); however, if the polarizers have antireflection coatings ($\epsilon_M \approx 0.95$), a larger θ and hence a larger counting rate can be achieved.

The authors gratefully acknowledge helpful discussions with Y. Aharonov, M. Jammer, L. Kasday, D. Nartonis, C. Papaliolios, F. Pipkin, D. Pritchard, J. L. Snider, H. Stein, and C. R. Willis.

*This paper is an expansion of ideas presented by one of us (J.F.C.) at the Spring 1969 meeting of the American Physical Society [Bull. Am. Phys. Soc. 14, 578 (1969)]. The same conclusions had been reached independently by two of us (A.S. and M.A.H.).

† Present address: Department of Physics, University of California, Berkeley, Calif.

[1] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. 47. 777 (1935),

[2] N. Bohr, Phys. Rev. 48, 696 (1935).

[3] For an excellent survey of these proofs see J. S. Bell, Rev. Mod. Phys. 38, 447 (1966).

[4] J. S. Bell, Physics 1, 19b (196b).

[5] D. Bohm, Quantum Theory (Prentice-Hall, Inc., Englewood Cliffs, New Jersey, 1951), p. 614.

[6] Albert Einstein: Philosopher-Scientist, edited by P. Schilpp (Library of Living Philosophers, Evanston, Ill., 1949), pp. 681-682.

[7] C. S. Wu and I. Shaknov, Phys. Rev. 77, 136 (1950); C. A. Kocher and E. D. Commins, Phys. Rev. Letters 18, 575 (1967). See also C. A. Kocher, thesis, University of California, 1967, University of California Radiation Laboratory Report No. UCRL-17587 (unpublished).

[8] It may appear that the assumption can be established experimentally by measuring detection rates when a controlled flux of photons of known polarization impinges on each detector. From the standpoint of hiddenvariable theories, however, these measurements are irrelevant, since the distribution of the hidden variables when the fluxes are thus controlled is almost certain to be different from the $\rho(\lambda)$ governing our ensemble. In view of the difficulty of an experimental check, the assumption could be challenged by an advocate of hidden-variable theories in case the outcome of the proposed experiment favors quantum mechanics. However, highly pathological detectors are required to con-
vert hidden-variable emergence rates into quantum mechanical counting rates.
[9] It has been shown by D. Bohm and Y. Aharonov, Phys. Rev. 108, 1070 (195%), that the WS experiment is a decisive refutation of a hypothesis studied by W.H.

Furry, Phys. Rev. 49, 393, 476 (1936).
[10] For details see M. A. Horne, thesis, Boston University, 1969 (unpublished).
[11] The distribution is given in II. S. Snyder, S. Pasternack, and J. Hornbostel, Phys. Rev. 73, 440 (1948).

26.8 III.7 Experimental Test of Local Hidden-variable Theories by Freedman, Ciauser

We have measured the linear polarization correlation of the photons cmitted in an atomic cascade of calcium. It has been shown by a generalization of Bell's inequality that the existence of local hidden variables imposes restrictions on this correlation in conflict with the predictions of quantum mechanics. Our data, in agreement with quantum mechanics, violate these restrictions to high statistical accuracy, thus providing strong evidence against local hidden-variable theories.

Since quantum mechanics was first developed, there have been repeated suggestions that its statistical features possibly might be described by an underiying deterministic substructure. Such
features, then, arise because a quantum state represents a statistical ensemble of "hiddenvariable states." Proofs by von Neumann and others, demonstrating the impossibility of a hidden-variable substructure consistent with quantum mechanics, rely on various assumptions concerning the character of the hidden variables. [1] Bell has argued that these assumptions are unduly restrictive. However, by considering an idealized case of two spatially separated but quantum-mechanically correlated systems, he was.able to show that any hidden-variable theory satisfying only the natural assumption of "locality" also leads to predictions ("Bell's inequality") in conflict with quantum mechanics. [2]

Bell's proof was extended to realizable systems by Clauser, Horne, Shimony, and Holt, [3] who also pointed out that their generalization of Bell's inequality can be tested experimentally, thus testing all local hidden-variable theories, but that existing experimental results were insufficient for this purpose. This Letter reports the results of an experiment which are sufficiently precise to rule out local hidden-variable theories with high statistical accuracy

In the present work we measured the correlation in linear polarization of two photons γ_1 and γ_2 emitted in a $J = 0 - J = 1 - J = 0$ atomic cascade. The decaying atoms were viewed by two symmetrically placed optical systems, each consisting of two lenses, a wavelength filter, a rotatable and removable polarizer, and a single-photon detector (see Fig. 1). The following quantities were measured: $R(\varphi)$, the coincidence rate for twophoton detection, as a function of the angle φ between the planes of linear polarization defined by the orientation of the inserted polarizers; R_1, the coincidence rate with polarizer 2 removed; R_2, the coincidence rate with polarizer 1 removed [4]; R_0, the coincidence rate with both polarizers re-

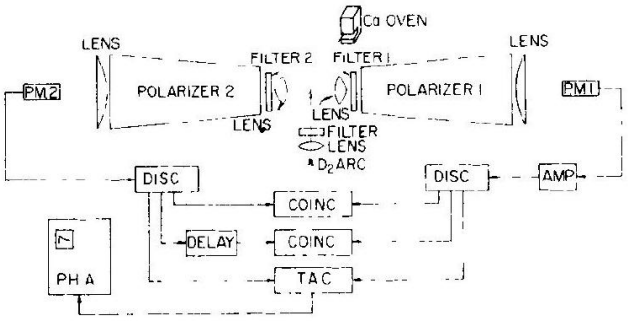


FIG. 1. Schematic diagram of apparatus and associated electronics. Scalers (not shown) monitored the outputs of the discriminators and coincidence circuits during each $100-\mathrm{sec} count period. The contents of the scalers and the experimental configuration were recorded on paper tape and analyzed on an IBM 1620-II computer.}

moved. Quantum mechanics predicts that $R(\varphi)$ and R_0 are related as follows [3,5] :

$$R(\varphi)/R_0 - \frac{1}{4}\left(\epsilon_M^1 + \epsilon_m^1\right)\left(\epsilon_M^2 + \epsilon_m^2\right) + \frac{1}{4}\left(\epsilon_M^1 - \epsilon_m^1\right) \times \left(\epsilon_M^2 - \epsilon_m^2\right) F_1(\theta)\cos 2\varphi \tag{1a}$$

while

$$R_1/R_0 = \frac{1}{2}\left({\epsilon_M}^1 + {\epsilon_m}^1\right), \tag{1b}$$

and

$$R_2/R_0 = \frac{1}{2}\left(\epsilon_M^2 + \epsilon_m^2\right). \tag{1c}$$

Here ${\epsilon_M}^i\,({\epsilon_m}^2)$ is the transmittance of the i th polarizer for light polarized parallel (perpendicular) to the polarizer axis, and $F_1(\theta)$ is a function of the half-angle θ subtended by the primary lenses. It represents a depolarization due to noncollinearity of the two photons, and approaches unity for infinitesimal detector solid angles. [For this experiment, $\theta \approx 30^\circ$, and $F_1\,(30^\circ) \approx 0.99$.]

We make the following assumptions for any local hidden-variable theory: (1) The two photons propagate as separated localized particles. (2) A binary selection process occurs for each photon at each polarizer (transmission or no-transmission). This selection does not depend upon the orientation of the distant polarizer.

In addition, we make the following assumption to allow a comparison of the generalization of Bell's inequality with out experiment: (3) All photons incident on a detector have a probability of detection that is independent of whether or not the photon has passed through a polarizer. [6]

The above assumptions constrain the coincidence rates by the following inequalities [7] :

$$-1 \leqslant \Delta(\varphi) \leqslant 0, \tag{2}$$

where

$$\Delta(\varphi) = \frac{3R(\varphi)}{R_0} - \frac{R(3\varphi)}{R_0} - \frac{R_1 + R_2}{R_0}.$$

For sufficiently small detector solid angles and highly efficient polarizers, these inequalities (2) are not satisfied by the quantum-mechanical prediction (1) for a range of values of φ.

Maximum violations occur at $\varphi = 22\frac{1}{2}^\circ[\Delta(\varphi) > 0]$ and $\varphi = 67\frac{1}{2}^\circ[\Delta(\varphi) < -1]$. At these angles of maximum violation, inequalities (2) can be combined into the simpler and more convenient expression

$$\delta = \left| R\left(22\frac{1}{2}^\circ\right)/R_0 - R\left(67\frac{1}{2}^\circ\right)/R_0 \right| - \frac{1}{4} \leqslant 0, \tag{3}$$

which does not involve R_1 or R_2.
The experimental arrangement was similar to

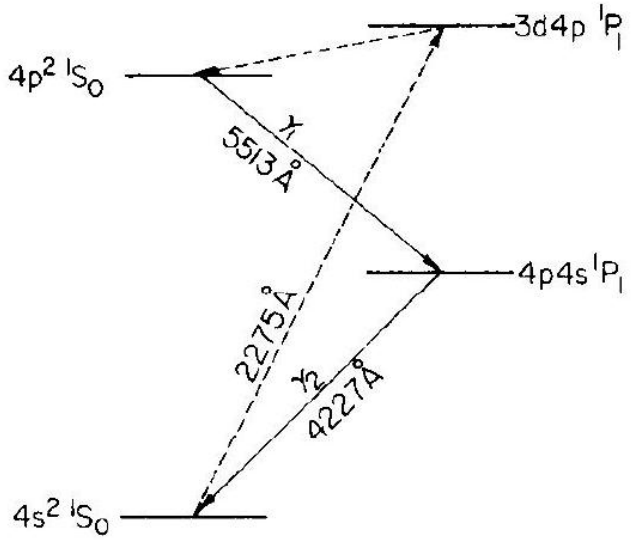


FIG. 2. Level scheme of calcium. Dashed lines show the route for excitation to the initial state $4 p^{2}{ }^{1} S_{0}$.

that of Kocher and Commins. [8] A calcium atomic beam effused from a tantalum oven, as shown in Fig. 1. The continuum output of a deuterium arc lamp (ORIEL C-42-72-12) was passed through an interference filter [250Å full width at half-maximum (FWHM), 20% transmission at 2275Å] and focused on the beam. Resonance absorption of a $2275-$ Å photon excited calcium atoms to the $3d4p^1P_1$ state. Of the atoms that did not decay directly to the ground state, about 7% decayed to the $4p^{21}S_0$ state, from which they cascaded through the $4s4p^1P_1$ intermediate state to the ground state with the emission of two photons at 5513Å (γ_1) and 4227Å (γ_2) (see Fig. 2). At the interacdion region (roughly, a cylinder 5 mm high and 3 mm in diameter) the density of the calcium was about 1×10^{10} atoms /cm^3. To avoid spherical aberrations which would have reduced counter efficiencies, aspheric primary lenses (8.0 cm diam, $f = 0.8$) were used. Photons γ_1 were selected by a filter with 10Å FWHM and 50% transmission, and γ_2 by a filter with 6Å FWHM and 20% transmission. The requirement for large efficient linear polarizers led us to employ "pile-ofplates" polarizers. Each polarizer consisted of ten $0.3-$mm-thick glass sheets inclined nearly at Brewster's angle. The sheets were attached to hinged frames, and could be folded completely out of the optical path. A Geneva mechanism rotated each polarizer through increments of $22\frac{1}{2}^\circ$. The measured transmittances of the polarizers were $\epsilon_M{}^1 = 0.97 \pm 0.01, \epsilon_m{}^1 = 0.038 \pm 0.004, \epsilon_M{}^2 = 0.96 \pm 0.01$, and $\epsilon_m{}^2 = 0.037 \pm 0.004$. The photomultiplier detectors (RCA C31000E, quantum efficiency ≈ 0.13 at 5513Å; and RCA 8850, quantum efficiency ≈ 0.28 at 4227Å) were cooled, reducing dark rates to 75 and 200 counts/sec, respectively. The measured counter efficiencies with polarizers removed were $\eta_1 \approx 1.7 \times 10^{-3}$ and $\eta_2 \approx 1.5 \times 10^{-3}$.[9]

A diagram of the electronics is included in Fig. 1. The overali system time resolution was about 1.5 nsec . The short intermediate state lifetime ($\sim$ 5nsec) permitted a narrow coincidence window (8.1 nsec). A second coincidence channel displaced in time by 50 nsec monitored the number of accidental coincidences, the true coincidence rate being determined by subtraction. [10] A time-to-amplitude converter and pulse-height analyzer measured the time-delay spectrum of the two photons. The resulting exponential gave the intermediate state lifetime. [11]
The coincidence rates depended upon the beam and lamp intensities, the latter gradualiy decreasing during a run. The typical coincidence rate with polarizers removed ranged from 0.3 to 0.1 countx/sec, and the accidental rate ranged from 0.01 to 0.002 counts /sec. Long runs required by the low coincidence rate necessitated automatic data collections.

The system was cycled with $100-$sec counting periods. Periods with one or both polarizers inserted alternated with periods in which both polarizers were removed. Both polarizers rotated according to a prescribed sequence. For a given run, $R(\varphi)/R_0$ was calculated by summing counts for all configurations corresponding to angle φ and dividing by half the sum of the counts in the adjacent periods of the sequence in which both polarizers were moved. Data for R_1/R_0 and R_2/R_0 were analyzed in a similar fashion. The values given here are averages over the orientation of the inserted polarizer. This cycling and averaging procedure minimized the effects of drift and apparatus asymmetry.

The results of the measurements of the correlation $R(\varphi)/R_0$, corresponding to a total integration time of $\sim$ 200 h, are shown in Fig. 3. All error limits are conservative estimates of 1 standard deviation. Using the values at $22\frac{1}{2}^\circ$ and $67\frac{1}{2}^\circ$, we obtain $\delta = 0.050 \pm 0.008$ in clear violation of inequality (3). [12] Furthermore, we observe no evidence for a deviation from the predictions of quantum mechanics, calculated from the measured polarizer efficiences and solid angles, and shown as the solid curve in Fig. 3. We consider these results to be strong evidence against local hidden-variable theories.

The authors wish to express their sincerest appreciation for guidance and help from Professor Eugene Commins, to Professor Charles Townes for his encouragement of this work, and to M. Sim-

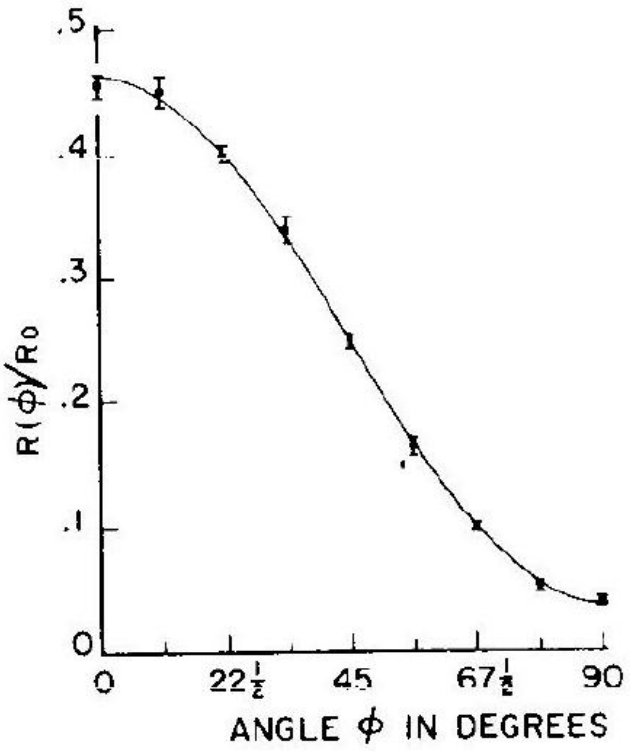


FIG. 3. Coincidence rate with angle ψ between the polarizers, divided by the rate with hoth polarizers removed, plotted versus the angle φ. The solid line is the prediction by quantum mechanics, calculated using the measured efficiencies of the polarizers and solid angles of the experiment.

mons for helpful suggestions.

[6] This assumption is much weaker than the assumption made by L. R. Kasday, J. Ullman, and C. S. Wu, Bull. Amer. Phys. Soc. 15, 586 (1970), in their discussion of the two- γ decay of positionium; sec L . R. Kasday, in "Foundations of Quantum Mechanics, Proceedings of the International School of Physics 'Enrico Fermi,' Course IL" (Academic, New York, to be published).

[7] The inequality $\Delta(\varphi) \leqslant 0$ is derived in Refs. 3 and 5. The other forms of the hidden-variable restriction are obtained by similar arguments; see S. Freedman, Ph. D. thesis, University of California, Berkeley, Lawrence Berkeley Laboratory Report No. LBL-391, 1972 (unpublished).

[8] C. A. Kocher and E. D. Commins, Phys. Rev. Lett. 18, 575 (1967); C. A. Kocher, Ph. D. thesis, University of California, Berkeley, Lawrence Berkeley Laboratory Report No. UCRL-17587, 1967 (unpublished).

[y] The counter efficiencies are given by $\eta_i = (\Omega L_i/4\pi)\, T_i \times \epsilon_i L_i$, where Ω_i is the solid angle, T_i

[8]*Work supported by U. S. Atomic Energy Commission.

[1] The best-known proof is by J. von Neumann, Mathematische Grundlagen der Quantemechanik (Springer, Berlin, 1932) [Mathematical Foundations of Quantum Mechanics (Princeton Univ. Press. Princeton, N. J., 1955)]. For a critical review of this and other proofs see J. S. Bell, Rev. Mod. Phys. 38, 447 (1966).

[2] J. S. Bell, Physics (Long Is. City, N.Y.) 1, 195 (1964).

[3] J. Clauser, M. Horne, A. Shimony, and R. Holt, Phys. Kev. Lett. 23, 880 (1969).

[4] A hidden-variable theory need not require that R_1 and R_2 be independent of the orientation of the inserted polarizer, and we do not assume this independence in our data analysis. However, the results are consistent with R_1 and R_2 being independent of angle, and for simplicity they are so denoted.

[5] M. Horne, Ph. D. thesis, Boston University, 1970 (unpublished). See also A. Shimony, in "Foundations of Quantum Mechanics, Proceedings of the International School of Physics 'Enrico Fermi,' Course IT." (Academic, New York, to be published).

is the transmission of the filter, ϵ_i is the quantum efficiency, and L_i accounts for other losses. The measurement of η_2 was made, employing the properties of the calcium cascade, by comparing the coincidence rate and the γ_1 singles rate after suitable background correction; η_1 was then inferred from the known quantum efficiencies and filter transmissions assuming that Ω_i and L_i were the same for both detector systems.

[10] An estimate of the accidental rate was also obtained from the singles rates. The two estimates gave consistent results. In fact, our conclusions are not changed if accidentals are neglected entirely; the signal-to-accidental ratio with polarizer removed is about 40 to 1 for the data presented.

[11] Resonance trapping, encountered at high beam densities, resulted in a lengthening of the observed iifetime and a slight decrease in the polarization correlation amplitude, see J. P. Barrat, J. Phys. Radium 20, 541, 633 (1059). At low beam densities the measured lifetime is consistent with previously measured values. See W. L. Weise, M. W. Smith, and B. M. Miles, Atomic Transition Probabilities, U. S. National Bureau of Standards Reference Data Series-22 (U.S. GPO, Washington, D.C., 1969), Vol. 2.

[12] The results that are of interest in comparison with the hidden-variable inequalities are $R_1/R_0 = 0.497 \pm 0.009$, $R_2/R_0 = 0.499 \pm 0.009, R\left(22\frac{1}{2}\right)/R_0 = 0.400 \pm 0.007$, and $R\left(67\frac{1}{2}^{\circ}\right)/R_0 = 0.100 \pm 0.003$. We thus obtain $\Delta\left(22\frac{1}{2}^{\circ}\right) = 0.104 \pm 0.026$ and $\Delta\left(67\frac{1}{2}\right) = -1.097 \pm 0.018$, in violation of inequalities (2).

26.9 III.8 Experimental Test of Local Hidden-variable Theories*

Abstract

We have measured the linear polarization correlation between the two photons from the $7^3S_1 \rightarrow 6^3P_1 \rightarrow 6^1S_0$ cascade of Hg^{200}. The results were used to evaluate Freedman's version of the Bell inequality, $\delta \leqslant 0$. Our result is $\delta_{\text{exp}} = +0.046 \pm 0.014$, in clear violation of the inequality and in excellent agreement with the quantum mechanical prediction, $\delta_{\text{QM}} = +0.044 \pm 0.007$. An important feature of the experiment was the explicit measurement of the initial density matrix for the cascading atoms.

We have measured the linear polarization correlation of photon pairs from the $7^3S_1 - 6^3P_1 - 6^1S_0$ cascade of Hg^{200}. Under appropriate experimental conditions, quantum mechanics (QM) predicts there should be a very strong correlation. The essence of Bell's theorem [1] is that any local hidden variable (LHV) theory restricts the strength of this correlation. This LHV restriction can be put in a form derived by Freedman, [2]

$$\delta = \left| n\left(67\frac{1}{2}^{0}\right)/n_0 - R\left(22_2^{10}\right)/n_0 \right| - \frac{1}{4} \leqslant 0. \tag{1}$$

Here the two photons are respectively detected on the $\pm Z$ axes, $R(\varphi)$ is the coincidence rate with an angle φ between the transmission axes of the polarizers, and R_0 is the coincidence rate with polarizers removed. A decisive experimental test of LHV theories can then be obtained by choosing experimental conditions such that inequality (1) is violated by the quantum mechanical predictions. [3] Previously, results have been obtained from three such experiments. The first by Freedman and Clauser [4] used the calcium cascade $6^1S_0\ 4^1P_1 - 4^1S_0$. Their results violated the inequality and were in agreement with the QM predictions. The second by Holt [5] used the mercury (Hg^{198}) cascade $9^1P_1 - 7^3S_1 - 6^3P_0$. The results satisfied the inequality and were in apparent disagreement with QM. The third, also by Clauser, [6] was recently completed using the same cascade in mercury (Hg^{202}) and the same excitation technique as Holt. The results violated the inequality and were in agreement with QM.

The present experiment used a different cascade, $7^3S_1 - 6^3P_1 - 6^1S_0$ in mercury (Hg^{200})

(see Fig. 1). The 7^3S_1 state was populated in a two-step process, i.e., electron bombardment excitation to the 6^3P_2 state followed by absorption of resonant $5461-\text{Å}$ radiation from a laser. An atomic beam was used and the two excitation steps occurred at physically different locations. Consequently, in the interaction region (where the 7^3S_1
state is populated) there are essentially no rapidly decaying states other than the cascade states. Therefore there is a one-to-one correspondence between all $4358-\text{Å}$ and $2537-\text{Å}$ photons. As a result comparatively high data accumulation rates were obtained.

The experimental arrangement is shown in Fig. 2. The mercury atomic beam passes through a solenoid electron gun where atoms are excited to the 6^3P_2 state. Laser beams tuned to the resonant frequency of the $5461-\text{Å}$ transition in Hg^{200} intersect the atomic beam at two locations. The $4358-\text{Å}$ fluorescence from the first location provides a reference to lock the laser cavity onto the Hg resonance. The second location is the interaction region. Its dimensions, defined by the intersection of the two beams, are $0.3 \times 0.8 \times 0.8$ mm^3. The first location is slightly off the atomic beam axis so that atoms which can "see" laser radiation in the first location cannot enter the interaction volume.

The laser radiation incident on the interaction region is polarized parallel to the Z axis. At the interaction region the emitted $4358-\text{Å}(2537-\text{Å})$ photons are collected over a half-angle $\theta = 19.9^\circ \pm 0.3^\circ$, pass through a pile-of-plates polarizer and a filter, and are detected on the $+(-)Z$ axis.

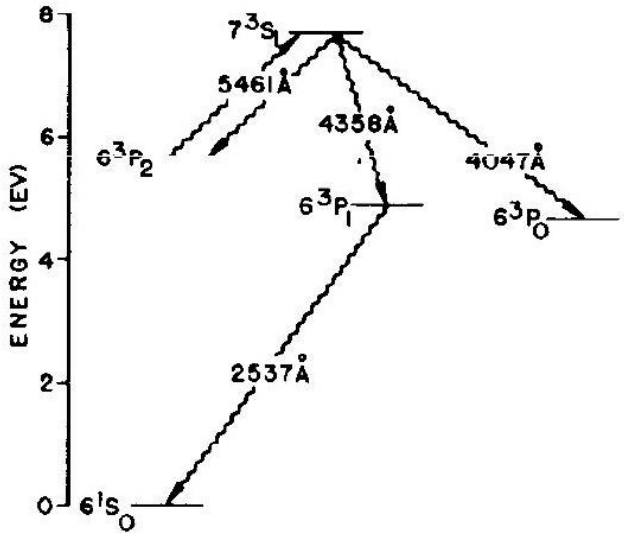


FIG. 1. Relevant energy levels and transitions in mercury

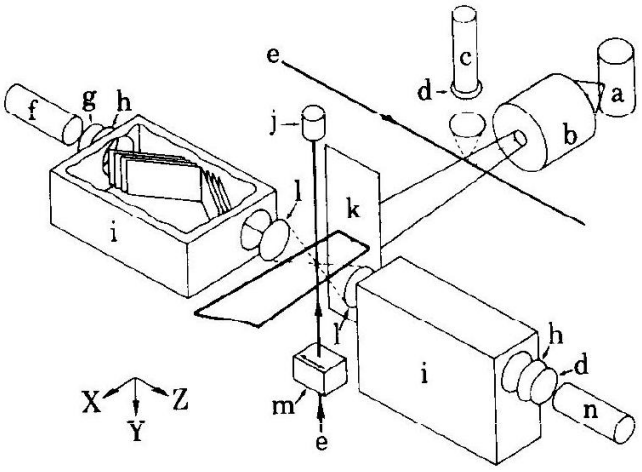


FIG. 2. Schematic of the apparatus. Polarizer plate arrangement is aiso indicaled. Actual pularizers have 14 plates. (a) Hg oven; (b) solenoid electron gun: (c) RCA 8575; (d) 4358-A filter; (e) 5461-A laser beam; (f) Amperex 56 DUVP/03: (g) 2537- filter; (h) focusing lens; (i) pile-of-plates polarizer; (j) laser beam trap; (k) atomic beam defining slit; (1) light collecting lens; (m) crystal polarizer; (n) RCA 8850.

The collection optics are lens pairs whose radii have been adjusted to minimize the Seidel spherical aberration coefficient. Each polarizer consists of two sets of seven plates symmetrically arranged so as to cancel out transverse ray displacements. The magnetic field in the interaction region is zeroed to less than 5 mG in all directions.

A valid test can only be made with zero-spin isotopes. Our beam uses mercury of natural isotupic abudance, but we selectively excite only atoms of the zero-spin isotope, Hg^{200}, to the initial state of the cascade by using 5461- radiation from a narrow-linewidth (15 MHz) tunable dye laser. By sweeping the laser frequency and observing the 4358-A fluorescence we can ob-

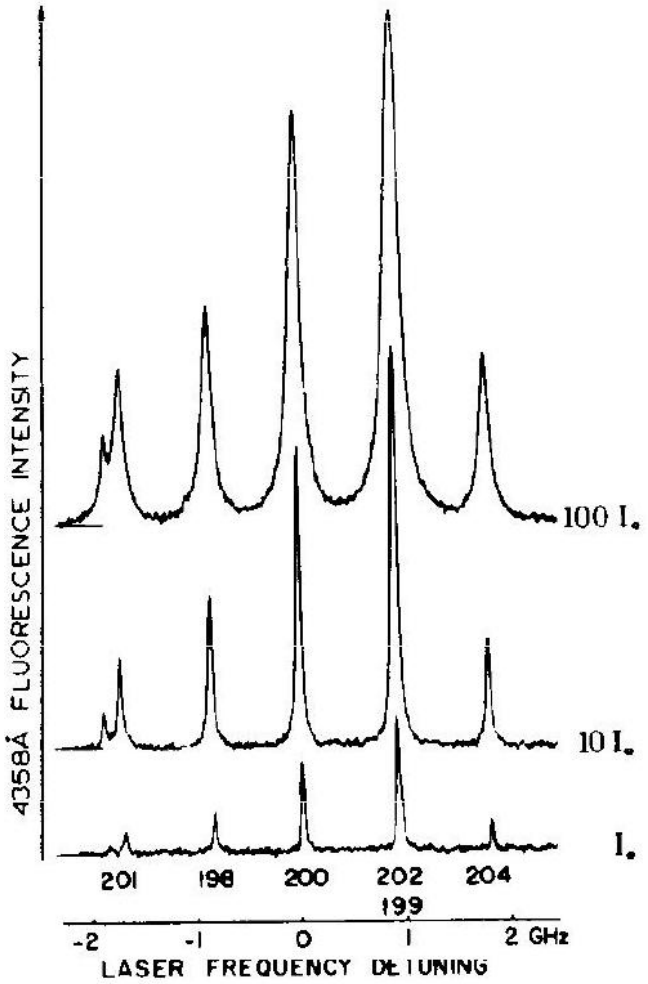


FIG. 3. Fluorescence intensity of $4358-$ Å radiation versus laser frequency for three intensities of the incident $5401-$ Å radiation. The lines for the various Hg isotopes are labeled with their mass numbers The vertical scale is the same for all three scans; the zeroes have been offset for clarity. \$I_{0

\sim 2.5 \mathrm{˜mW} / \mathrm{cm}ˆ{2}\$.}

serve the structure of the $5461-$ Å absorption line. [7] Figure 3 shows the results for the central portion of the line for three incident laser intensities. The transition is power broadened, but at our operating intensity, $I_U \sim 2.5$ mW/cm^2, the isotope separation is very clean.

The initial state of our cascade has $J = 1$. Its density matrix is 3×3 and has elements ρ_{ij} where i and j are magnetic quantum numbers. With detectors on the $\pm Z$ axes, the QM prediction for the coincidence rate $S(\varphi)$ shows no dependence on ρ_{10} or ρ_{0-1}. (The coordinate system is indicated in Fig. 2.) When ρ_{1-1} is zero, the normalized coincidence rate is

$$R(\varphi)/R_0 = \frac{1}{4}\left({\epsilon_M}^1 + {\epsilon_m}^1\right)\left({\epsilon_M}^2 + {\epsilon_m}^2\right) - \frac{1}{4}\left({\epsilon_M}^1 - {\epsilon_m}^1\right)\left({\epsilon_M}^2 - {\epsilon_m}^2\right) F(\theta)\cos 2\varphi. \qquad (2)$$

Here ${\epsilon_m}^i$ (${\epsilon_m}^i$) is the transmission efficiency of the i th polarizer for light polarized parallel (perpendicular) to the transmission axis, and $F(\theta)$ is given by

$$F(\theta) = \rho' J^2(\theta)\left[(1+\rho')\,G^2(\theta) - (1-2\rho')\,G(\theta)H(\theta) - (2-\rho')\,H^2(\theta)\right]^{-1}. \qquad (3)$$

The functions [8] $G(\theta), H(\theta)$, and $J(\theta)$ depend on the half-angle θ subtended by the light collection optics, and ρ' is given by

$$\rho' = \rho_{00'} / (\rho_{11} + \rho_{-1-1}) . \tag{4}$$

It is essential to measure ρ'; to check that ρ_{1-1} is zero; and to verify that the QM prediction, Eq.
(2), violates inequality (1).

The density matrix for atoms in the 7^3S_1 state is determined experimentally by measuring the polarization of the $4358-$ Å fluorescence at appropriate angles. It is found that at the high intensities at which the transition is saturated, the off-

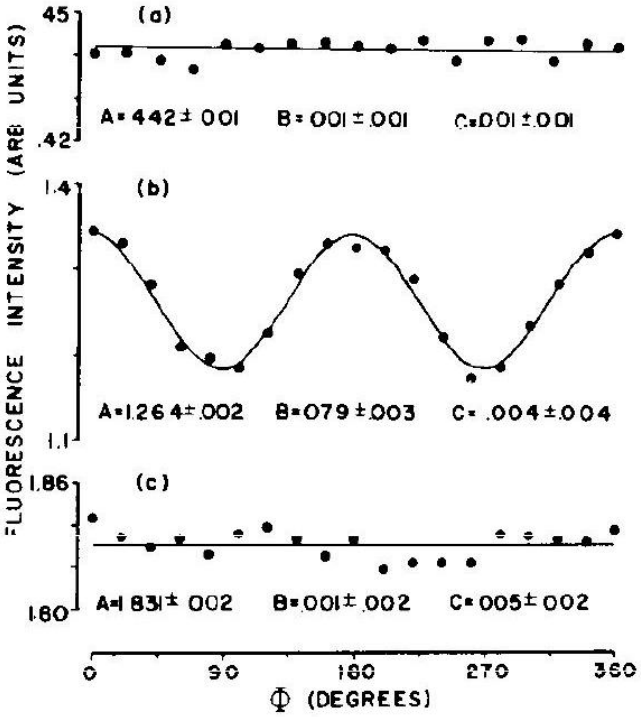


FIG. 4. Linear polarization dependences of the intensities of the cascade photons. Φ is the angle of the polarizer transmission axis with respect to the X axis. The data are least-squares fitted by a function of the form $A + B\cos 2\Phi + C\sin 2\Phi$ and the fitted parameters are given with each curve. (a) $4358-$ Å intensity on the $+Z$ axis. (b) $4358-$ Å intensity on the $-Y$ axis. (c) 2537 Å on the $-Z$ axis.

diagonal elements are nonzero and all elements are intensity dependent. With the intensity reduced to $I_0 \sim 2.5$ mW/cm^2, our data (Fig. 4) show that the density matrix has the desired form. Figure 4(a) shows the results for the $4358-$ Å fluorescence on the $+Z$ axis. The absence of a linear polarization dependence here implies $\rho_{1-1} = 0$. Figure 4(b) shows the polarization measurements of $4358-$Å radiation detected on the $-Y$ axis; from the fitted parameters we find $\mathrm{Re}\,(\rho_{10} - \rho_{0-1}) = 0$, and $\rho' = 0.633 \pm 0.005$. For completeness, Fig. 4(c) shows the polarization measurements of $2537-$ Å fluorescence on the $-Z$ axis.

The polarizer efficiency parameters are ${\epsilon_M}^1 = 0.98 \pm 0.01, {\epsilon_m}^2 = 0.97 \pm 0.01, {\epsilon_m}^1 = {\epsilon_m}^2 = 0.02 \pm 0.005$. Hence the QM prediction, Eq. (2), for the normal-

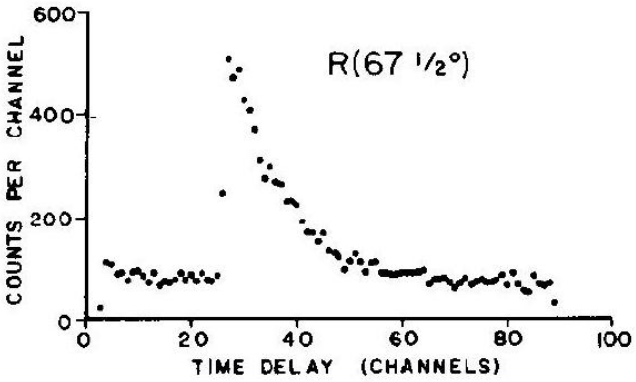


FIG. 5. Polarization coincidence spectrum. The total accumulation time is 80 min .

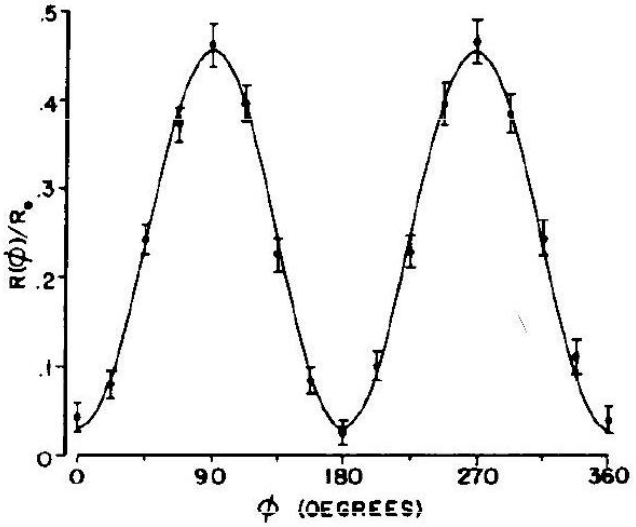


FIG. 6. Normalized polarization coincidence data from 0 to \$360ˆ{\circ \$. The datum point at 0° is duplicated at 360°. The smooth curve is a least squares fit to $R(\psi)/R_0 = A + B\cos 2\varphi + C\sin 2\varphi$. The fitted parameters are $A = 0.242 \pm 0.003; B = -0.212 \pm 0.004; C = -0.003 \pm 0.004.$}

ized coincidence rate is

$$R(\varphi)/R_0 = (0.248 \pm 0.004) - (0.208 \pm 0.004)\cos 2\varphi \tag{5}$$

and we also find

$$\delta_{\mathrm{OM}} = 0.044 \pm 0.007. \tag{6}$$

All errors are ±1 standard deviation.

Coincidence data were obtained using a time-toamplitude converter and a pulse-height analyzer. Figure 5 shows the total coincidence spectrum with $67\frac{\pi}{2}°$ between the polarizer axes. The total accumulation time for this spectrum was 80 min . To obtain the true coincidences, one must subtract out the accidental coincidence background. Consequently, the error depends on the width of the coincidence window. For our data, minimum error is obtained for a window width

of 12 to 14 channels (1.3 τ). The quality factor, defined by Freedman, [2] was $Q = 1.03$ with the polarizers removed.

Figure 6 shows the polarization data for the full 360° together with a least-squares fit. The fitted parameters are in good agreement with the QM prediction, Eq. (5).

From the $R_0, R\left(22\frac{1}{2}^\circ\right)$, and $R\left(67\frac{1}{2}^\circ\right)$ data, we find

$$\delta_{\text{exp}} = 0.046 \pm 0.014 \tag{7}$$

in excellent agreement with the QM prediction, Eq. (6), and in clear violation of the LHV restriction, inequality (1).

The authors wish to thank the many people who have contributed to this work, especially Jim McGuire, Jim Ellis, Norman Alexander, and our instrument shop personnel.
*Work supported by the Robert A. Welch Foundation, Grant No. A437, and by a grant from the Research Corportion.

[1] J. S. Bell, Physics (L. I. City, N. Y.) 1,195 (1965).
[2] S. J. Freedman, Lawrence Berkeley Laboratory Report No. LBL-391, 1972 (unpublished).
[3] J. F. Clauser and M. A. Horne, Phys. Rev. D10, 526 (1974).
[4] S. J. Freedman and J. F. Clauser, Phys. Rev. Lett. 28, 938 (1972).
[5] R. A. Holt, Ph.D. thesis, Harvard University, 1973 (unpublished).
[6] J. F. Clauser, Phys. Rev. Lett. 36, 1223 (1976).
[7] J. Blaise and H. Chantrel, J. Phys. Radium 18, 193 (1957).
[8] E. S. Fry, Phys. Rev. A 8, 1219 (1973).

26.10 III.9 Quantum Mechanics and Hidden Variables: a Test of Bell's Inequality by the Measurement of the Spin Correlation in Low-energy Proton-proton Scattering

Abstract

The inequality of Bell has been tested by the measurement of the spin correlation in proton-proton scattering. Measurements were made at $E_p = 13.2$ and 13.7 MeV using carbon analyzers of 18.6 and 29mg/cm^2, respectively, accumulating a total of 10^4 coincidences. The experimental analyzing power, geometric correlation coefficients and energy spectra are compared to the result of a Monte Carlo simulation of the apparatus. The results are in good agreement with quantum mechanics and in disagreement with the inequality of Bell if the same additional assumptions are made. The conditions for comparing the results of the experiments to the inequality of Bell are discussed.

26.10.1 I. Introduction

Since the beginning of quantum mechanics (QM) a number of physicists who contributed the most to the development of this theory had serious doubts about its logical foundations. Most of the problems were illustrated by a number of paradoxes, such as those of Einstein, Podolsky. and Rosen [1] and Schrödinger (namely, the cat paradox). [3] These discussions never died down and even today there is no theory of measurement which satisfies everybody.

One attempt to overcome these difficulties was to suppose that there are some supplementary variables outside the scope of QM ("hidden variables") which determine the result of the individual measurement. A theorem derived by J. von Neumann was taken for a long time as proof that such interpretations are impossible. But Bohm [3] in 1952 developed a model of the hidden-variables theory which was in complete agreement with the predictions of QM, and Bell [4] showed in 1965 why the theorem of von Neumann was not valid as applied to physical systems. Bell showed. too, that all hidden-variables models which give complete agreement

with QM must have an undesirable feature. They do not obey the principle of locality as stated by Einstein [5] : "If S_1 and S_2 are two systems that have interacted in the past but are now arbitrarily distant, the real, factual situation of system S_1 does not depend on what is done with system S_2, which is spatially separated from the former."

Developments [6–8] of the argumentation of Bell led for the first time in a more than 30 -year-old discussion to the possibility of a critical experimental test which could distinguish among the different interpretations. The consequences of such experimental verifications have more profound implications than just eliminating special models which
interpret the measuring process. They will test the validity of a general conception of the foundations of microphysics: the principle of locality or, as written more precisely in Ref. 7, the validity of objective local theories.

26.10.2 II. Bell's Inequality

The first derivation of the inequality, which later led to an experimental test, was given by Bell. [4] It has been generalized by Clauser et al. [6,7] In the meantime various ways of demonstration have been derived and can be found in Ref. 9 together with a description of the actual state of hidden-variables theories. We will follow here a demonstration given by Bell. [8]

To be definite we take the example of two spinparticles which have been coupled in the past in a singlet state and which are now widely separated. The principle of locality as formulated by Einstein means that each of these particles has some properties, which we will denote by λ(λ can be a whole set of variables) which do not depend on what is happening to the other particle. The result of the measurement is determined by these properties λ. We denote by A, B the result of the measurement in the direction $\overrightarrow{\mathbf{a}}$ and $\overrightarrow{\mathbf{b}}$ of the sign of the spin of the two particles respectively. For a realistic apparatus and/or if the dependence on λ is not strictly deterministic, but only stochastic, one will have

$$|A(\lambda, \vec{a})| \cdot 1 \text{ and } |B(\lambda, \vec{b})| \leqslant 1.$$

The correlation function $P(\overrightarrow{\mathrm{a}}, \overrightarrow{\mathrm{b}})$ is defined to be the mean value of the product AB and thus

$$P(\overrightarrow{\mathrm{a}}, \overrightarrow{\mathrm{b}}) = \int A(\lambda, \overrightarrow{\mathrm{a}}) B(\lambda, \overrightarrow{\mathrm{b}}) \rho(\lambda) d\lambda$$

where $\rho(\lambda)$ denotes the frequency of the properties λ with the normalization condition $\downarrow \rho(\lambda) kl\lambda = 1$. Thus,

$$\begin{aligned}
\left|P(\overrightarrow{\mathrm{a}}, \overrightarrow{\mathrm{b}}) - P\left(\overrightarrow{\mathrm{a}}, \overrightarrow{\mathrm{b}}'\right)\right| &= \Big| \int A(\lambda, \overrightarrow{\mathrm{a}}) B(\lambda, \overrightarrow{\mathrm{b}}) \rho(\lambda) d\lambda - \int A(\lambda, \overrightarrow{\mathrm{a}}) B\left(\lambda, \overrightarrow{\mathrm{b}}'\right) \rho(\lambda) d\lambda \pm \int A(\lambda, \overrightarrow{\mathrm{a}}) B(\lambda, \\
&\quad \mp \int A(\lambda, \overrightarrow{\mathrm{a}}) B\left(\lambda, \overrightarrow{\mathrm{b}}'\right) A\left(\lambda, \overrightarrow{\mathrm{a}}'\right) B(\lambda, \overrightarrow{\mathrm{b}}) \rho(\lambda) d\lambda \Big| \\
&= \left| \int A(\lambda, \overrightarrow{\mathrm{a}}) B(\lambda, \overrightarrow{\mathrm{b}}) \right| 1 \pm A\left(\lambda, \overrightarrow{\mathrm{a}}'\right) B\left(\lambda, \overrightarrow{\mathrm{b}}'\right) \Big| \rho(\lambda) d\lambda - \int A(\lambda, \overrightarrow{\mathrm{a}}) B\left(\lambda, \overrightarrow{\mathrm{b}}'\right) \Big| \\
&\quad \cdot \int |A(\lambda, \overrightarrow{\mathrm{a}}) B(\lambda, \overrightarrow{\mathrm{b}})| \left| 1 \pm A\left(\lambda, \overrightarrow{\mathrm{a}}'\right) B\left(\lambda, \overrightarrow{\mathrm{b}}'\right) \right| \rho(\lambda) d\lambda + \int \left| A(\lambda, \overrightarrow{\mathrm{a}}) B\left(\lambda, \overrightarrow{\mathrm{b}}\right.\right. \\
&\quad - 2 \left| P\left(\overrightarrow{\mathrm{a}}', \overrightarrow{\mathrm{b}}'\right) + P\left(\overrightarrow{\mathrm{a}}', \overrightarrow{\mathrm{b}}\right) \right| \text{ using } |AB| \cdot 1.
\end{aligned}$$

For coplanar vectors $\vec{a}, \vec{a}', \vec{b}, \vec{b}'$ only the angle between these vectors is important, and one can write

$$|P(\theta) - P(\theta+\gamma)| + |P(\theta+\gamma+\phi) + P(\theta+\phi)| \geq 2$$

QM predicts for this correlation function [4,17,15]

$$\begin{aligned} P(\vec{\mathrm{a}}, \vec{\mathrm{b}})_{\mathrm{QM}} &= \left\langle \vec{\sigma}, \cdot \vec{\mathrm{a}} \vec{\sigma}_2 \cdot \vec{\mathrm{b}} \right\rangle \\ &= -\cos\left(\vec{\mathrm{a}}, \vec{\mathrm{b}}\right) \\ &- -\cos\theta. \end{aligned}$$

Putting in special values for the angles θ, γ, ϕ and using the invariance of P by reflection and rotation one gets the upper limits for the absolute value of $P(\theta)$ as compared to predictions of QM in Table I. As can be seen, there is a definite contradiction between the values predicted by QM and the upper limit as implied by the inequality of Bell.

26.10.3 III. Description of a "perfect" Experimental Setup and Discussion of Realized Experiments

The inequality of Bell can be tested by special experimental devices. We will first describe an example of an ideal experiment and then discuss how the actually performed experiments differ from such an ideal arrangement.
We will take as an example Bohm's [10] version of the Einstein-Podolsky-Rosen paradox. Consider (Fig. 1) a source which prepares two particles of spin $J = \frac{1}{2}$ in an intermediate state $J = 0$. This state disintegrates by emitting the two particles with a velocity v in opposite directions. The two possible states, + and -, of the direction of spin are split up for example by Stern-Gerlach magnets and the particles are detected by the detectors d. The vectors $\vec{a}$ and $\vec{b}$ denote the orientations of the magnets. Then we define N_0 as the number of pairs of particles which enter the analyzers in coincidence (preparation of a beam of coincident particles) which would be measured in the case of charged particles of sufficiently high energy for example by the use of thin ΔE counters as entrance collimators of the analyzers without depolarization of the particles. As in Ref. 7 we define $p_1^+(\vec{a}, \lambda)$ as the probability of having a count
in the counter d_1^r, and in the same way for the other counters. For sufficiently large number N_1 we have

$$p_1^+(\vec{\mathrm{a}}) = \frac{N_1^+}{N_0} = \int P_1^+(\vec{\mathrm{a}}, \lambda)\rho(\lambda)d\lambda,$$

and clearly $p_1^+(\vec{a}, \lambda) \leqslant 1$ and $-1 \leqslant p_1^+(\vec{a}, \lambda) - p_1^-(\vec{a}, \lambda)$

1. For objective local theories one gets

$$\frac{N_{+\pm}}{N_0} = \int p_1^+(\vec{\mathrm{a}}, \lambda) p_2^+(\vec{\mathrm{b}}\ .\lambda)\rho(\lambda)d\lambda$$

where $N_{++}$are coincidences between the counters $d_1^+$and d_2^+.
Defining the measured correlation function as

$$P'_{\mathrm{meas}}\,(\vec{\mathrm{a}}, \vec{\mathrm{b}}) = \frac{N_{++} + N_{---} - N_{-+} - N_{+-}}{N_0}$$

and using the above relation for $N_{++}$and an analogous relation for N_{T-} and so on we get

$$P'_{\text{meas}}\,(\overrightarrow{\text{a}},\,\overrightarrow{\text{b}}) = \int \left|\rho_1^+(\overrightarrow{\text{a}},\lambda) - \rho_1^-(\overrightarrow{\text{a}},\lambda)\right| \left|\rho_2^+(\overrightarrow{\text{b}},\lambda) - \rho_2^-(\overrightarrow{\text{b}},\lambda)\right| \times \rho(\lambda) r(\lambda.$$

Setting

$$p_1^+(\overrightarrow{\text{a}},\lambda) - p_1^-(\overrightarrow{\text{a}},\lambda) = A(\overrightarrow{\text{a}},\lambda)$$

and

$$p_2^+(\overrightarrow{\text{b}},\lambda) - p_2^-(\overrightarrow{\text{b}},\lambda) = B(\overrightarrow{\text{b}},\lambda)$$

we see that this is equivalent to the function $P(\vec{a},\vec{b})$ defined earlier and thus must obey the same inequality, if objective local theories are valid. Quantum mechanics predicts for this correlation

TABLE I. Comparison of predictions of QM for $|P(\phi)|$ with the upper limit given by the inequality of Bell.

ϕ	Q11	Upper limit of Bell's inequality
0-	1	$\leqslant 1$
30c	$\frac{3}{2}$	$\leq \frac{2}{3}$
45	1/. 2	≤ 1
60c	1 2	[2 - $P(0)°$)]/ 3
90°	0	0

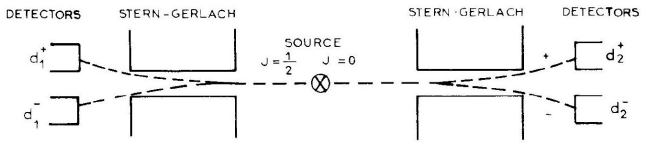


FIG. 1. Schematic experimental setup for the test of the inequality of Bell.

function

$$P'_{\text{meas}}\,(\overrightarrow{\text{a}},\,\overrightarrow{\text{b}}) = P_1 P_2 T_1 T_2 \cos\left(\overrightarrow{\text{a}},\,\overrightarrow{\text{b}}\right)$$

where $P_{1,2}$ and $T_{1,2}$ are the analyzing power and transmission of the analyzers. Therefore in order to get a contradiction with the inequality an ideal apparatus should have the property (a) $|P_1 P_2 T_1 T_2| > 1/\sqrt{2}$, which is a very stringent condition, and supposes yet that one has measured the number of particles which enter the analyzer in coincidence. Apart from this, the ideal apparatus should have the following properties:
(b) The lifetime τ of the intermediate state should be short and the source should be pulsed (or by some other information-coincidence-one should know when the particles enter the analyzers) with a resolution l, and the restrictions

$$\tau v \ll D \text{ and } t_r l \ll D,$$

where l is the velocity of the particles and D is the dimension of the apparatus. This ensures that one knows at each moment with a good precision where to find the particles in

the apparatus.
(c) The time l_v between the moment when the particles enter the analyzer and the detection should satisfy the relation

$$t_v c < d,$$

where c is the speed of light and d is the distance between the analyzers. Thus the theory of relativity excludes the coupling of the particles after or during the measurement process.
(d) The orientation $\vec{a}, \vec{b}$ of the two analyzers should be changed in an arbitrary way during the time of flight of the particles, satisfying the relation

$$(t_{\rm ch} - l_{\rm det})\, c < d$$

where $l_{\rm ch}$ denotes the time of the change of orientation and $l_{\rm det}$ denotes the time of detection of the particles. Thus one analyzer cannot "know," with a speed of exchange of information $\leqslant c$, what the other one is doing.

If *all* these conditions are satisfied the abovedefined correlation can directly be compared to the inequality of Bell without extra assumptions. To
see what can happen if there are deviations from the above-described ideal setup let us consider as an example the case where the detection probability is low, $P_{\rm det} \ll 100\%$. It is possible to imagine that for a perfect apparatus with $P_{\rm det} = 100\%$, one would measure a correlation function which agrees with the inequality of Bell. When the detection probability becomes low the properties of the particles, which determine the result of the spin measurement, determine at the same time the probability of joint detection, doing so in such a way that agreement of the counting rates with QM is reestablished. This means that the properties of the particles which determine the result of the spin measurement would determine in a correlated way other properties (in this example to be detected or not). One can imagine that for one special experiment there is such a correlation of properties. But it seems difficult to imagine that in very different experimental setups different properties will always be correlated in just such a way to reestablish agreement with QM. This shows that it is necessary to test the inequality of Bell in very different experimental conditions. If the spacelike separation of the particles and of the different parts of the measuring device is not realized, one can imagine some hypothetical coupling or exchange of information. This would mean that the result of the measurement on one particle could depend on what is done with the other particle and agreement with QM could be obtained.

The first experiment done specifically to verify the inequality of Bell was the measurement of the correlation of polarization of positronium annihilation γ rays by Kasday. [11] Agreement with QM was obtained. Somewhat later the correlation of polarization of photons of an atomic cascade was studied by Freedman and Clauser, [12] and again agreement with QM was obtained. The experiment with atomic photons has the advantage that in atomic physics one can build polarization analyzers of nearly 100% transmission and analyzing power, which is not the case for the experiment with annihilation γ rays. Some of this advantage is lost by the low probability of response of photomultipliers used to detect the photons ($\sim 10\%$) and
the fact that the second photon is not emitted in a well-defined direction with respect to the first one, but into the whole space. The photon experiment is related to a three-body phenomenon. involving the two photons and the atom which emits the photons. Thus, as in the other experiment, only a very small number of the photons detected in one analyzer is in coincidence with the photons detected in the other analyzer. In the atomic photon experiment the additional assumption necessary concerns the response probability of the photomultiplier ("no enhancement assumption"), whereas in the annihilation γ experiment it concerns the scattering process in the first scatterer.

Both types of experiments used photons. Photons cannot be localized by a Lorentz transformation. One can attribute to photons a length, the cohe rence length $l = c\tau$. where r is the speed of light and τ is the mean lifetime of the state which produced the photon. For experiments with annihilation γ rays this length is ~ 17 cm and ~ 300 cm for the atomic cascade case. These dimensions are comparable to or bigger than the dimension of the apparatus used and therefore it is not clear that the condition of localization is respected. This is why it had been suggested [13] that we use particles with a mass at rest different from zero.

We developed an experimental device to measure the spin correlation of protons after scattering in a singlet state, and this will be described in some detail below. Since the beginning of the development of this device the experimental situation for the photons became more confused. The experiment with annihilation γ rays was repeated by Faraci et al. [14] and results in contradiction with QM and in agreement with Bell's inequality were obtained. For another atomic cascade Holt and Pipkin [15] found a result which is also in contradiction with QM and in agreement with Bell's inequality. These experiments will be repeated in other laboratories, and so we can hope that in the not-too-distant future the experimental situation for the photon experiments will be clarified. [28]

26.10.4 IV. Measurement of the Spin Correiation in Low-energy Proton-proton Scattering

26.10.5 A. The Experimental Setup

In Fig. 2 the schematic experimental device is shown. A beam of protons, delivered by the Saclay tandem accelerator, hits a target containing hydrogen. After scattering, the two protons enter in kinematical coincidence into the analyzers at $\theta_{\text{lab}} = 45 \quad (\theta_{\text{cm}} = 90)$. In the analyzers the protons are scattered by a carbon foil and the coincidences between the detectors of one analyzer with the dctectors of the other are counted. The detectors of one analyzer are in the reaction plane, and the

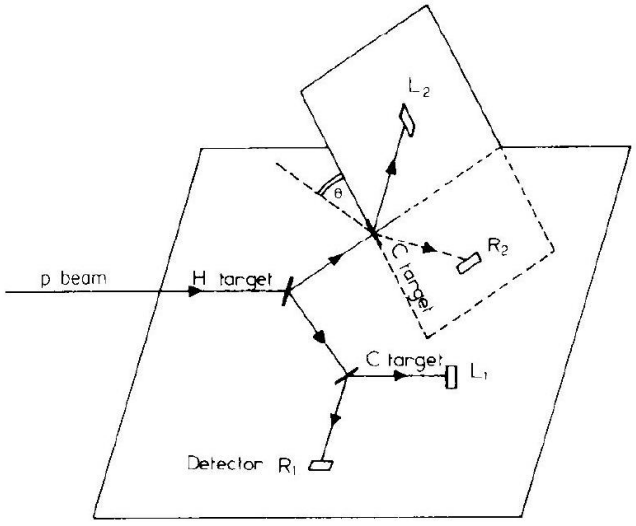


FIG. 2. Schematic experimental setup for the measurement of the spin correlation in proton-proton scattering.

detectors of the other are rotated by an angle θ around the axis defined by the protons entering in the analyzer.

We define the measured correlation function

$$P_{\text{meas}}\,(a,b) = \frac{N_{LL} + N_{RR} - N_{RL} - N_{LR}}{N_{LL} + N_{RR} + N_{RL} + N_{LR}}$$

where N_{LL} are the coincidences between left counters L_1 and L_2, and so on.
It is not possible to compare this correlation function directly with the inequality of Bell. Some extra assumptions are necessary because our apparatus does not fulfill the conditions for a perfect apparatus. The following assumptions are necessary:
H1: It is possible to construct a perfect apparatus. As in the annihilation γ case, there is no experimental method known which could give ne arly 100% analyzing power and transmission, even extrapolating present techniques. A SternGerlach apparatus is not suited for charged particles as can be shown by uncertainty relations. [16] Nonetheless, there does not seem to exist a priori an obstacle to constructing such a perfect apparatus.
H2: Our device does not fulfill the conditions of spacelike separation discussed in the preceding section. We assume that this does not affect the result of the measurement. In the experiment the coherence length can be estimated from the lifetime of the intermediate state formed in $p-p$ scattering. Because there are no sharp resonances this lifetime is of the order of $\tau \simeq 10^{-22}$sec, resulting in a coherence length of $\lambda \simeq 4 \times 10^{-13}$ cm. This is very small compared to the dimension of
the apparatus (5 cm), in distinction with the photon experiments where the coherence length and the dimension of the apparatus are of the same order of magnitude. We tried to minimize the distance between the detectors and the carbon foil, in order to prevent a hypothetical coupling between the particles after the second scattering. In our device the time of flight $t_v = 0.3$nsec, whereas $d/c = 0.2$nsec. This means that we were quite near the condition (c) in Sec. III, but we did not yet fulfill it.

The analyzing power of our measuring device is ~ 0.7 which is very similar to the one obtained in the annihilation γ experiments and, as in the case of annihilation γ 's the transmission of the analyzers is very low. Therefore the product $P_1P_2T_1T_2$ does not fulfill the conditions of a perfect device. Examples for which it is not possible to compare with the inequality without additional assumptions have been given. [7,8,11] Consider a pair of particles which enter the analyzers in coincidence. Suppose that a perfect device would give the results $p^{id}_{IL}(\vec{a},\lambda), p^{id}_{IR}(\vec{a},\lambda)$, etc. for the probability of having a count in the detectors d_{IL}, d_{IR}, etc. It makes sense to consider such a device because of assumption H1. We now make the following as sumption:

H3: The analyzing power and the transmission of the measuring apparatus can be considered as intrinsic constants of the apparatus. This means that the parameters λ which determine the result of the spin measurement do not determine in a correlated way the value of the analyzing power and/or transmission of the analyzers. A similar assumption is necessary in the atomic photon experiment concerning the response probability of the photomultipliers.

Then one can write

$$\begin{aligned} p_{1L}(\vec{\mathrm{a}},\lambda) + p_{1R}(\vec{\mathrm{a}},\lambda) &= T_1 \mid p^{id}_{1L}(\vec{\mathrm{a}},\lambda) + p^{id}_{1R}(\vec{\mathrm{a}},\lambda)\Big] \\ &= T_1, \\ p_{1L}(\vec{\mathrm{a}},\lambda) - p_{1R}(\vec{\mathrm{a}},\lambda) &= T_1P_1\left[p^{id}_{1L}(\vec{\mathrm{a}},\lambda) - p^{id}_{1R}(\vec{\mathrm{a}},\lambda)\right] \\ &= T_1P_1A(\vec{\mathrm{a}},\lambda), \end{aligned}$$

where $p_{IL}(\vec{\mathrm{a}},\lambda)$ is the probability of having a count in the left counter of the analyzer [1] and so on, and P_1 and T_1 are the mean analyzing power and transmission. Analogous equations hold for the apparatus 2.

Then for N_0 particles which enter the analyzers in coincidence, one has

$$
\begin{aligned}
N_0\,(p_{1L}-p_{1R})\,(p_{2L}-p_{2R}) =& N_0 P_1 P_2 T_1 T_2 \\
& \times \int A(\overrightarrow{\mathrm{a}},\lambda) B(\overrightarrow{\mathrm{b}},\lambda)\rho(\lambda)d\lambda \\
=& N_{LL}+N_{RR}-N_{LR}-N_{RL} \\
N_0\,(p_{1L}+p_{1R})\,(p_{2L}+p_{2R}) =& N_0 T_1 T_2 \\
=& N_{LL}+N_{RR}+N_{RL}+N_{LR}
\end{aligned}
$$

Using these relations one has

$$
\begin{aligned}
P_{\mathrm{meas}}\,(\overrightarrow{\mathrm{a}},\,\overrightarrow{\mathrm{b}}) &= \frac{N_{LL}+N_{RR}-N_{RL}-N_{LR}}{N_{LL}+N_{RR}+N_{RL}+N_{LR}} \\
&= P_1 P_2 \int A(\overrightarrow{\mathrm{a}},\lambda) B(\overrightarrow{\mathrm{b}},\lambda)\rho(\lambda)d\lambda
\end{aligned}
$$

The transmission coefficients for left-right scattering of the analyzers depend slightly on the angle ψ of the first scattering. Replacing N_0 by $dN_0/d\psi$ and introducing the dependence of the transmission coefficient on ψ, one finds after some arithmetic and integration between ψ' min and $\psi_{\max}$ a correction to the preceding formula; and the final result is, to first order in the correction term,

$$
P_{\mathrm{mcas}}\,(\overrightarrow{\mathrm{a}},\,\overrightarrow{\mathrm{b}}) = P_1 P_2 \int A(\overrightarrow{\mathrm{a}},\lambda) B(\overrightarrow{\mathrm{b}},\lambda)\rho(\lambda)d\lambda + C_s \left\{1-\left[P_1 P_2 \int A(\overrightarrow{\mathrm{a}},\lambda) B(\overrightarrow{\mathrm{b}},\lambda)\rho(\lambda)d\lambda\right]^2\right\}\cos\Big(\overrightarrow{\mathrm{a}},\,\overrightarrow{\mathrm{b}}
$$

where

$$
C_\varepsilon = \frac{\int (T_{1L}T_{2L}+T_{1R}T_{2R}-T_{1L}T_{2R}-T_{1R}T_{2L})\,d\psi}{\int (T_{1L}T_{2L}+T_{1R}T_{2R}+T_{1L}T_{2R}+T_{1R}T_{2L})\,d\psi}
$$

Defining

$$
\int A(\vec{\mathrm{a}},\lambda) B(\vec{\mathrm{b}},\lambda)\rho(\lambda)d\lambda = P_{\mathrm{exp}}(\vec{\mathrm{a}},\,\vec{\mathrm{b}})
$$

we can write

$$
\begin{aligned}
P_{\mathrm{mcas}}(\overrightarrow{\mathrm{a}},\,\overrightarrow{\mathrm{b}}) =& \frac{N_{LL}+N_{RR}-N_{RL}-N_{LR}}{N_{LL}+N_{RR}+N_{RL}+N_{LR}} \\
=& P_1 P_2 P_{\mathrm{exp}}(\overrightarrow{\mathrm{a}},\,\overrightarrow{\mathrm{b}}) \\
& + C_g\left[1-\left|P_1 P_2 P_{\mathrm{exp}}(\overrightarrow{\mathrm{a}},\,\overrightarrow{\mathrm{b}})\right|^2\right]\cos\Big(\overrightarrow{\mathrm{a}},\,\overrightarrow{\mathrm{b}}\Big)
\end{aligned}
$$

Measuring P_1, P_2, and C_5, the experimental counting rates can be used to extract $P_{\mathrm{exp}}(\overrightarrow{\mathrm{a}},\,\overrightarrow{\mathrm{b}})$.

Now we must remind the reader that in order to derive the inequality of Bell it is necessary to vary $\vec{a}$ as well as $\vec{b}$ (see Sec. II). Because in the laboratory system the two proton directions form

90 and not, as in the center-of-mass system, 180 , when rotating $\vec{a}$ and $\vec{b}$ around the propagation direction of the protons to $\vec{a}', \vec{b}'$, the vectors $\vec{a}$, $\vec{b}, \vec{a}'$, and $\vec{b}'$ are not coplanar. The prediction of QM is

$$
\begin{aligned}
P_{QM}(\overrightarrow{\mathrm{a}},\,\overrightarrow{\mathrm{b}}) &= C_{nn}\cos\Big(\overrightarrow{\mathrm{a}},\,\overrightarrow{\mathrm{b}}\Big) + C_{kp}\sin\varphi_1\sin\varphi_2 \\
&= C_{nn}\cos\varphi_1\cos\varphi_2 + C_{kp}\sin\varphi_1\sin\varphi_2,
\end{aligned}
$$

where φ_1, φ_2 are the angles by which the analyzers are turned out of the reaction plane. Using this correlation function directly one sees that it does not violate the inequality of Bell. This comes from the fact that our analyzers are sensitive only to the transversal component of the polarization. Nonetheless, it is possible to obtain a contradiction using the fact that most of the scattering passes through a $J = 0$ intermediate state and the correlation function of $J = 0$ must be invariant with respect to rotation. We can decompose the correlation function into a part $/(\overrightarrow{\mathrm{a}}, \overrightarrow{\mathrm{b}}) = f(\varphi)$ that is rotationally invariant, and another part $g(\overrightarrow{\mathrm{a}}, \overrightarrow{\mathrm{b}})$ that is not, with

$$P(\vec{a}, \vec{b}) = f(\varphi) + g(\vec{a}, \vec{b}),$$

and therefore

$$P(\overrightarrow{\mathrm{a}}, \overrightarrow{\mathrm{b}}) - g(\overrightarrow{\mathrm{a}}, \overrightarrow{\mathrm{b}}) = P\left(\overrightarrow{\mathrm{a}}', \overrightarrow{\mathrm{b}}'\right) - g\left(\overrightarrow{\mathrm{a}}', \overrightarrow{\mathrm{b}}'\right)$$

if $(\vec{a}, \vec{b}) = \left(\vec{a}', \vec{b}'\right)$. We define β such that $|\therefore (\vec{a}, \vec{b}) - \beta$ for all $\vec{a}, \vec{b}$. The singlet scattering cannot contribute to the part of $P(\overrightarrow{\mathrm{a}}, \overrightarrow{\mathrm{b}})$ that is not rotationally invariant. Therefore an upper limit for β is the probability of triplet scattering. From the measurements of Catillon el al. [14] one obtains $\beta \leqslant 0.02 \pm 0.01$. We make the following assumption:

H1: An upper limit for the contribution of triplel scallering can be obtained from the scallering of polarized protons on polarizad protons. This assumption could be eliminated by the use of a 90 (electrostatic) deflector before one of the polarimeters. This would give a 180 correlation and thus the vectors $\vec{a}, \vec{b}, \vec{a}'$, and $\vec{b}'$ would be coplanar. Introducing the above expressions in the equality gives
$|P(\varphi) + P(\varphi')| + |P(\varphi + \gamma) - P(\varphi' + \gamma)| \cdot 2 + 4\beta \cdot 2.08,$
where φ, φ' and $\varphi + \gamma, \varphi' + \gamma$ are the angles that one polarimeter is turned out of the reaction plane, whereas the other remains fixed in the reaction plane.

Quantum mechanics predicts that

$$P_{\mathrm{crp}}(\theta) = -C_{nn} \cos\theta,$$

when one analyzer is in the reaction plane and the other is rotated by an angle θ out of it (Fig. 2). Experimental values obtained by Catillon el al. [19] can be interpolated to the energies used for this
experiment (13.2 and 13.7 MeV) and give $C_{nn} = -0.95 \pm 0.015$. The deviation of C_{nn} from -1 reflects the 2_C contribution of triplet scattering. In order to get a contradiction between predictions of quantum mechanics and the inequality of Bell, we need some additional assumptions ($\mathrm{H1} - \mathrm{H4}$).

Because the analyzing power and the transmission are similar to the experiment w ith annihilation γ 's, equivalent assumptions are needed. The main difference for protons is the fact their coherence length is $\sim 10^{-13}$ cm. which is extremely small compared to the dimension of the apparatus ($\sim$ 5 cm), whereas for the photons the coherence length is larger than or comparable to the size of the measuring apparatus. Therefore for photons the locality condition seems not as clear as in the present experiment.

Even if in the atomic cascade experiments it is possible to construct polarizers of nearly 100% analy zing power and transmission, the assumption made concerning the response probability of the photomultipliers is qualitatively the same as needed here, only it concerns a more simple effect (photoelectric effect) than the scattering process here, and is better isolated from other effects such as analyzing power.

26.10.6 B. Design of the Experimental Device

The design of the experimental device is mainly conditioned by the low transmission of polarization analyzers available in nuclear physics. For the analyzers used here it was of the order of 10^{-5}; because of the coincidence between the analyzers only roughly one of 10^{10} pairs of protons which enter in the analyzers is detected in coincidence. To have, in spite of this, high enough counting rates, it is necessary to have a high beam intensity, thick targets, and large solid angles.

As hydrogen targets, polyethylene (CH_2) foils of $9mg/cm^2$ were used. The beam used of 1.5μ A with a spot size of $1.5-$ mm diameter instantly burned a hole in the target. Therefore it was necessary to construct a target rotating in an eccentric way with respect to the beam with the speed of 1rev/sec. Thus, mechanically, the targets well withstood the beam, but still a chemical burning resulted in a blackening of the target and, after some hours, the hydrogen content on the beam trace diminished by a factor of 2 . Thus every two hours the eccentricity was changed together with the orientations of the analyzers and every six hours the target was changed. Because the detectors were cooled to -20 C , ice buildup by the humidity contained in air had to be avoided and thus the opening was done under argon atmosphere.

The main problem for the analyzer was the reduction of the background. γ rays, mainly from the target, produce a background which rises exponentially for low energies and which completely covers the events of interest if one does not take great care. This background was reduced to essentially zero in the region of interest by a lead protection and by using silicon detectors 300 to 400μ thick. The use of thinner detectors would have leduced the background even more but they would not have stopped the most energetic protons ($\sim$ 6MeV) and thus the energy spectrum would have been deformed, not allowing a detailed interpretation. A careful design of slits is necessary to reduce the background produced by protons. The protons which are scattered by an angle $< 10°$ leave the analyzer by a tube which serves at the same time as a rotation axis. The mean angle of scattering of the protons detected in the analyzer was fixed to 50°.

The final design of the analyzers is shown in Fig. 3. In an early stage of the experiment, one of the analyzers contained only two detectors. This was changed to have simultaneously a measurement of the geometric correlation (see Sec. IV F). All
pieces, including beam-defining slits, were mounted on the cover of the scattering chamber and aligned to better than $\frac{1}{10}$ mm. The most important dimensions are given in Table II.

C. Monte Carlo simulation

Apart from suitable experimental tests, it seemed highly desirable to make exact calculations simulating the experimental device in order to have a supplementary control that the apparatus not show any undesirable and uncontrolled feature. At the same time this provides help for the choice of geometry and for the optimization of the apparatus. A numerical integration is excluded because of the dimension of the integrals involved. Thus a Monte Carlo evaluation of the integrals was programmed for the CII 10020 computer.

The geometry was treated exactly taking into account the three dimensions of the device. The energy loss in the targets was calculated using the tables of Northcliff and Schilling. [20] Angular straggling was taken into account. The carbon cross section and polarization were obtained using the results of phase-shift analyses. [21–24] The

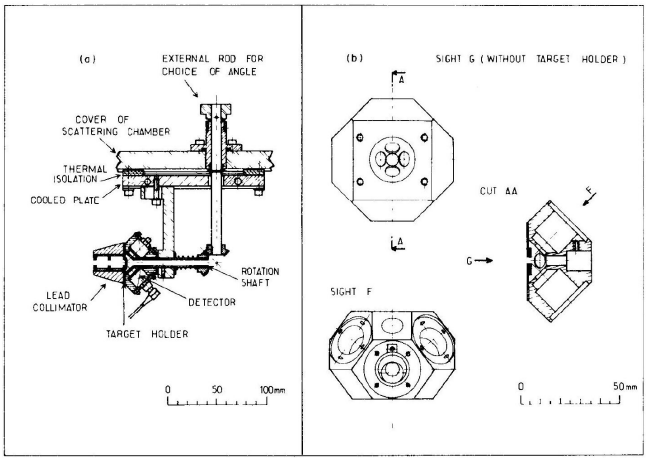


FIG. 3. Design ef the polarization analyzers: Part (a) shows the general design, and part (b) shows the details of the analyzer.

TABLE II. Most important dimensions used in the experimental device.

	Diameter (mm)	Distance (mm) from target	Number
beam-defining slit 1	2	180	1
beam-defining slit 2	2	150	1
beam-defining slit 3	1.5	50	1
beam-defining slit 4	2	20	1
entrance slit of the analyzers	4.5	51.5	1
slit before detectors	7	12.5	2

phase shifts were parametrized and resonances at 4808 and 5373 keV (see Ref. 22) were included. Good agreement with published [21–24] cross sections and analyzing powers was obtained. For Ta scatterers pure Rutherford scattering was assumed, which is justified because the energy of the protons is much lower than the Coulomb barrier.

In the following the experimental results will be compared to the results of the Monte Carlo calculation.

26.10.7 D. Measurement of the Analyzing Power

The analyzing power was measured in a doublescattering arrangement. A beam of protons of 8.07 MeV is scattered by a $2-\mathrm{mg/cm^2}$ carbon target. The scattered protons enter at $\theta_{\mathrm{lab}} = 70°$ in the analyzer and are scattered with a mean angle of 50° a second time by the carbon foil of the analyzer, and one measures the asymmetry of the counting rates of the left-right detectors. Polyethylene foils are put between the first and second target to slow down the protons to the desired energy. The protons after the first scattering are polarized to 100% with an error of less than 2%.[21,22] Thus the analyzing power is directly obtained by the measured asymmetry. Before the measurement of the analyzing power the carbon target of the analyzer was replaced by a gold target ($35\mathrm{mg/cm^2}$) to be sure that no misalignment affected the results.
The main problems connected with these measurements, once the background problem was solved, were target problems. First we used, for the analyzer, carbon targets prepared with Aquadag (Acheson Company). For proton energies above 6 MeV the experimental analyzing power was much lower than the calculated one, as stated in Ref. 25. Exposing the targets to

the beam showed no significant target contamination. Heating them for several days to 200°C gave no improvement. But when these targets were heated in a vacuum to 1500°C they lost 20% of their weight, demonstrating that they contained still
a large amount of the liquid solvent. After heating to 1500°C the targets were so frail that they could no longer be used. Thus the targets finally used were mechanically worked out of solid carbon (Carbone Lorraine).

In Fig. 4 a typical energy spectrum is shown. The results of the asymmetry measurements for the two targets used, 18.6 and 29mg/cm^2, are shown in Figs. 5 and 6. A background correction of about 2% was applied with an estimated error of 1%. The transmission of the analyzer, defined as the number of protons detected by the two detectors in the reaction plane divided by the number of protons which enter the analyzer, was 4.4×10^{-5} and 6.5×10^{-5} for the $18.6 - \mathrm{mg/cm^2}$ and the $29 - \mathrm{mg/cm^2}$ targets respectively.

26.10.8 E. Electronics Associated with Coincidence Measurements

Ablock diagram of the coincidence measurements which will be described below is shown in Fig. 7.

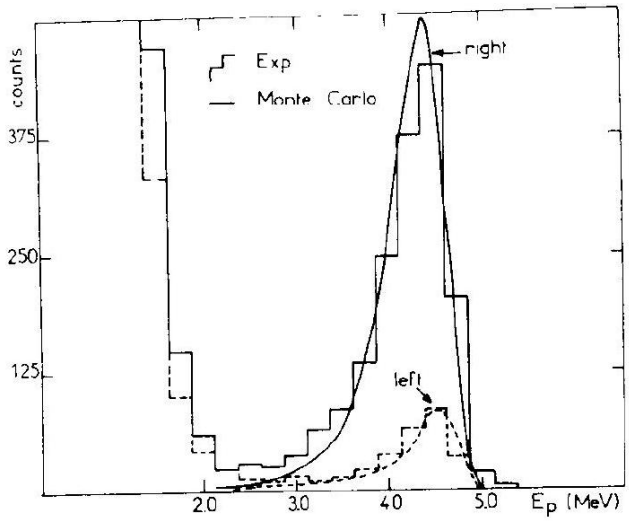


FIG. 4. Typical energy spectrum obtained in the measurement of the analyzing power of the polarimeters by double scattering of the protons, with $E_{p =8.07 \mathrm{MeV}}$, a first target of carbon of 2mg/cm^2 and a second carbon target of 18.6mg/cm^2. The protons entering in the analyzer were slowed down by a $17 - \mathrm{mg/cm^2 CH_2}$ foil to $E_p = 5.95$MeV.}

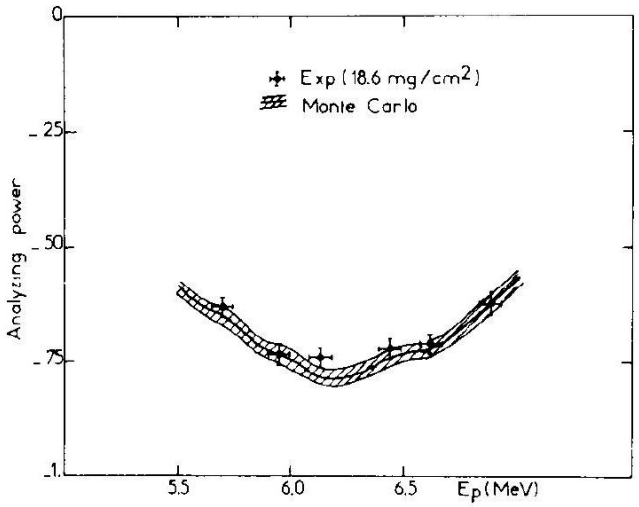


FIG. 5. Analyzing power of the analyzer with a $18.6-\mathrm{mg / \mathrm{cm}^{2}$ carbon target, as a function of the energy of the incoming protons. The width of the Monte Carlo calculation shows the uncertainty which was used to calculate the errors of the final results.}

All the electronic devices up the analog-to-digital converters (ADC) used were standard electronics developed at the SPNBE at Saclay, [26] and they provide great versatility and facility toward a fast logic control of coincidence, anticoincidence, dead time, selection of energy domain, and con-

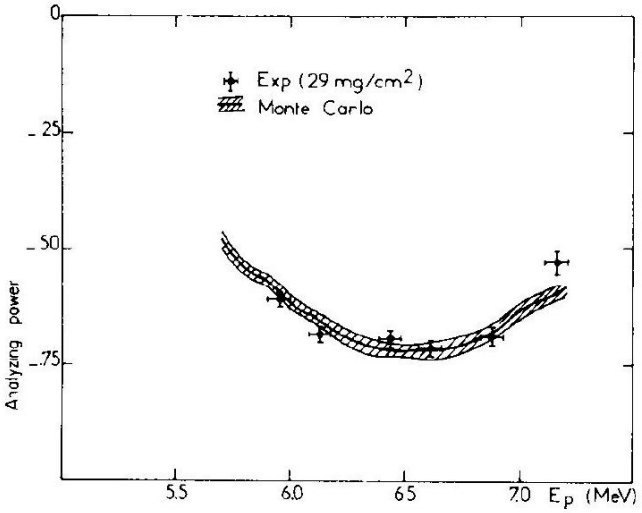


FIG. 6. Same as Fig. 5 for a $29-\mathrm{mg / \mathrm{cm}^{2}$ carbon target.}

trol of counting rates at each level before the numerical analys is.

The four detectors of each analyzer are connected to a device which delivers a rapid pulse if one, and only one of the detector pulses delivered by a rapid proportional amplifier, is above a discriminator level. If there is a coincidence in the time-to-pulse converter, linear gates are opened which let the slower energy pulse of the

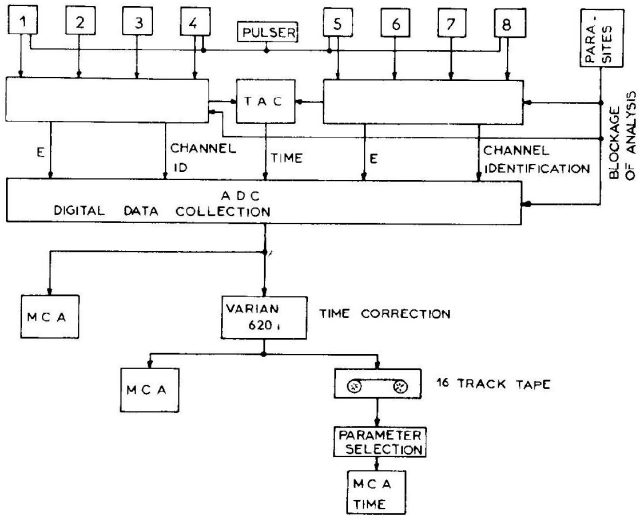


FIG. 7. Block diagram of the electronic setup used for coincidence measurements.

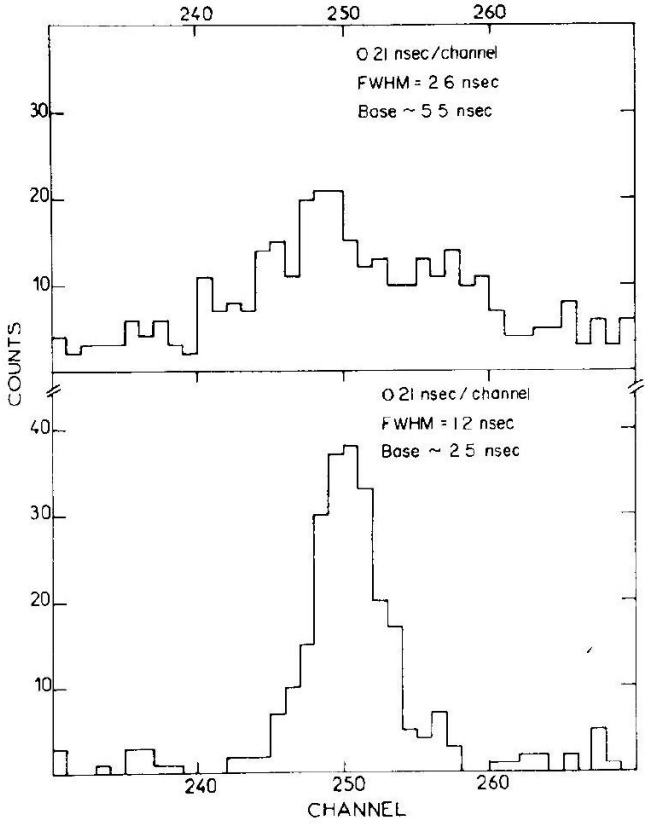


FIG. 8. Typical timc spectra before and after risetime correction by the 620 I Varian computer.

two, and only of these, detectors in coincidence pass, and an order is given to the ADC to analyze the energy and time signals. The results of this analysis together with an identification of the detectors in coincidence are sent to a Varian 620 I computer. This computer had mainly two roles: It coded the spectra following the 16 possibilities of coincidence and made a correction for the finite rise time ($\sim$ 50nsec) of the rapid pulses. The rise-time correction was done by the formula

$$t_c = t_o + \frac{C_1}{E_1 + D_1} - \frac{C_2}{E_2 + D_2}$$

where t_o and t_c are the uncorrected and the corrected times, $E_{1,2}$ is the pulse height (energy) of the signals, and C, D were adjusted to give the best time resolution. A typical uncorrected and corrected time spectrum is shown in Fig. 8. A pulse generator was used continuously to control the electronic setup.

A good protection against electric parasites had to be included to prevent these parasites from simulating coincidences. A first protection is the anticoincidence between detectors which should not be in coincidence. A supplementary protection is given by an amplifying chain mounted in the same conditions as for the detectors. A discriminator is set just above the noise, and if it delivers a pulse, the coincidence circuits at the rapid level are blocked and the analysis of the pulses by the ADC is inhibited for 200μsec. With these safeguards it was verified that over a period of several days no parasites were analyzed.

The Varian 620 I computer delivers for each event sequences containing the two energies, the corrected time, and the coded coincidence possibility, together with the number of the run. This information is written on magnetic tape. After an appropriate energy selection the 16 time spectra are accumulated in a 4096-channel memory. Because the information was written event-by-event on magnetic tape, various controls could be made out of beam time. For example, it was verified, by repeating the data reduction with different energy windows, that the results were insensitive to the setting of the energy windows within reasonable limits.

26.10.9 F. The Geometric Correlation

The geometric correlation which arises from the kinematic correlation between the protons after the first scattering and the anisotropy of the carbon (p, p) cross section gives rise to an enhancement of the coincidences between left-left and right-right detectors with respect to the

TABLE III. Results of the measurements of the geometric correlation and comparison with Monte Carlo predictions (see text).

E_p(MeV)	Target (analyzer 1)	Target (analyzer 2)	C_g (Monte Carlo)	C_g (experiment)
13.7	Ta (70mg/cm^2)	Ta (70mg/cm^2)	0.26	0.22 ± 0.01
	Ta (70mg/cm^2)	C (27mg/cm^2)	0.17	0.12 ± 0.02
	C (27mg/cm^2)	C (27mg/cm^2)	0.11	0.07 ± 0.02
13.2	Ta (70mg/cm^2)	Ta (70mg/cm^2)	0.26	0.225 ± 0.01
	Ta (70mg/cm^2)	C (18.6/mg/cm^2)	0.15	0.10 ± 0.03
	C (18.6mg/cm^2)	C (18.6/mg/cm^2)	0.09	0.05 ± 0.02

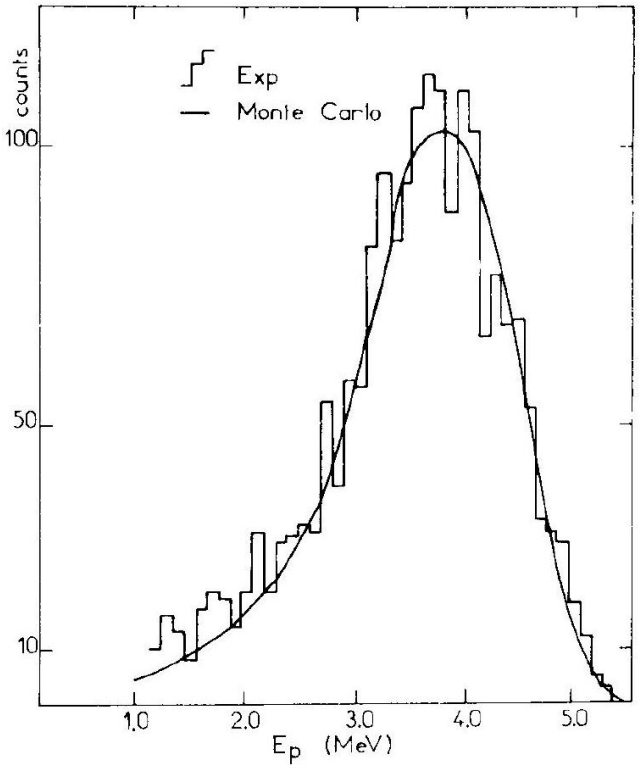


FIG. 9. Typical energy spectrum obtained in coincidence between the two analyzers with a $29-\mathrm{ng / \mathrm{cm}^{2}$ carbon target. Accidental coincidences have been subtracted.}

right-left coincidences. Two methods were used to determine the coefficient of geometric correlation.

One method consists of first measuring the geometric correlation with both carbon foils in the analyzers replaced by $70-\mathrm{mg/cm}^2$ tantalum foils The analyzing power of tantalum is zero; thus the measured correlation function is, for one pair of detectors in the reaction plane and the other rotated out of it by an angle $\theta, P(\theta) = C_e(\mathrm{Ta}-\mathrm{Ta})\cos\theta$, where C_g (Ta-Ta) is the geometric correlation coefficient for this arrangement. At the same

TABLE IV. Final results for the measured correlation function $P_{\text {meas }}{ }^{(\theta)}$ as a function of the angle θ for $18.6-\mathrm{mg'cm}^2$ and $29-\mathrm{mg'/cm}^2$ targets. Errors are statisticel one-standard-deviation errors.}

θ	19.6mg/cns′	$29\mathrm{mg/cm}^2$
0	$-0.10 \pm 0.0.5$	$-0.3 \times \pm 0.025$
30°	-0.35 ± 0.04	-0.27 ± 0.025
15	-0.29 ± 0.01	0.26 ± 0.023
60	-0.24 ± 0.04	-0.17 ± 0.025
90	-0.01 ± 0.03	$-0.03 \pm 0.0.4$

time this setup permits an easy control of the electronic setup and of the whole apparatus; the coincidence rates (about 1000 counts/hour and coincidence possibility) are about a factor of 100 larger than with the carbon foils. Then one re places one tantalum foil by a carbon foil and one gets the coefficient $C_\xi(\mathrm{Ta}-\mathrm{C})$. The coefficient for two carbon foils is connected to these coefficients by the relation

$$C_\varepsilon(\mathrm{C}-\mathrm{C}) = \frac{C_\varepsilon(\mathrm{C}-\mathrm{Ta})^2}{C_\varepsilon(\mathrm{Ta}-\mathrm{Ta})}.$$

The second method is provided by the measurement with two carbon foils, one pair of detectors turned out of the reaction plane by 90 , and the other by an angle θ. Then $P_{\mathrm{cip}}(\theta) - 0$ (see Sec. III) and $P_{\mathrm{meas}}(\theta) = -C_\xi \sin\theta$. Because the analyzers contained two detector pairs with 90 between them, simultaneously with the final results the value for the geometric correlations was obtained. Both methods gave within error bars identical results. The results are given in Table III.

As can be seen, the Monte Carlo simulation predicts a somewhat higher geometric correlation.

TABLE V. Final results for $P_{\text {exp }}(\theta)$ as compared to QM and to the limit of Bell. The results are given separately for the $18.6 - \mathrm{mg/cm^2}$ and the $29 - \mathrm{mg^2/cm^2}$ targets together with their weighted mean. $\langle P_1 P_2 \rangle$ and C_g are the values of the product of the analyzing power and of the geometric correlation coefficient, respectively, which were used to extract the values of P_{exp} from the values of $P_{m\ \mathrm{eas}}$ given in Table IV.}

0	$29\mathrm{mg/cm^2}\ \langle P_1P_2\rangle = 0.44 \pm 0.025 C_g = +0.07 \pm 0.02$	$18.6\mathrm{mg/cm^2}\ \langle P_1P_2\rangle = 0.52 \pm 0.025 C_k = 0.05$
$0'$	-0.99 ± 0.09	-0.85 ± 0.11
30°	-0.74 ± 0.08	-0.81 ± 0.10
45^c	-0.69 ± 0.08	-0.63 ± 0.09
60^c	-0.48 ± 0.07	$-0.50 + 0.10$
90°	$+0.07 \pm 0.10$	-0.01 ± 0.07

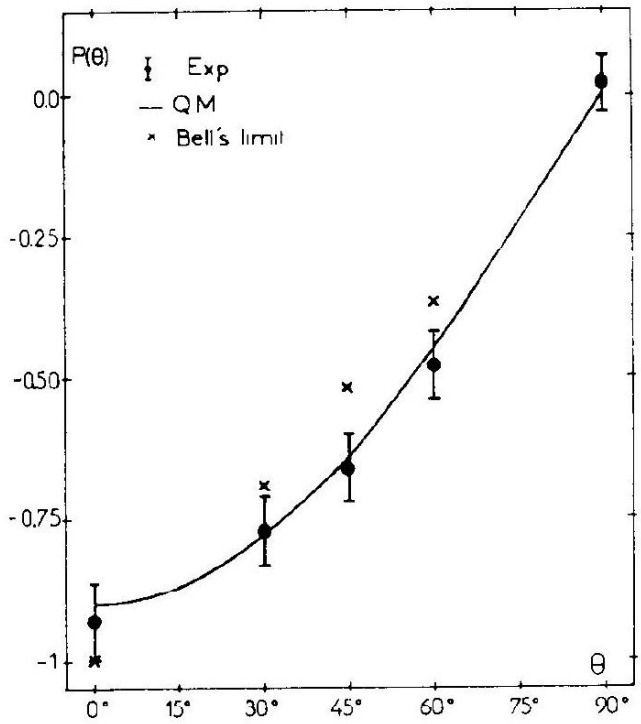


FIG. 10. Experimental results (see Table V) for $P_{\exp}(\theta)$ as compared to the limit of Bell and predictions of QM .}

The angular straggling mainly in the first target has some influence on the geometric correlation. To be sure that the values from Ref. 27 used in the Monte Carlo code were not the cause of this disagreement, we measured in a special device the angular straggling for the different targets; a good agreement was found.

The Monte Carlo calculation given in Table III was done for a perfect alignment of the apparatus. All misalignment contributes coherently to reduce the geometric corrclation. Allowing for misalignment within the experimental uncertainties, $\frac{2}{10}$ nm for the center of gravity of the beam spot and $\frac{1}{10}$ mm for other geometric misalignments, the Monte Carlo code well reproduces the experimental results. These calculations showed, too, as one would expect, that the product of the analy zing powers, $\langle P_1 P_2 \rangle$, is independent of such small misalignments.

26.10.10 G. Final Results

After all these preliminary measurements the final measurements of the coincidences of the two analyzers with carbon scatters could be made. It was verified that the final results for the correla-
tion function did not depend on the lower limits set on the energies of the detected protons. A typical energy spectrum is shown in Fig. 9. Accidental coincidences, which represent about 5% of the total, have been subtracted. For each angle about 30 individual measurements were made with different combinations of orientations of the analyzers. A total of 10^4 true coincidences were accumulated. The final results for $P_{\text{meas}}(\theta)$ are given in Table IV. In Table V the results for $P_{\text{exp}}(\theta)$ together with the values of the product of the analyzing power and of the geometric correlation used to extract the value of $P_{cip}(\theta)$ are given.

In Table V the weighted mean of these results for $P_{\text{ivp}}(\theta)$ is also given and compared to predictions of QM and to the limit of Bell. The quoted experimental errors are one-standard-deviation errors containing statistical crrors and uncertainties in the analyzing power and in the geometri-cal-correlations coefficient. In Fig. 10, the values of Table V are shown. As can be seen, the agreement with QM is good, whereas the results are in contradiction with the limit of Bell with a statistical significance of $\frac{7}{10000}$. Using the prediction of QM for $P_{\text{cvp}}(\phi_1, \phi_2) = C_{nn} \cos\phi_1 \cos\phi_2$ one obtains

$$C_{nn} = -0.97 \pm 0.05$$

in good agreement with the value of $A_{yy} = C_{mn} = -0.95 \pm 0.015$ of Catillon el al. [19]

26.10.11 V. Conclusion

The measurement of the spin correlation of protons gave good agreement with QM. To compare with the limit of Bell, as in previous experiments with photons, some extra assumptions are necessary. With these assumptions which seem natural but cannot be tested in our device, a contradiction is obtained with the limit of Bell providing an argument against the validity of this limit, and thus being in favor of nonlocal properties of microphysics.

All experiments performed up to now do not respect all the conditions necessary to permit a direct comparison with the limit of Bell. The conditions for transmission and/or analyzing power and the spacelike separation of the particles and the different parts of the measuring device [29] are not respected and seem very difficult to realize even extrapolating up today's techniques in spin or polarization correlation measurements. Thus it would be interesting to find some other type of experiments where it would be more easy to fulfill these conditions.

Bibliography

[1] A. Einstein, N. Podnlsky, and B. Rosen, Phys. Rev. 47, 777 (1935).
[2] E. Schrödinger, Naturwiss. 23, 807 (1935).
[3] D. Bohm, Phys. Rev. 85, 166 (1952); 85, 180 (1952).
[1] J. S. Bell, Rev. Mod. Phys. 38, 447 (1966); Physics (N.Y.) 1, 195 (1964).
[5] A. Einstein, in A. Einstein Philosopher Scientist, edited 1y P. Schilpp (Library of Living Philosophers, Evanston, Ill., 1949).
[6] J. F. Clauser, M. A. Horne, A. Shimony, and R. Holt, Phys. Rev. Lett. 23, 880 (1969).
[7] J. F. Clauser and M. A. Horne, Phys. Rev. D10, 526 (1974).
[8] J. S. Bcll, in Foundations of Quantum Wechanics, proceedings of the International School of Physics, Varenna, 1970. "Enrico Fcrmi," Course 49, edited by B. D'Espagnat (Academic. New York, 1972).
[9] F. J. Belinfante, A Survey of Hidden Variables Theories (Pergamon, New York, 1973).
[10] D. Bohm, Quantum Theory (Constable, London, England, 1954).
[11] L. R. Kasday, in Foundations of Quantum Mechanics, Ref. 8.
[12] S. J. Frcedman and J. F. Clauser, Phys. Rev. Lett. 28. 938 (1972).
[13] R. Fox, Lett. Nuovo Cimento 2, 565 (1971).
[14] C. Faraci, D. Gutkowski, S. Notarrigo, and A. R. Pennisi, Lett. Nuovo Cimento 9, 607 (1974).
[15] R. A. Holt and F. M. Pipkin, report (unpublished).
[16] N. F. Mott and F. E. Mayers, Theory of Atomic Collisions, 2nd ed. (Oxford Univ. Press, London, 1949).
[17] L. Wolfenstein, Annu. Rev. Nucl. Sci. 6, 43 (1956).
[18] J. Ravnal, Nucl. Phvs. 28, 220 (1961).
[19] P. Catillon, M. Chapellior, and D. Garreta. Nucl. Phys. B2, 93 (1067).
[20] L. C. Northeliff and R. F. Schilling, Nucl. Data Tables 7, 233 (1970).
215.5. *J. Moss and W. Haeborli. Nucl. Phys.* 72, 417 (1965).
[22] C. W. Reich et al., Phys. Rev. 104, 143 (1956).
[23] E. M. Bernstein and G. E. Terrel, Phys. Rev. 173, 937 (1968).
[24] J. S. Duval, A. C. L. Barnard, and J. B. Swint, Nucl. Phys. A93, 164 (1967).
[25] G. Gurd, G. Roy, and H. Leighton, Nucl. Instrum. Meth. 61, 72 (1968).
[26] M. Avril et al., Compte rendu d'activit du Dpartement de Physique Nuclaire, Note No. CEA N-1232, 1968-1969 (unpublished), p. 66, and Note No. CEA N-1390, 1969-1970 (unpublished), p. 7t.
[27] J. B. Marion and F. C. Young, Nuclear Reaction Analysis (North-Holland, Amsterdam, 1968).
[23] The experiment of Holt and Pipkin has been repeated very recently with a slightly different experimental device by J. F. Clauser [Phys. Rev. Lett. 36, 1223 (1976)], and he obtained agreement with QM . E. S. Fry [Phys. Rev. Lett. 37, 465 (1976)] made a measurement for another atomic cascade in Hg and obtained agreement with QM.
[29] An experiment with atomic cascade is in progress at Orsay, Institut d'Optique, where the orientation of the polarizers will be changed randomly [A. Aspect, Phys. Lett. 54A, 117 (1975)] .

26.11 III.10 Proposed Experiment to Test the Nonseparability of Quantum Mechanics by Aspect

Abstract

As a criterion between quantum mechanics and local hidden-variable theories, the so-called Einstein-PodolskyRosen paradox is mainly tested in the form of the statistical

correlation between polarizations of photons issuing from a cascade transition. It has been stated more than once that an improved form of the test would make use of polarizers, the orientation of which would change randomly in a time comparable with the time of flight of the two photons; the Bell locality assumption could then be replaced by a weaker assumption also considered by Bell: The Einstein principle of separability. However, to our knowledge, no workable experimental scheme has yet been proposed, and we believe the one described in this paper to be a workable one. After explaining the difference between the Bell locality assumption and the Einstein principle of separability, we briefly discuss the theoretical implications of the modified experiment. The overall scheme of the apparatus we are proposing is described, and the generalized Bell inequalities, modified for our case, are derived. As in previous experiments, supplementary assumptions are made in order to derive experimentally testable inequalities. Finally, we describe the device we intend to use to carry out the proposed scheme.

26.11.1 I. Test of the Principle of Separability

The so-called nonlocality paradox of Einstein, Podolsky, and Rosen [1] has been much discussed. Bell [2] has shown the possibility of bringing the question into the experimental domain. Then, several experiments have been proposed and performed. [3–8] All these experiments are able to discriminate between quantum mechanics and "local" hidden-variable theories that fulfill Bell's condition of locality: The setting of a measuring device does not influence the result obtained with another remote measuring device (nor does it influence the way in which particles are emitted by a distant source). Most of the experiments contradict these local hidden-variable theories, [4,5,7] although conflicting results exist. [6,8]

Although such a condition of locality looks highly reasonable, it is not prescribed by any fundamental physical law. Following a suggestion made by Bell, [2] we are proposing an experiment able to discriminate between quantum mechanics and "separable" hidden-variable theories fulfilling Einstein's principle of separability [9,10] that we can formulate in the following way for the experiments under consideration: The setting of a measuring device at a certain time (event A) does not influence the result obtained with another measuring device (event B) if the event B is not in the forward light cone of event A (nor does it influence the way in which particles are emitted by a source if the emission event is not in the forward light cone of event A).

Any theory fulfilling Bell's condition of locality also obeys Einstein's principle of separability. But one can conceive separable theories that do not fulfill Bell's condition of locality; such theories
take into account the possibility of interactions between remote measuring devices (i.e., these theories do not fulfill Bell's condition of locality), but these interactions do not propagate with velocity greater than that of light (i.e., these theories obey Einstein's principle of separability). These theories were not within the reach of previous experiments, but they could be tested with a modification of these experiments.

To discuss this point, let us recall the optical transposition of Bohm's "Gedankenexperiment" [11] as performed by Freedman and Clauser [4] (Fig. 1). Letting $N(a_i, b_j)$ be the joint detection rate when the polarizers are in orientations a_i and b_j (the value ∞ represents the removal of the corresponding polarizer), one considers the quantiy

$$S = [1/N(\infty,\infty)][N(a_1,b_1) - N(a_1,b_2) + N(a_2,b_1) + N(a_2,b_2) - N(a_2,\infty) - N(\infty,b_1)] \quad (1)$$

where a_1, a_2, b_1, b_2 denote specific orientations of the polarizers in successive measurements. Local hidden-variable theories fulfilling Bell's condition of locality predict (modulo a supple-

mentary assumption on the detector's efficiency) that S is constrained by the generalized Bell inequalities [3,12–15]

$$-1 \leqslant S \leqslant 0 \tag{2}$$

For certain values of the orientation parameters a_1, a_2, b_1, b_2 the quantum-mechanical predictions violate the inequalities (2). Hence an experimental test between the conflicting theories is possible.

It has been emphasized that a crucial point in the derivation of the Bell inequalities is the locality assumption. [16] These inequalities could not be

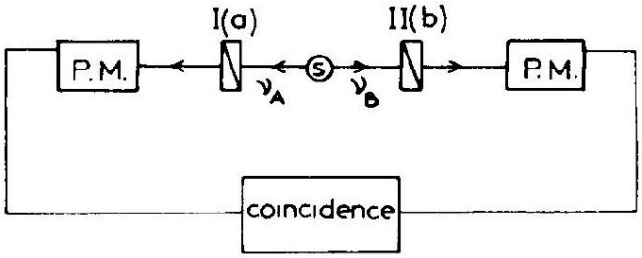


FIG. 1. Optical transposition of Bohm's "Gedankenexperiment." The correlated photons ν_A and ν_B, issuing from the cascade source S, impinge upon the linear polarizers I and II in orientations a and b. The rate of joint detections by the photomultipliers is monitored for various couples of orientations (a, b).}

proved if the response of one polarizer was depending on the orientation of the other one (or if the emission of the pairs of photons was depending on the orientations of the polarizers). In the previous experiments, such interactions are not precluded by the principle of separability because "the settings of the instruments are made sufficiently in advance to allow them to reach some mutual rapport by exchange of signals with velocity less than or equal to that of light". [2] Therefore the separable theories that do not fulfill Bell's condition of locality cannot be tested by the previous experiments.

To test these theories, it has been proposed [2,13,15,17] to change rapidly, repeatedly, and independently the orientations of the polarizers. Then one finds as a consequence of the principle of separability that the response of one polarizer, when analyzing a photon, cannot be influenced by the orientation of the other polarizer at the same time (when analyzing the coupled photon); likewise, the way in which a pair of photons is emitted cannot be influenced by the orientations of the polarizers when later analyzing this pair. Therefore, for such improved experiments, inequalities (2) can be derived from the principle of separability, with no further locality assumption made. Since inequalities (2) still conflict with the quantum-mechanical predictions, such modified experiments would be able to discriminate between quantum mechanics and separable hidden-variable theories.

A result consonant with the quantum-theory predictions would imply the rejection of separable hidden-variable theories. But as a matter of fact, it would imply more. [18] According to a recent analysis [19] it would constitute an experimental confirmation of the reality of the nonseparability introduced formally in the quantum theory. More generally, d'Espagnat [20] pointed out that such a result would entail consequences practically amounting to a disproof of the principle of separability, and he showed that these consequences (violation of some general assumptions) could be derived without reference to any specific theory (in particular without incorporating in the general assumptions just mentioned any a priori hypothesis

about the existence of hidden variables [21]). Then, some reinterpretations of the quantum theory. would be untenable, while others would be upheld. [22]

26.11.2 II. Proposed Experimental Scheme and Corresponding Generalized Bell Inequalities

Several authors [2,13,15,17] have already proposed to change rapidly and repeatedly the orientations of the polarizers, but few experimental practical suggestions have been given. One could think of using Kerr or Pockels cells, allowing changes in the polarization orientations in less than one nanosecond. Unfortunately, there are several drawbacks: Only very narrow beams could be transmitted, yielding very low coincidence rates; as these cells heat up, and then become inoperative, long runs would be prohibited. Last, a very sophisticated system would be needed for monitoring the change in time of the orientations; the calibration of the system would thus be exceedingly difficult.

We believe that these difficulties could be overcome by using optical commutators (Fig. 2). During a short time interval, the commutator C_A directs the photons ν_A towards the polarizer I_1; then its state changes and, during the following period, it directs ν_A towards the polarizer I_2. The commutator C_B works similarly with the photons ν_B, independently of C_A. The time intervals between two commutations are taken to be stochastic, so that two states of the commutator, separated by a time longer than the autocorrelation time, are statistically independent. The autocorrelation time

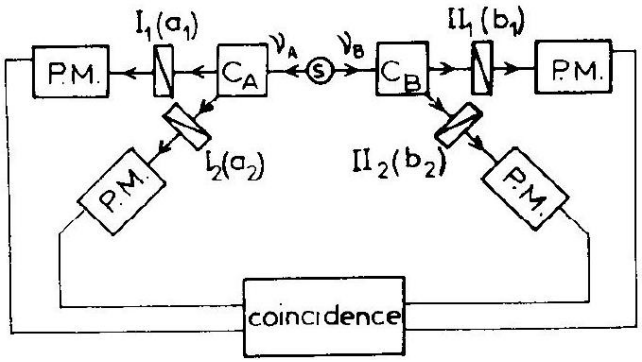


FIG. 2. Proposed experimental scheme. The commutator $C_{A} directs the photon ν_A either towards polarizer I_1 (in orientation a_1) or towards polarizer I_2 (in orientation a_2). Similarly C_B directs ν_B towards Π_1 or Π_2 (in orientations b_1 and b_2). The two commutators work independently in a stochastic way. The four joint detection rates are monitored, and the orientations a_1, a_2, b_1, and b_2 are not changed for the whole experiment.}

of each commutator is taken as short as L/c; L denotes the distance between the commutators and c denotes the speed of light.

One guesses that the separability assumption then leads to inequalities analogous to Bell's, with the arguments the same as in Sec. I[23,24]

Let us proceed to the actual derivation of the modified inequalities. We use the formalism of hidden-variable theories, but, as emphasized in Sec. I, the validity of the result will be more general.

Each emitted pair of photons is assumed to be characterized by a hidden variable λ (λ might stand for any number of parameters). We denote by t_1 the time of emission [25] of a pair of photons in the laboratory frame, and by $\hat{u}(\lambda, t_1)$ the probability distribution of λ. At the time $t_2 = t_1 + L/2c$ the photons ν_A and ν_B impinge upon the commutators. We define

"commutation functions" $\hat{\alpha}_i(t)$ and $\hat{\beta}_f(t)$ ($i = 1$ or 2 and $j = 1$ or 2), the values of which are 1 or 0 according as, respectively, the photons are sent along the corresponding channel or not; $\hat{\alpha}_i(t)$ and $\hat{\beta}_j(t)$ are of course λ independent. We denote by $t_3 > t_2$ the time at which the photons are anlayzed by the polarizers, and by $\hat{\alpha}_i(\lambda, t_3)$ and $\hat{\alpha}_j(\lambda, t_3)$ the corresponding response functions, the values of which are 1 or 0 according as the corresponding photon does or does not pass the polarizer. Thus $\hat{\alpha}_i(t_2)\,\hat{\beta}_j(t_2) \times \hat{\hat{G}}_i(\lambda, t_3)\,\hat{\hat{d}}_j(\lambda, t_3)$ assumes the value 1 if both photons ν_A and ν_B emerge from the polarizers I_i and Π_j and 0 otherwise. Finally, the probability that a pair of photons ν_A and ν_B emerge in coincidence from I_i and Π_j is

$$P_{ij} = \lim_{T\to\infty} \frac{1}{T} \int_T dt_1 \int d\lambda \hat{u}(\lambda, t_1)\,\hat{\alpha}_i(t_2)\,\hat{\beta}_j(t_2) \times \hat{Q}_i(\lambda, t_3)\,\hat{\Phi}_j(\lambda, t_3) \tag{3}$$

where the considered λ is the initial value at the time t_1 of emission.

Following Bell, we can generalize this to the case where the polarizers themselves contain hidden variables contributing to the result. We denote by λ'_{I_i} and λ'_{I_j} the instrumental parameters of each polarizer; then the response of each polarizer is $\hat{Q}_i\left(\lambda, \lambda'_{I_i}, t_3\right)$ and $\hat{Q}_j\left(\lambda, \lambda'_{I_i}, t_3\right)$. This formalism is also appropriate for a stochastic theory, [16] since λ'_{I_i} and λ'_{II}, can be taken as random variables without any specific interpretation. Then the probability P_{ij} assumes the form

$$P_{ij} = \lim_{T\to\infty} \frac{1}{T} \int_T dt_1 \int d\lambda \int \cdots \int d\lambda'_{\mathrm{I}_1} \cdots d\lambda'_{\mathrm{II}_2} \hat{u}\left(\lambda, \lambda'_{\mathrm{I}_1}, \ldots, \lambda'_{\mathrm{II}_2}, t_1, t_3\right) \times \hat{\alpha}_i(t_2)\,\hat{\beta}_j(t_2)\,\hat{\alpha}_i\left(\lambda, \lambda'_{\mathrm{I}_i}, t_3\right) \hat{\mathrm{B}}_j\left(\lambda, \lambda'_{\mathrm{II}_j}, t_3\right) \tag{4}$$

where $\hat{u}(\cdots)$ is the probability distribution of λ at time t_1 and of the instrumental parameters at time t_3.

Correlations may exist between the instrumental parameters λ'_{I_i} and λ'_{I_j}. However, in accordance with the principle of separability, correlations at time t_3 can be produced only by common causes at times $t \leqslant t_1$. Introducing these common causes in formula (4), one remarks that these common causes are always coupled with λ : then for simplicity these common causes are included as a part of the fully general λ.

In accordance with the principle of separability, the given λ at times $t \leqslant l_1$, describe in a complete manner all the correlations between the instrumental responses at time t_3; therefore the conditional probability distribution of the instrumental parameters, given a particular value of λ, is factorized. [26] Hence, with $\hat{u}\left(\lambda, \lambda'_{\mathrm{I}_1}, \ldots, \lambda'_{\mathrm{II}_2}, t_1, t_3\right)$ expressed as a function of the probability distribution $\hat{\rho}(\lambda, t_1)$ of λ at time t_1 and of the conditional probability distributions of each instrumental parameter, P_{ij} (formula 4) assumes the form

$$P_{ij} = \lim_{T\to\infty} \frac{1}{T} \int_T dt_1 \int d\lambda \hat{\rho}(\lambda, t_1)\,\hat{\alpha}_i(t_2)\,\hat{\beta}_j(t_2) \times \hat{A}_i(\lambda, t_3)\,\hat{B}_j(\lambda, t_3) \tag{5}$$

where $\hat{A}_i(\lambda, t_3)$ and $\hat{B}_j(\lambda, t_3)$ are the average val-ues–over the respective instrumental parame-ters-of the instrumental response functions at time t_3.

When integrating over time, we must consider the possibility of interactions between the commutators and the other devices. The principle of separability precludes instantaneous interactions but not retarded ones. Hence the response of polarizer I_i (for instance) at time

t_3 might depend upon the state of commutator C_A at times $t \leqslant t_2$ and also upon the state of commutator C_B at times $t \leqslant t_2 - L/c$. Similarly, the emission at time t_1 might depend upon the states of both commutators at times $t \leqslant t_1 - L/2c$. Taking into account these possible interactions, it can be shown (see Ap-pendix)-by using the assumed properties of the commutators (stochastic independent workings, autocorrelation times shorter than L/c)-that the
probability of coincident emergence factorizes as

$$P_{ij} = \alpha_i \beta_j \int d\lambda \rho(\lambda) A_i(\lambda) B_j(\lambda) \tag{6}$$

where α_i and β_j denote the averages over time of the commutation functions $\hat{\alpha}_i(t)$ and $\hat{\beta}_j(t), \rho(\lambda)$ is a function with the properties of a probability distribution, and $A_i(\lambda)$ and $B_j(\lambda)$ are functions related to the responses of polarizers I_i and Π_j, con strained by the inequalities

$$\begin{aligned} 0 \leqslant A_i(\lambda) \leqslant 1, \\ 0 \leqslant B_f(\lambda) \leqslant 1. \end{aligned} \tag{7}$$

With the same notations, the probabilities that one photon emerges from I_i (or Π_j) are (respectively)

$$\begin{aligned} P_{i0} = \alpha_i \int d\lambda \rho(\lambda) A_i(\lambda) \\ P_{0j} = \beta_i \int d\lambda \rho(\lambda) B_j(\lambda) \end{aligned} \tag{8}$$

Thus, using the principle of separability, we have derived a factorized form similar to the definition of objective local theories. [15] Nevertheless, there is a large difference: The response of one polarizer, which (given λ) depends upon its orientation, might also depend upon the orientations of the other polarizers (since we do not make the Bell locality assumption). Similarly, the way in which the pairs of photons are emitted [and therefore $\rho(\lambda)$] might depend upon the polarizers' orientations. But, in our experiment, all the orientations remain unchanged during the whole course of the experiment; hence, in formula (6), $\rho(\lambda)$ does not depend upon the indices i or j; likewise, $A_i(\lambda)$ does not depend upon the index j [nor does $A_1(\lambda)$ depend upon i].

Therefore, the derivation of Clauser and Horne [15] holds. Inequalities (7) entail

$$-1 \leqslant U \leqslant 0 \tag{9}$$

with (λ is dropped for simplicity)

$$U \equiv A_1 B_1 - A_1 B_2 + A_2 B_1 + A_2 B_2 - A_2 - B_1.$$

After multiplication by $\rho(\lambda)$ and integration, one obtains

$$-1 \leqslant S \leqslant 0 \tag{10}$$

with

$$S \equiv \frac{P_{11}}{\alpha_1 \beta_1} - \frac{P_{12}}{\alpha_1 \beta_2} + \frac{P_{21}}{\alpha_2 \beta_1} + \frac{P_{22}}{\alpha_2 \beta_2} - \frac{P_{20}}{\alpha_2} - \frac{P_{01}}{\beta_1}. \tag{11}$$

Inequalities (10) are isomorphic to the generalized Bell inequalities. [15] On the other hand, the quantum-mechanical predictions, which are

$$\begin{aligned} P_{ij} &= \frac{1}{2}\alpha_i\beta_j \cos^2(a_i, b_j), \\ P_{i0} &= \frac{1}{2}\alpha_i \\ \text{and} & \\ P_{0j} &= \frac{1}{2}\beta_j \end{aligned} \tag{12}$$

lead to a violation of the inequalities (10), the maximum of which occurs respectively for

$$(a_1, b_1) = (b_1, a_2) = (a_2, b_2) = \begin{cases} 22.5^\circ \\ \text{or} \\ 67.5^\circ \end{cases}$$

and

$$(a_1, b_2) = \begin{cases} 67.5^\circ \\ \text{or} \\ 202.5^\circ \end{cases} \tag{13}$$

For these specific orientations, we indeed have

$$S = \begin{cases} 0.207 \\ \text{or} \\ 1.207 \end{cases}$$

All the quantities involved in formula (11) are probabilities of coincident-or single-emergence and could, in principle, be measured. We thus have a test for separable hidden-variable theories. This test will be operational if we find means for measuring these probabilities and designing commutators obeying the assumptions we have made.

26.11.3 III. Testable Inequalities

Although theoretically measurable, the probabilities in formula (11) cannot be measured directly for two reasons. [3,15] First, optical photomultipliers have a low quantum efficiency; hence the rate of joint detection will be lower than the true rate of coincident emergence from the corresponding polarizers. Second, in atomic cascades only a fraction of pairs fly in opposite directions (since we have a three-body decay); hence a photon ν_A (for instance) may impinge upon commutator C_A and be analyzed while the corresponding ν_B is lost; therefore the rate of single detection is not a faithful measurement of the probability that a single photon is transmitted by the corresponding polarizer.

Denoting by N the average rate of emission of processed pairs (i.e., with both photons impinging upon the commutators) and by ϵ_{ij} a numerical factor accounting for the quantum efficiency of the corresponding photomultipliers, the rate of joint detection may be expressed as

$$N_{ij}(a_i, b_j) = \epsilon_{ij} P_{ij} N \tag{14}$$

As in previous work, [3,4,8,12] we assume that ϵ_{ij} does not depend on whether or not the photons have

passed through a polarizer. [27] We also assume that the average rate of pair emissions N is not changed when a polarizer is removed [although, as stated in Sec. II, we accept that $\hat{u}(\lambda, t)$ might be changed]. Therefore the rate of joint detection in channels I_i and II_j when the corresponding polarizers are removed will be

$$N_{ij}(\infty, \infty) = \epsilon_{ij}\alpha_i\beta_j N \tag{15}$$

where $\alpha_i\beta_j$ is the probability of a coincident emergence from the commutators C_A and C_B along the corresponding channels.

We thus obtain

$$\frac{P_{ij}}{\alpha_i\beta_j} = \frac{N_{ij}\left(a_i, b_j\right)}{N_{ij}(\infty, \infty)} \tag{16}$$

and then the four first terms in formula (11) are put as functions of measurable quantities.

One more assumption is needed to render the two last terms of S measurable: that the probability that a photon emerges out of a polarizer does not depend upon whether or not another polarizer has been removed [28] (although, as stated above, we accept that the elementary response might be changed).

Therefore, if the polarizer II_j is removed, the probability of joint emergence of ν_A from polarizer I_i and of ν_B along channel Π_j is $\beta_j P_{i0}$ (see Appendix), and the rate of joint detections, with polarizer II, removed, is

$$N_{ij}\left(a_i, \infty\right) = \epsilon_{ij}\beta_j P_{i0} N. \tag{17}$$

We finally obtain

$$\begin{aligned} \frac{P_{i0}}{\alpha_i} &= \frac{N_{ij}\left(a_i, \infty\right)}{N_{ij}(\infty, \infty)} \\ \frac{P_{0j}}{\beta_j} &= \frac{N_{ij}\left(\infty, b_j\right)}{N_{ij}(\infty, \infty)} \end{aligned} \tag{18}$$

and the two last terms in formula (11) can be measured.

On the whole, S in formula (11) is expressed as

$$\begin{aligned} S = &\frac{N_{11}\left(a_1, b_1\right)}{N_{11}(\infty, \infty)} - \frac{N_{12}\left(a_1, b_2\right)}{N_{12}(\infty, \infty)} + \frac{N_{21}\left(a_2, b_1\right)}{N_{21}(\infty, \infty)} \\ &+ \frac{N_{22}\left(a_2, b_2\right)}{N_{22}(\infty, \infty)} - \frac{N_{2j}\left(a_2, \infty\right)}{N_{2j}(\infty, \infty)} - \frac{N_{11}\left(\infty, b_1\right)}{N_{i1}(\infty, \infty)} \end{aligned} \tag{19}$$

The four quantities $N_{ij}\left(a_i, b_j\right)$ are measured during one single run of the experiment, and this is a very significant difference between our proposal and the previous schemes. The other quantities are measured in auxiliary calibrations.

Concluding this section, we have been able to define a practical scheme for measuring the probabilities, modulo some reasonable assumptions which, however, restrict somewhat the generality of the derivation of Sec. II.

26.11.4 IV. Overall Experimental Setup

Clauser et al. [3] have already discussed the case of nonideal polarizers and extended beams. These features of a realistic experiment decrease somewhat the quantum-mechanical violation

of the inequalities (10). Significant experiments have nevertheless been carried out to test the locality condition. Our experiment could be built with the same sort of source, polarizers, and detecting devices.

The specificity of our experiment is the presence of two optical commutators. These can consist of acoustic standing waves working as adjustable gratings (Fig. 3). The deviation of a light beam by strong interactions with an acoustic wave has been studied [29] both theoretically and experimentally. We are planning to use commutators with a surface of 4 cm^2 and an angular aperture of $1° \times 30°$. By appropriately adjusting the various parameters, we should be able to obtain one single beam diffracted, i.e., two channels.

The transmitted and diffracted beams will be modulated in opposition at twice the frequency of the sound wave. We expect the modulation rate of the transmitted beam to be over 90%, and polarization independent.

We finally must discuss to what extent our commutators obey the assumptions stated in Sec. II. Since the modulation rate is not exactly 100% and the commutation is not instantaneous, the values of the commutation functions $\hat{\alpha}_i(t)$ and $\hat{\beta}_j(t)$ are not restricted to 0 and 1 . Nevertheless, the reasoning in Sec. II still holds if, with $\hat{\alpha}_i(t)$ and $\hat{\beta}_j(t)$ denoting the probability that a photon is directed towards channel I_i or Π_j, these commutation func-

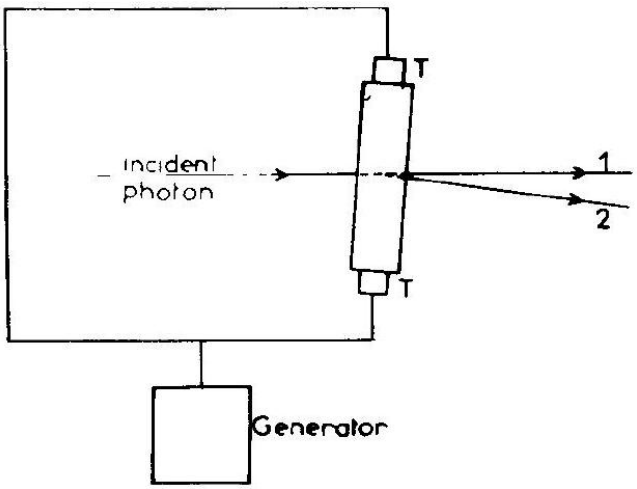


FIG. 3. Optical commutator. The generator supplies two identical transducers T, producing an acoustic standing wave in a crystal. The diffracted beam (channel 2) is modulated at twice the frequency of the standing wave. The transmitted beam (channel 1) can be modulated at a rate greater than 90%; hence the commutation is nearly complete.

tions do not depend on the hidden variable λ. This makes one more assumption. If it is unsatisfied, a fraction of the photons could be directed one way or the other, depending on the value of λ, and a "conspiracy" of the commutators and polarizers could decrease the difference between the quantummechanics predictions and the separable hiddenvariable theories predictions. However, if the quantum-mechanics predictions were vindicated for various modulation rates, the occurrence of such a conspiracy might appear as a priori unlikely. Nevertheless, such a "conspiracy" could be avoided by inhibiting the detectors when the commutation functions assume values significantly different from 0 or 1 (during the rise time).

Another difficulty is that the commutators are operated periodically and not in a truly stochastic way. However, the significant requirement is that we have two independent commutation functions, each with autocorrelation time shorter than L/c say, shorter than 20 nsec if L is 6 m . It seems that these conditions will be fulfilled if the commutators are separately driven by macroscopic generators whose frequencies deviate independently. We can drive a

pseudorandom deviation of the frequency of each commutator, and a direct action of the source upon the driving mechanisms (and possibly upon the operator's descision; see footnote 13 of Ref. 15) seems very unlikely. For instance, the standing-wave frequency can vary between 100 and 125 MHz , and the commutation frequency will vary between 200 and 250 MHz . Then the autocorrelation time, which is of the order of the inverse of the line width, is about 20 nsec . If a sweeping of the frequency over a broad line turned out to be too difficult, a supplementary assumption should be exhibited: The polarizers have no "memory," i.e., they can be influenced by signals received at a certain time from the commutators (with a certain delay) but they cannot store all this information for a long time and extrapolate in the future even if there is some regularity in the working of the commutators. With this very natural supplementary assumption, the experiment would be significant even with periodic commutations.

26.11.5 V. Brief Conclusion and Acknowledgments

We believe that the experimental scheme we are proposing, although it is not an ideal one, is interesting in that it embodies a device for changing the orientations of the analyzers in a time comparable to the time of flight of the photons. Such a feature has been considered a crucial one by quite a few workers in the field, and therefore such experiments are worth making, even if they are not ideal.

The author gratefully acknowledges Professor C. Imbert and Dr. O. Costa de Beauregard for having suggested this study and for many fruitful discussions. He especially thanks Dr. J. S. Bell for his encouragement, and Professor B. d'Espagnat for his thorough consideration and discussion of the theoretical aspects of our scheme.

26.11.6 Appendix

The probability P_{ij} in Eq. (11) is the time average of the quantity [see Eq. (5)]

$$\hat{F}_{ij}(\lambda, t_1) = \int d\lambda \hat{\rho}(\lambda, t_1)\, \hat{\alpha}_i(t_2)\, \hat{\beta}_j(t_2) \times \hat{A}_i(\lambda, t_3)\, \hat{B}_j(\lambda, t_3)$$

where $t_2 = t_1 + L/2c$ and $t_3 - t_2$ is the time of flight of photons between a commutator and a polarizer.

Since the commutators work in a stationary stochastic way, we may replace the time average by ensemble averages. Denoting by $X(t)$ and $Y(t)$ random variables specifying the states at the time t of commutators C_A and C_B, respectively, we replace the time functions " by functions of these random variables. Taking care of the various possible interactions (as explained in Sec. II) we obtain

$$\begin{aligned}
&\hat{\alpha}_i(t_2) \to \tilde{\alpha}_i[X(t_2)] \\
&\hat{\beta}_j(t_2) \to \tilde{\beta}_j[Y(t_2)] \\
&\hat{\rho}(\lambda, t_1) \to \tilde{\rho}[\lambda, X(t_0), Y(t_0)] \\
&\hat{A}_i(\lambda, t_3) \to \tilde{A}_i[\lambda, X(t_0), X(t_2), X(t_4), Y(t_0)] \\
&\hat{B}_j(\lambda, t_3) - \tilde{B}_j[\lambda, Y(t_0), Y(t_2), Y(t_4), X(t_0)]
\end{aligned}$$

and in general

$$\hat{F}_{ij}(\lambda, t_1) - \tilde{F}_{ij}[\lambda, X(t_0) \cdots Y(t_4)]$$

where

$$t_0 \leqslant t_1 - L/2c$$

and

$$t_1 - L/2c < t_4 < t_2.$$

As the two commutators are working independently, $X(t)$ and $Y(t)$ are independent random variables. As the autocorrelation time of each commutator is shorter than L/c, $X(t_0)$ and $X(t_2)$ are independent random variables, and so are $Y(t_0)$ and $Y(t_2)$.
We average $\bar{F}_{ij}$, i.e., we integrate after multiplying by the probability distribution

$$\tilde{g}\left[X(t_0), X(t_2), X(t_4)\right] \hbar\left[Y(t_0), Y(t_2), Y(t_4)\right]$$

in a factorized form since $X(t)$ and $Y(t)$ are independent. Integrating over $X(t_2)$ and $X(t_4)$, we then define

$$A_i\left[\lambda . X(t_0), Y(t_0)\right] = \left\{\alpha_1 \tilde{g}'\left[X(t_0)\right]\right\}^{-1} \times \iint dX(t_2)\, dX(t_4)\, \bar{g}\left[X(t_0), X(t_2), X(t_4)\right] \tilde{\alpha}_i\left[X(t_2)\right] \tilde{A}_i\left[\lambda, X(t_0), X(t_2), X(t_4)\right]$$

where

$$\tilde{g}'\left[X(t_0)\right] = \iint dX(t_2)\, dX(t_4)\, \tilde{g}\left[X(t_0), X(t_2), X(t_4)\right]$$

is the probability distribution of $X(t_0)$ and α_i is the average of $\tilde{\alpha}_i\left[X(t_2)\right]$. Remembering that $\tilde{A}_i$ assumes values 0 or 1 and that all the factors are positive, we obtain

$$0 \leqslant A_i\left[\lambda, X(t_0), Y(t_0)\right] \leqslant \left\{\alpha_i \tilde{g}'\left[X(t_0)\right]\right\}^{-1} \iint dX(t_2)\, dX(t_4)\, \tilde{g}\left[X(t_0), X(t_2), X(t_4)\right] \tilde{\alpha}_i\left[X(t_2)\right]$$

hence, remarking that $\int dX(t_4)\, \bar{g}\left[X(t_0), X(t_2), X(t_4)\right]$ factorizes, because $X(t_0)$ and $X(t_2)$ are independent random variables, we obtain

$$0 \leqslant A_i\left[\lambda, X(t_0), Y(t_0)\right] \leqslant 1$$

By a completely similar fashion, with $\hbar'\left[Y(t_0)\right]$ replacing $\tilde{g}'\left[X(t_0)\right]$, we obtain

$$0 \leqslant B_f\left[\lambda, X(t_0), Y(t_0)\right] \leqslant 1$$

The average of $\tilde{F}_{ij}$ is then

$$P_{ij} = \alpha_i \beta_j \iiint d\lambda dX(t_0)\, dY(t_0)\, \tilde{g}'\left[X(t_0)\right] \tilde{h}'\left[Y(t_0)\right] \tilde{\rho}\left[\lambda, X(t_0), Y(t_0)\right] A_i\left[\lambda, X(t_0), Y(t_0)\right] B_j\left[\lambda, X(t_0),\right.$$

For simplicity we can include $X(t_0)$ and $Y(t_0)$ into the parameter λ, thus obtaining formulas (6) and (7). Similarly, the single probability that a photon emerges from polarizer I_i is the time average of

$$\int d\lambda \hat{\rho}(\lambda, t_1)\, \hat{\alpha}_i(t_2)\, \hat{A}_i(\lambda, t_3)$$

and, through the same procedure as above, we obtain formula (8).
Finally, the joint probability of photon ν_A emerging from polarizer I_i and photon ν_B emerging from commutator C_B into the channel II_j is the time average of

$$\int d\lambda \hat{\rho}(\lambda, t_1)\, \hat{\alpha}_i(t_2)\, \hat{\beta}_j(t_2)\, \hat{A}_i(\lambda, t_3)$$

Remembering that $X(t_2)$ and $Y(t_2)$ are independent, we obtain $\beta_j P_{i0}$ as the expression of this probability; this expression is used in Sec. III [Eq. (17)].

[1] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. 47, 777 (1935).
[2] J. S. Bell, Physics 1, 195 (1965).
[3] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. 23, 880 (1969).
[4] S. J. Frcedman and J. F. Clauser, Phys. Rev. Lett. 28, 938 (1972).
[5] L. Kasday, in Foundations of Quantum Mechanics, Proceedings of the International School of Physics "Enrico Fermi," Course 49, edited by B. d'Espagnat (Academic, New York, 1972).
[6] G. Faraci, D. Gutkowski, S. Notarrigo, and A. R. Pennisi, Lett. Nuovo Cimento 9, 607 (1974).
[1] M. Lamehi-Rachti and W. Mittig, Phys. Rev. D (to be published).
[8] R. A. Holt, Ph.D. thesis, Harvard University, 1973
(unpublished).

[9] The words "locality" and "separability" (and likewise "local" and "separable") are sometimes taken as synonymous. However, the specific definitions given here are natural and, in the context of the present paper, useful.
[10] The expression "principle of separability of Einstein" is used by B. d'Espagnat in Conceptual Foundations of Quantum Mechanics (Benjamin, Reading, Mass., 1971). This principle is applied to "the real, factual situation of the system" [A. Einstein, in Albert Einstein: Philosopher-Scientist, edited by P. Schilpp (Open Court, La Salle, Ill., 1949)]; it is more stringent than the principle of causality; for instance, in the Einstein-Podolsky-Rosen situation, the principle of separability may be violated, although one cannot send orders
faster than light.

[11] D. J. Bohm, Quantum Theory (Prentice-Hall, Englewood Cliffs, N. J., 1951).
[12] M. A. Horne, thesis, Boston Univ., 1970 (unpublished).
[13] A. Shimony, in Foundations of Quantum Mechanics (Ref. 5).
[14] E. P. Wigner, Am. J. Phys. 38, 1005 (1970).
[15] J. F. Clauser and M. A. Horne, Phys. Rev. D 10, 526 (1974).

[16] J. S. Bell (in Ref. 5) and Clauser and Horne (Ref. 15) have proved that the hypothesis of determinism is not necessary to derive inequalities conflicting with some quantum-mechanical predictions. The latter have shown that such inequalities hold for objective local theories which are "essentially...stochastic hidden variable theories with a certain local character considered by Bell" (see Ref. 15).

[17] Y. Aharonov and D. Buhm, Phys. Rev. 108, 1970 (1957).

[18] The hypothesis of Furry (that the wave function of a many-body system tends to factorize into a product of localized states when the two parts are separated) would be rejected without the locality assumption (see Ref. 17).

[19] H. P. Stapp, LBL Report No. 3837, 1975 (unpublished).
[20] B. d'Espagnat, Phys. Rev. D 11, 1424 (1975).

[21] The idea that the hypothesis of the existence of a hidden variable would not be necessary to derive Bell's inequalities is in several papers [see for instance L. E. Ballentine, Phys. Today 27 (No. 10), 53 (1974); A. Baracca, C. J. Bohm, and B. J. Hiley, report (unpublished); see also Ref. 15 and a recent paper of J. S. Bell: CERN Report No. TH. 2053, 1975 (unpublished)]. [22] A mong the authors who have considered a possible rejection of the principle of separability, Costa de Beauregard considers "the paradoxical scheme accepting an indirect spacelike connec-

tion via the two timelike vectors connecting the cascade event to the commutation events (and to the two subsequent counting events)." He goes on to say the following: "The corresponding space-time channels are indeed carrying waves and, moreover, the calculation of the quantal correlation probabilities does imply the phase binding between these waves. In this sense the (indirect) spacelike correlation, or nonseparability, predicted by the quantum theory, can be said to be physical and mathematical and logical.
"This correlation is nevertheless paradoxical, inasmuch as it asserts that the two (apparently) independent reductions of the wave function occurring in the
distant pieces of apparatus are indeed in contact through their common past (and, thus, not really independent).
"This implied in some sense that Einstein's prohibition to telegraph into the past does not hold at the level of the individual quantal stochastic event (transition, or Ψ collapse). This is in line with the intrinsic timesymmetry also postulated in classical statistical mechanics for the individual stochastic event" (private communication).
See also O. Costa de Beauregard, unpublished work and work reported in Proceedings of the International Conference on Thermodynamics, edited by P. T. Landsberg (Butterworths, London, 1970), p. 540.
[23] A. Aspect, Phys. Lett. 54A, 117 (1975).
[24] A modification of our scheme has been suggested by J. F. Clauser (private communication). The two detectors I_1 and I_2 (Fig. 2) could be "or-wired", giving the equivalent of a single-variable polarizer with an orientation jumping from a_1 to a_2 and reversely. The time of change of the orientation should be monitored in order that the experiment be significant.
[25] The time of emission is not actually the same for the two photons, but our derivation remains valid when the lifetime of the medium state is shorter than the time of flight of the photons.
[26] A similar argument is used by Bell for a very general derivation of inequalities [J. S. Bell, CERN Report No. TH. 2053, 1975 (unpublished)].
[27] Clauser and Horne (Ref. 15) found a weaker assumption for previous experiments. However, the widening of their reasoning to our case is not straightforward.
[28] This hypothesis may appear as strong as the Bell condition of locality. Actually it is quite a different hypothesis, concerning the probability and not the elementary response. It could then be experimentally tested with an ideally efficient photomultiplier. We can practically make several tests; for instance, we can verify that

$$\frac{N_{i1}\left(a_i,\infty\right)}{N_{i1}(\infty,\infty)}=\frac{N_{i2}\left(a_i,\infty\right)}{N_{i2}(\infty,\infty)}$$

Such verifications would give good confidence in our hypothesis.
[29] J. M. Bauza, C. Carles, and R. Torguet, Acustica 30, 137 (1974); V. N. Mahajan and Jack D. Gaskill, Optica Acta 21, 893 (1974).
rs' Note: A letter of 7 July 1982 from Alain Aspect to W.H.Z. its that the experiment proposed in this paper has been comd by Alain Aspect, Jean Dalibard, and Grard Roger, and that esults will be submitted to Physical Review Letters. They find with the two commutators separated by the distance $L = c \cdot 0^{-8}$ s, and with the choice of polarization observable switched $r^1 0^{-8}$ s, the correlation parameter S, defined by Eq. (19) in
the paper, is $S_{ExP} = 0.101 \pm 0.020$. "This result violates the generalized Bell's inequality ($-1 \leqslant S \leqslant 0$) by 5 standard deviations and is in good agreement with [the quantum-mechanical prediction] $S_{QM} = 0.112$ [estimated for the actual experimental setup]. . . . The commutators did not work completely at random, but of course were driven by two independent generators. . . . The total duration of data accumulation was 7 hours."

26.12 III.11 Complementarity in the Double-slit Experiment: Quantum Nonseparability and a Quantitative Statement of Bohr's Principle

Abstract

A detailed analysis of Einstein's version of the double-slit experiment, in which one tries to observe both wave and particle properties of light, is performed. Quantum nonseparability appears in the derivation of the interference pattern, which proves to be surprisingly sharp even when the trajectories of the photons have been determined with fairly high accuracy. An information-theoretic approach to this problem leads to a quantitative formulation of Bohr's complementarity principle for the case of the double-slit experiment. A practically realizable version of this experiment, to which the above analysis applies, is proposed.

26.12.1 I. Introduction

In Einstein's version of the double-slit experiment, [1,2] one can retain a surprisingly strong interference pattern by not insisting on a 100% reliable determination of the slit through which each photon passes. The analysis leading us to this conclusion involves the following considerations. The plate which receives the kick from each photon can either be stopped and its position measured, or released and its momentum measured. These two options give us two ways of subdividing the original ensemble of photons: (1) according to the measured position of the plate, and (2) according to the measured momentum of the plate. In case (1) each subensemble produces a perfect but differently shifted interference pattern. In case (2) each subensemble produces a smeared out pattern, but also gives us some information about the photons' paths. We will thus be led to study the following questions. Does our choice of what to measure affect the total interference pattern? Do we not violate the complementarity principle by measuring both the fringes and the kick? Can this kind of experiment be performed in practice?

A monochromatic wave passing through the familiar apparatus shown in Fig. 1 will produce a perfect interference pattern on plate 3. This kind of experiment was used by Young to demonstrate the wave nature of light, and by Davisson and Germer to demonstrate the wave nature of electrons. How does one reconcile this result with the fact that these same photons or electrons also have distinctly particlelike features, such as being individually detectable? For if they are indeed particles, then each one should go through a definite slit, and we should see a sum of single-slit diffraction patterns, rather than the observed interference pattern. This apparent
contradiction has served as an archetypal example of the wave-particle duality encountered in the microworld. As stated by Feynman, the doubleslit experiment is a phenomenon "which has in it the heart of quantum mechanics; in reality it contains the only mystery" of the theory. [3] The traditional resolution of this problem, consistent with the rest of quantum mechanics, states that unless we actually measure the path of each photon (for definiteness let us restrict our attention to photons; similar arguments apply to any other particle), we have no right to maintain that any given photon actually follows a definite path. Indeed, according to this view, if we were to succeed in measuring the path of each photon, then the interference pattern would be destroyed. Thus, we can observe either the wave properties or the particle properties of light, but not both simultaneously.

At the Fifth Solvay Congress at Brussels, Finstein devised a modification of the double-slit experiment by which he hoped to show the inconsistency of quantum mechanics. [1,2] He considered an experiment in which the first screen (Fig. 1) is free to move up or down. Photons deflected toward a given slit always impart a characteristic momentum to screen 1. Thus,

Einstein hoped that by measuring the momentum imparted one could determine the path of each photon without disturbing the interference pattern. If that were the case, then the complementarity principle would be proven false.

Bohr, in his defense of the consistency of quantum mechanics, pointed out that in order to deduce the slit through which the photon will pass from a knowledge of the final momentum of screen 1 , one would also have to know the initial momentum of screen 1 to within an uncertainty $\Delta p - (s/L)p = (h/\lambda) \times (s/L)$($\lambda$ is the wavelength of the light), since this is the difference between the momenta

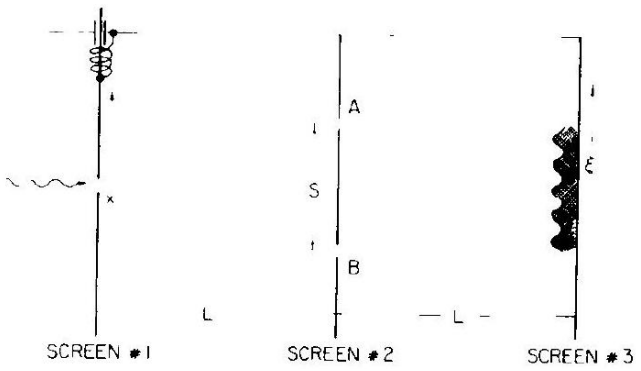


FIG. 1. Path determination in the double-slit experiment, as proposed by Einstein (Ref. 2).

transferred by photons following the two possible paths to the final screen. But then the Heisenberg uncertainty principle requires that the initial position of screen 1 be uncertain by at least $\Delta x \sim h/\Delta p = \lambda s/L$. This is exactly what is needed to wash out the interference pattern, since this Δx is the spacing between fringes. In this way Bohr succeeded in defending the consistency of quantum mechanics. [1]

The purpose of this paper is to examine Bohr's idea in detail; that is, we will find out exactly what interference pattern is produced when we attempt to determine the slit through which each photon passes. To do this, we shall represent the plate as a quantum-mechanical harmonic oscillator. The photon and the plate, having once interacted, become nonseparable parts of a single quantum-mechanical system. This forces us to consider the effect of our measurement of the plate on the photon wave function, and, consequently, on the interference pattern produced by these photons.

In the next section we shall derive the interference pattern attenuated as a result of our measurements on the position of the plate. There we shall also obtain the distribution of momentum of plate 1 associated with the relevant photons, that is, those which contribute to the image on the photographic plate.

In Sec. III we shall find what partial interference patterns correspond to ensembles of photons correlated to definite final momenta of the first plate. We shall also show that although these partial interference patterns depend on the measurements performed on the first plate, the total interference pattern (the sum of the partial interference patterns) is always the same. In Sec. IV we shall find an analogy between this situation and the celebrated Einstein-RosenPodolsky paradox.

Section V discusses in terms of Shannon's theory
the information one can obtain about the slit through which the photon passed. The complementarity principle is stated in terms of an inequality, which sets the limit on the amount of retrievable information about the photons' paths (photon-particle) for an assumed sharpness of the interference pattern (photon-wave). A practically realizable version of Einstein's double-slit experiment is discussed in Appendix A. Appendix B gives details of the proof of the inequality derived in Sec. V.

26.12.2 II. Approximate Path-determination

Let us now analyze in more detail the experiment described in Sec. I. Assuming that the Heisenberg uncertainty principle holds, let us ask exactly to what extent the interference pattern is smeared out if we insist on determining the path of each photon with a given accuracy. In the spirit of Bohr's rebuttal, we will represent screen 1 by a quantum-mechanical wave function.

The harmonic-oscillator wave function is a natural choice, since it satisfies (in its lowestenergy state) the equality

$$\Delta x \Delta p = \hbar/2,$$

thus minimizing the cost (disturbance of photon's phase due to Δx) of obtaining information about the photon's momentum with an error Δp.[11] Both in the position (x) and wave-vector (k) representation it is given by a Gaussian:

$$\begin{aligned} \psi(x) &= \pi^{-1/4} a^{-1/2} \exp\left(-x^2/2a^2\right), \quad \Delta x^2 = a^2/2, \\ \phi(k) &= \pi^{-1/4} a^{1/2} \exp\left(-a^2 k^2/2\right), \quad \Delta k^2 = 1/\left(2a^2\right), \end{aligned} \tag{1}$$

where $k = p/\hbar$ is the x component of the wave vector of plate 1. [One sees that $(\Delta x)(\Delta k) = \frac{1}{2}$, the minimal irreducible demand of the uncertainty principle.]

The object of this section is to calculate the interference pattern one obtains when plate 1 has this wave function. But first we need to state the assumptions we will be making regarding the photon wave function in a single slit experiment. Let us consider for example the wave function at plate 3 of photons which have passed through slit A, slit B being closed for the time being. This wave function is

$$\mu_A(\xi) = f(\xi) \exp\left\{ i(2\pi/\lambda) \left[L^2 + (\xi - s/2)^2\right]^{1/2} \right\},$$

where f is a slowly varying envelope function whose presence is due to the fact that the slit is not infinitesimally narrow. For an ordinary slit, f would be the usual diffraction pattern. Moreover, one could also consider a slit containing one or another type of lens, and this would lead to a different envelope function. For example, the process of apodization can be used to smooth out the diffraction pattern. [12] In any case, all we ask is that there be a region $|\xi| < \xi_0$ in which $f(\xi)$ is essentially constant. We will then restrict our attention to a section of plate 3 where $|\xi| < \xi_0$ and $|\xi| \ll L$. There the wave function can be approximated by

$$\mu_A(\xi) = f(0) e^{i\alpha(0)} e^{ik_0 \xi}$$

where $\alpha(\xi) = (2\pi/L)\left[L^2 + (s^2/8) + (\xi^2/2)\right]$ and $k_0 = (\pi s)/(L\lambda)$. Similarly, the wave function for photons coming only from slit B is

$$\mu_B(\xi) = f(0) e^{i\alpha(\xi)} e^{-ik_0 \xi}$$

When we superimpose these two wave functions, the common factor $e^{i\alpha(i)}$ does not contribute to the interference pattern. We will therefore omit this factor throughout the rest of this paper. Finally, coming back to the double-slit experiment, since we have abandoned the usual normalization in considering only a part of plate 3 , our convention will be to let the average of the interference pattern over one period be 1.

Just after each photon passes, we can measure exactly either the position or momentum of plate 1. Let us assume for now that we measure the position, and let us calculate the resulting interference pattern. In this case we know exactly where each photon starts its journey to plate

3. All photons starting at the same place x form a subensemble whose contribution $I_x(\xi)$ to the total interference pattern is perfect, but shifted by an amount $\Delta\xi = -x$:

$$I_x(\xi) = 1 + \cos 2k_0(\xi + x)$$

where $k_0 = \pi s/(L\lambda)$, and s and L are defined in Fig. 1. The number of photons in the subensemble characterized by the position x is proportional to $|\psi(x)|^2$. Therefore, the total interference pattern $\mathcal{F}(\xi)$ is just the sum of all the contributions from the various subensembles, weighted by $|\psi(x)|^2$:
$\mathcal{F}(\xi) \propto \int dx|\psi(x)|^2 I_x(\xi) = 1 + e^{-k_0^2 a^2} \cos 2k_0\xi$.

This is our smeared-out interference pattern. Now how much can we determine about the paths of the photons using the same experimental arrangement, if we choose to measure the momentum of screen 1 rather than its position? Clearly the only photons which concern us are those which succeed in arriving at the final screen. Therefore, we will record only the momenta imparted by these photons. From the geometry of the apparatus we see that for these photons there are only two possible values of the wave vector imparted to screen 1 , namely, $\pm\pi S/(L\lambda) = \pm k_0$.
(We have assumed here that $a \ll s \ll L$, and that all photons arrive at screen 1 with no initial momentum in the x direction.) The measured momentum of screen 1 , however, will not be confined to these two values, even if our measurements are exact. As before, the uncertainty comes from the fact that the initial momentum of the plate is not definite, but rather has a distribution given by $|\varphi(k)|^2$. If the plate has initial wave vector k, then its final wave vector κ (after the plate has collided with one of the photons under consideration) can have either of the two values $\kappa = k \pm k_0$. The total recorded distribution $\mathfrak{D}(\kappa)$ of wave numbers of the plate will be the sum of all the partial distributions $D_k(\kappa)$, weighted by $|\phi(k)|^2$:

$$\begin{aligned} D_k(\kappa) =& \frac{l}{2}\left[\delta\left(\kappa - k + k_0\right) + \delta\left(\kappa - k - k_0\right)\right] \\ \mathscr{D}(\kappa) =& \int dk|\phi(k)|^2 D_k(\kappa) \\ =& \left[a/\left(2\pi^{1/2}\right)\right]\left\{\exp\left[-a^2\left(\kappa + k_0\right)^2\right]\right. \\ &\left. + \exp\left[-a^2\left(\kappa - k_0\right)^2\right]\right\} \end{aligned} \tag{3}$$

It is convenient to define a dimensionless "smudging parameter" $u = ak_0$. From Eq. (2) it is clear that this is the parameter characterizing the suppression of the interference pattern. It is also a measure of the uncertainty of our determination of the path of each photon. To clarify these points, let us choose a particular value of u, namely, $u = 0.4769$. If we use this value of u to calculate the interference pattern according to Eq. (2), and the distribution of measured momenta according to Eq. (3), then the results are those shown in Fig. 2.

If the measured momentum is positive, then we will guess that the photon passed through slit A; if it is negative, then we will guess that the photon passed through slit B. Clearly some of our guesses will be wrong-there are photons that have positive values of measured momentum even though their actual momentum was negative and they went through slit B. The fraction of photons which misbehave in this way equals the fraction $F(u)$ of our guesses which are wrong. This fraction is just the ratio of the area under the "tails" of the Gaussians (that is, the parts lying on the wrong side of $k = 0$) to the total area under $\mathfrak{D}(\kappa)$:

$$
\begin{aligned}
F(u) &= \left(a/\pi^{1/2}\right) \int_{-\infty}^{0} \exp\left[-a^2\left(\kappa - k_0\right)^2\right] d\kappa \\
&= \left(1/\pi^{1/2}\right) \int_{u}^{\infty} e^{-\eta^2} d\eta \\
&= \frac{1}{2}[1 - \operatorname{erf}(u)]
\end{aligned}
$$

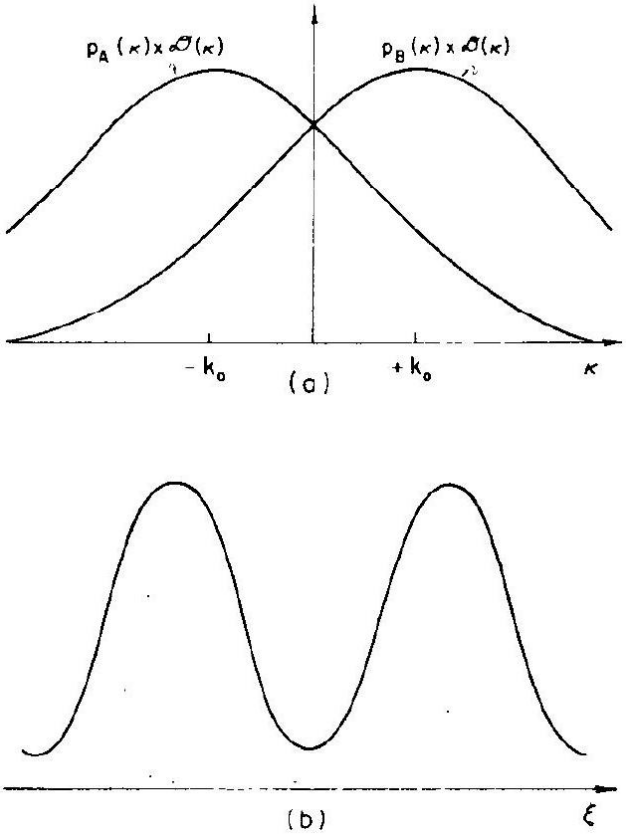


FIG. 2. Results of the approximate momentum measurement in the double-slit experiment, for the smudging parameter $u = 0.4796$. (a) Distributions of measured momenta. (b) The corresponding total interference patterns.

Our particular value of u was chosen so that $F(u) = 0.25$. That is, out of four guesses, one is usually wrong. Thus, we have done a fairly good (but not perfect) job of determining the path of each photon, and therefore we might expect an almost completely obliterated interference pattern. But in fact this is not true. Figure 2(b) shows that we still get an almost perfect interference pattern; the crest-to-valley ratio $R(u)$ of intensities is $R(u) = [1 + \exp(-u^2)] / [1 - \exp(-u^2)] = 8.8$ for our value of u. Have we not then succeeded in observing both particlelike and wavelike properties of the same photons?

One will no doubt object: The interference pattern $\mathcal{F}(\xi)$ was calculated for an experiment in which the position of screen 1 was measured. The path determination depended on the wave vector k of the photon inferred from the measured momentum of the screen 1. But these two measurements cannot both be performed for the same photons, and so Figs. 2(a) and 2(b) do not refer to the same experiment. Hence, in accord with the Copenhagen interpretation of quantum mechanics, there is no paradox. The complementarity principle does not prevent photons from behaving once as waves and once as particles. It only states that the same photon should not reveal this "split personality" in the same experiment.

The above objection is certainly valid. However, we shall see in the next section that even when we perform the momentum measurements on screen 1 , obtaining information about the slit each photon chooses, the same total interference pattern $\mathcal{F}(\xi)$ forms on the photosensitive screen 3. That is, Figs. 2(a) and 2(b) describe the outcome of the same hypothetical experiment.

26.12.3 III. Correlation between the Measured Momentum and the Corresponding Interference Pattern

In this section we will analyze the experiment in which the momentum of screen 1 is measured rather than the position. From each momentum measurement we will infer the relative probabilities of the photon's passing through one slit or the other. In practice, we cannot actually perform this momentum measurement with the necessary accuracy. However, as is shown in Appendix A, one can perform an experiment which will give the desired probabilities. The analysis in this section is sufficiently general to be applicable to the experiment considered in Appendix A.

In our experiment (Fig. 1), photons entering the apparatus change the momentum of screen 1. Then some of them pass through the slits in plate 2 , as announced by a flash of light emitted by a scintillator on plate 3. We wait for these scintillations, and immediately record the momentum of plate 1 and the position of the scintillation. That is, our record contains for each photon two numbers: the measured position on plate 3 and the measured momentum. Of course, we can obtain from this record both the interference pattern $\mathcal{F}(\xi)$ and the distribution $\mathfrak{D}(\kappa)$ of measured photon momenta. Indeed, these two distributions could have been obtained directly, without keeping a photon-by-photon record. The fact that each scintillation is actually associated with a definite kick to plate 1 can have no effect on the shapes of $\mathcal{F}(\xi)$ and $\mathfrak{D}(\xi)$. Given that we do have a photon-by-photon record, we find $\mathfrak{F}(\xi)$ simply by counting all the photons that landed in the interval $\xi - \xi + d\xi$. $\mathfrak{D}(\kappa)$ is clearly constructed in an analogous manner.

But a new question which we have not considered so far comes to our attention. We can look for the distribution of scintillations arising only from those photons which have been associated with a definite measured momentum κ of the plate 1. What kind of interference pattern will these photons produce? The first thing to notice is that these partial interference patterns $i_\kappa(\xi)$ cannot be independent of κ; that is, they cannot all have the shape of the total interference pattern. For
if we consider only the photons with a high-enough κ, we could improve indefinitely our chances of a correct determination of their paths; that is, by increasing κ we would be able to tell with as small a margin of error as we wish through which of the two slits the photon has passed. In this way we would be able to get around Bohr's resolution of the double-slit paradox.

Therefore, a correlation between κ-the measured value of the plate's momentum - and $i_\kappa(\xi)$-the partial interference pattern -seems inescapable. To find out the shape of $i_\kappa(\xi)$, let us consider the fraction of error $f(\kappa)$ defined as the ratio of the probability of the photon's passing through slit A to the probability of passing through slit B,

$$\begin{aligned} f(\kappa) &= p_A/p_B \\ &= \exp\left[-a^2\left(\kappa + k_0\right)^2\right] / \exp\left[-a^2\left(\kappa - k_0\right)^2\right]. \end{aligned} \tag{4}$$

Here p_A and p_B are defined by this formula together with the relation $p_A + p_B = 1$. This ratio $f(\kappa)$ clearly represents the uncertainty in our knowledge about the two possibilities from which the photon can choose.

The same situation and identical error ratio appear when we consider a double-slit experiment in which the two slits have different areas. The uncertainty ratio f will in this case

be expressed by the ratio of the two areas. In this situation the interference pattern can be immediately written:

$$i_f(\kappa) = 1 + 2p_A^{1/2} p_B^{1/2} \cos 2k_0\xi. \tag{5}$$

It is natural to expect that if our correlation measurement is characterized by the same value of f as this unequal-double-slit experiment, then it should yield the same interference pattern. Therefore,

$$i_\kappa(\xi) = 1 + 2p_A^{1/2}(\kappa) p_B^{1/2}(\kappa) \cos 2k_0\xi. \tag{6}$$

These formulas (5) and (6) are certainly compatible with quantum mechanics and with the uncertainty and complementarity principles. What do they predict for a definite value of f ? For instance, let us take $f = \frac{99}{1}$; that is, out of 100 photons we expect 99 of them to pass through the more likely slit. An accuracy of 99% is certainly high, and one would expect that such a measurement should destroy the interference pattern. But a straightforward calculation shows that the crest-to-valley ratio R given by $R = \left(1 + 2{p_A}^{1/2}{p_B}^{1/2}\right) / \left(1 - 2{p_A}^{1/2}{p_B}^{1/2}\right)$ equals approximately $\frac{3}{2}$. Despite the fact that we know with 99% certainty the paths of the photons, they still have strong wavelike properties. In a sense we have localized the cause of what appeared to be a violation of the

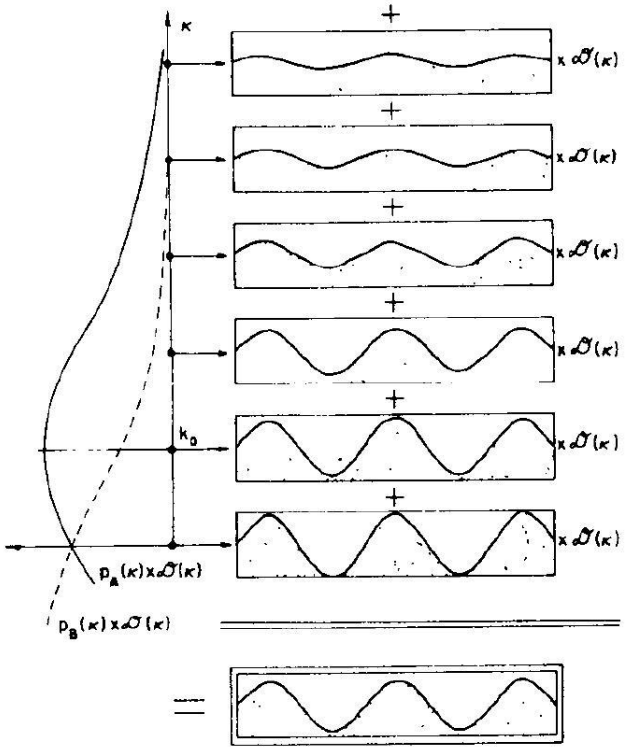


FIG. 3. Partial-interference patterns $i_{\kappa}(\xi)$ corresponding to the different measured momenta κ and the resulting total interference pattern $\mathfrak{F}(\xi)$, according to formula (7).}

complementarity principle.

To make sure that our present reasoning is consistent and that our apparent paradox survives the objection raised at the end of Sec. I, let us add up all the partial interference patterns, all the differently smudged-out contributions. According to Eqs. (3) and (5), each of them can be written as

$$i_\kappa(\xi) = 1 + \frac{2\exp\left[-a^2\left(\kappa^2+k_0^2\right)\right]}{\exp\left[-a^2\left(\kappa-k_0\right)^2\right]+\exp\left[-a^2\left(\kappa+k_0\right)^2\right]} \times \cos 2k_0\xi$$

Weighting them by $\mathscr{D}(\kappa)$ and adding them together, as represented in Fig. 3, we obtain

$$\begin{aligned}\mathcal{F}(\xi) &= \int D(\kappa) i_\kappa(\xi) d\kappa \\ &= 1 + e^{-a^2k_0^2}\cos 2k_0\xi \end{aligned} \tag{7}$$

This is exactly what we obtained previously [Eq. (1)] by adding perfect, but shifted, interference patterns. This way of obtaining the total interference pattern is illustrated symbolically in Fig. 3.

26.12.4 IV. Einstein-rosen-podolsky "paradox" in the Double-slit Experiment

Let us recall the two possible measurements one can perform using the experimental set-up of Fig. 1: (1) Measure the position of screen 1-
get perfect but shifted partial interference patterns. (2) Measure the momentum of screen 1get smeared out but centered partial interference patterns.

Notice that in both cases the measurement on screen 1 is performed after the photon has interacted with it. How does the photon know in which partial interference pattern to fall? How can it know what we decided to measure when it is already separated from the plate by a large distance?

There is no doubt that our choice affects the wave function of the photon: (1) If we measure plate 1 to have position x, the photon arrives at plate 3 in the state

$$\mu_x(\xi) \propto e^{ik_0(\xi+x)} + e^{-ik_0(\xi+x)} \tag{8a}$$

(2) If we measure plate 1 to have momentum κ, the photon arrives at plate 3 in the state

$$\nu_\kappa(\xi) \propto p_A^{1/2}(\kappa)e^{ik_0\xi} + p_B^{1/2}(\kappa)e^{-ik_0\xi} \tag{8b}$$

This effect of our measurement on the photon's wave function can be understood in the following way. After the photon has interacted with plate 1, it no longer has an individual wave function; there is only the state Ψ of the combined system (plate 1+ photon). This combined state can be expanded in terms of any complete set of orthogonal states of plate 1 . For example, if σ_x is the eigenstate of position of plate 1 corresponding to the eigenvalue x, we can always write the combined state as

$$\Psi = \int dx c_x \mu_x \otimes \sigma_x \tag{9a}$$

where the photon states μ_x are all normalized but not necessarily orthogonal, and $|c_x|^2$ is the probability distribution of the plate's position x. Alternatively, we can use the set of eigenstates of momentum of plate 1, $\{\tau_k\}$, as our basis, in which case Ψ is written as

$$\Psi = \int d\kappa d_\kappa \nu_\kappa \otimes \tau_\kappa \tag{9b}$$

Thus, each plate eigenstate (σ_x or τ_κ) has its corresponding photon state. When we measure the plate's position and obtain the value x, the photon is forced into the state μ_x, and similarly for momentum. In this way our choice affects the wave function of the photon.

Our object now is to identify the various quantities which appear in Eqs. (9), and thus to check that this idea of the combined state is consistent with the analys is of the previous sections. For definiteness we will write ψ as a function of the positions of plate 1 and the photon, to which we assign the symbols " z " and " ξ " respectively (" x "
is reserved as a lable for eigenfunctions; hence the necessity of introducing " z "). According to our previous analysis, μ_x and ν_κ should be given by Eqs. (8), and the other quantities in Eqs. (9) should be interpreted as follows:

$$c_x = \psi(x) = \frac{1}{\pi^{1/4}a^{1/2}} e^{-x^{2/2}a^2} \text{ [see Eq. (1)}\Big]$$
$$\sigma_x(z) = \delta(z-x)$$
$$d_\kappa = D^{1/2}(\kappa)\text{[see Eq. (3)]}$$
$$\tau_\kappa(z) = e^{i\kappa z}$$

Inserting these identifications into Eqs. (9), we obtain the following expressions for Ψ :
According to Eq. (9a),

$$\Psi = \frac{1}{2^{1/2}a^{1/2}\pi^{1/4}} \int dx e^{-x2/2a^2} \left[e^{ik_0(\xi+x)} + e^{-ik_0(\xi+x)}\right] \times\delta(z-x) \tag{10a}$$

according to Eq. (9b),

$$\Psi = \frac{a}{2\pi^{1/4}} \int d\kappa \mathfrak{D}^{1/2}(\kappa) \left[p_A^{1/2}(\kappa)e^{ik_0\xi} + p_B^{1/2}(\kappa)e^{-ik_0\xi}\right] \times e^{i\kappa z} \tag{10b}$$

where the constant factors have been chosen so that Ψ conforms to our normalization convention; i.e., $\int dz|\Psi|^2$ is a function of ξ whose average value is 1 . One can verify that these two expressions for the combined wave function are indeed equal. This is in fact the real justification for our identification of ν_κ [Eq. (8b)] as the wave function of photons corresponding to plate momentum κ, and hence also for our expression (6) for the partial interference pattern. In Secs. II and III we found that although our choice of what to measure (about plate 1) does affect the photon's wave function, it does not affect the total interference pattern. From the point of view of the present section, this result is seen quite easily. The total interference pattern is

$$f(\xi) = \int dz|\Psi(z,\xi)|^2$$

which is independent of any measurements made on plate 1.

The situation described here and the analysis outlined above are essentially the same as in the Einstein-Podolsky-Rosen "paradox."4,5,6 There too what we choose to measure on one system affects the wave-function of another system far away. But the final distribution of measured values of the far away system is again independent of our choice. Thus in discussing Einstein's
double-slit experiment we have encountered the classic nonseparability feature of quantum mechanics. [7]

To make sure that the analogy is complete, one may consider a situation where the photon is first localized on screen 3, and the position (or
momentum) of screen 1 is measured only afterwards. In that case the wave function of the photon is simply $\delta(\xi - \xi_0)$. It is readily seen that the total wave function $\Psi(z, \xi)$ can be decomposed into a wave function of a photon localized at ξ_0 and a wave function describing plate 1 :

$$\Psi(z,\xi) = \int d\xi_0 \left\{\delta(\xi - \xi_0)\right\} \otimes \left\{(2a)^{-1/2}\pi^{-1/4} \exp\left(-z^2/\left(2a^2\right)\right)\left[\exp\left(ik_0\left(\xi_0 + z\right)\right) + \exp\left(-ik_0\left(\xi_0 + z\right)\right)\right]\right\}$$

From this expression a wave function, and, consequently, a corresponding probability distribution correlated to an ensemble of photons landing at the given coordinate value ξ_0 can be obtained.

That is, the measurement can be first performed either on the plate 1 or on the photon, and the obtained information will allow us to determine what is the probability distribution of the other, yet unmeasured part of an unseparable system.

26.12.5 V. Information and the Complementarity Principle

In the preceding sections we have presented a a result which, although not paradoxical, was nevertheless surprising (that is, that one can make a fairly precise determination of the slit through which each photon comes with only a slight disturbance of the interference pattern). It is worthwhile to notice that the two limiting cases of Einstein's version of the double-slit experiment do not surprise us at all. These are the cases in which the smudging parameter u takes the values zero (no determination is made of the path of the photon) and infinity (each photon's path is determined completely). As we can see from Eq. (1), in the former case the interference pattern is perfect, while in the latter case it is completely washed out. This result has been known for so long that we have learned how to talk about it, and it is therefore no longer surprising.

The apparent paradox of our present example clearly arises from the fact that we are considering an intermediate situation in which one obtains some information about the photons' paths, and still retains an interference pattern having some degree of clarity. The problem is that we lack a good way of talking about such a situation, and we have no simple rule which tells us what to expect. The aim of this section is to fill this gap. We will find that information theory
provides a good language for dealing with an imprecise path determination, and this will lead us naturally to a rule which defines the extent to which the two complementary aspects of light (wave and particle) may be manifested simultaneously.

Intuitively, one expects that if the interference pattern has a certain sharpness of definition, then there must be some limit on the amount of information which could have been obtained regarding through which slit each photon passed. What we wish to do here is simply to make this statement more precise. For this we need a way to quantify "information." We will use the measure of information discovered by Shannon, [8] which has all the mathematical properties one usually requires of information, and which has been fruitfully applied to a wide variety of problems, [9] including quantum mechanics itself. [10] Its most general definition is the following: If a system can be in one of N possible states, but if we know only the probabilities p_i of its being in each state i, then the amount of information we lack about the system is the positive number

$$H = -\sum_{i=1}^{N} p_i \ln p_i$$

In our experiment we can consider each photon as a system with two possible states (in the above sense): passing through slit A and passing through slit B. If we determine the probabilities of these two paths to be p_A and p_B (where $p_A + p_B = 1$), then the information we lack about the path of that photon is

$$H = -\left(p_A \ln p_A + p_B \ln p_B\right). \tag{11}$$

As an example, we note that if we know nothing about the path of a photon, that is, if each slit is equally likely, then the amount of information we lack is

$$H_0 = -\left(\frac{1}{2}\ln\frac{1}{2} + \frac{1}{2}\ln\frac{1}{2}\right) = \ln 2.$$

Now we are ready to formulate the problem.

Suppose we are interested in obtaining an interference pattern with a certain crest-to-valley ratio of intensities, say, 8.8 as in the above example. Notice that there are many ways to make such a pattern. We list a few of them here:

(1) Perform the experiment described in Sec. II, in which the measured momentum of plate 1 is used to judge the path of each photon. In this case we have seen that the paths of some photons will be better determined than the paths of others, depending on the value κ of the measured momentum.

(2) Keep all the plates fixed, but let one of the slits be bigger than the other. We have seen in Sec. III that the resulting pattern will again be partially smeared out, and that the same pattern arises from a subensemble of photons all having the same value of κ. The crucial thing about these experiments is that we cannot differentiate further among the photons. There is only one subensemble (the whole ensemble); each photon gives us the same amount of information; the photons are in a pure state.

(3) Allow some of the photons to pass through one slit only (the other being blocked), making a completely smeared out pattern; then open the other slit, allowing the rest of the photons to interfere perfectly. The sum of the two patterns can be arranged to have the desired crest-tovalley ratio.

(4) Make no measurement of the photons' paths, but let the slit in plate 1 be of a size comparable to the spacing between fringes, so that the resulting pattern is smudged.

The point is that the amount of information one obtains about the photons' paths varies from one case to another, even though the "summed-up interference pattern" is the same in each case. For example, in case 4 one loses some of the sharpness of the pattern without gaining any information at all.

The question naturally arises: Of all possible methods of generating this particular interference pattern, which one gives us the most information regarding the photons' paths? If we can find this method, then we will have found the limit on the amount of information which can be obtained, given that we insist on a certain sharpness of definition of the pattern. We will then have to admit that no amount of cleverness can produce an experiment in which the information gained exceeds this limit.

We will find that this question is indeed answerable, and that the best method turns out to be experiment (2) above, in which the photons are in a pure state. To see this, we first need to write down a general expression for information which

applies to all the experiments we are considering. A typical experiment can be described as follows. As in Sec. III, all the photons can be divided into different subensembles, such that the photons of a given subensemble all have the same probability of passing through slit A. In Sec. III we labeled the subensembles by the measured quantity κ, and we called the probabilities of the two paths $p_A(\kappa)$ and $p_B(\kappa)$. In the general case which we are considering now, it will be more convenient simply to label each subensemble by its values of p_A and p_B. To simplify

the notation let us define $\gamma = p_A$, from which it follows that $p_B = 1 - \gamma$. For our purpose, each experiment is completely characterized once we specify the fraction of the photons in each subensemble. Therefore, let $\rho(\gamma)d\gamma$ be the fraction of the photons whose probabilities of going through slit A are between γ and $\gamma + d\gamma$.

According to Eq. (7) the information we lack about the path of each photon of the subensemble γ is

$$H(\gamma) = -[\gamma \ln \gamma + (1-\gamma)\ln(1-\gamma)].$$

The total information we lack is the sum of $H(\gamma)$ over all photons. To obtain the average information H we lack per photon, we divide this sum by the total number of photons, arriving at the formula

$$\begin{aligned} H &= \int_0^1 d\gamma \rho(\gamma) H(\gamma) \\ &= -\int_0^1 d\gamma \rho(\gamma)[\gamma \ln \gamma + (1-\gamma)\ln(1-\gamma)] \end{aligned} \tag{12}$$

Now we would also like to write an expression for the interference pattern $\mathcal{F}(\xi)$ in terms of the function $\rho(\gamma)$. As in Sec. III [Eq. (6)], we again associate with each subensemble γ a partial interference pattern $i_\gamma(\xi)$, given by

$$i_\gamma(\xi) \propto 1 + 2\gamma^{1/2}(1-\gamma)^{1/2}\cos 2k_0\xi$$

Notice that we have assumed the best possible $i_\gamma(\xi)$. One could always be sloppy (as in experiment 4) and obtain a more smudged pattern. Furthermore, we have assumed that all of the contributions i_γ from the various subensembles are not shifted relative to each other; that is, they all have their maxima at the same places. For our purpose here, these assumptions entail no loss of generality; we are trying to get as good a pattern as we can in order to investigate the theoretical limit on the amount of information which can be obtained. We now generalize Eq. (7), and find that the total interference pattern is

$$\mathcal{F}(\xi) = \int_0^1 d\gamma \rho(\alpha) i_r(\xi) = 1 + S\cos 2k_0\xi \tag{13}$$

where

$$S \equiv 2\int_0^1 d\gamma \rho(\gamma)\gamma^{1/2}(1-\gamma)^{1/2} \tag{14}$$

From Eq. (13) it is clear that the quantity S is a measure of the sharpness of definition of the interference pattern. In terms of S, the main problem of this section can now be stated very simply: For a given value of S, what distribution ρ minimizes H, and what is this minimum value of II ?

Our answer, whose proof is outlined in Appendix B, is that the best ρ is

$$\rho_0(\gamma) = \delta(\gamma - \gamma_0) \tag{15}$$

where γ_0 is determined by the chosen sharpness of the interference pattern. In fact, according to Eqs. (13)-(15),

$$S = 2\gamma_0^{1/2}(1-\gamma_0)^{1/2}$$

or, if we solve this for γ_o,

$$\gamma_0 = \frac{1}{2}\left[1 \pm \left(1 - S^2\right)^{1/2}\right]. \tag{16}$$

What F.q. (15) says is that if we wish to get as much information as we can about the photons' paths, the best experiment we can do is of the kind exemplified by experiment 2 , where all photons have the same probability γ_0 of passing through slit A, and are thus in a pure state. (Actually, as is shown in Appendix B, there is a one-parameter family of distributions which are as good as ρ_0; they differ from ρ_0 only in that some of the photons have their probabilities p_A and p_B reversed.) We have thus answered the first part of our question.

For an interference pattern of given sharpness S, the amount of information $H(S)$ one gives up when he uses this "best" method can be found from Eqs. (12) and (15) (and this answers the second part of our question):

$$H(S) = -\left[\gamma_0 \ln \gamma_0 + (1-\gamma_0)\ln(1-\gamma_0)\right], \tag{17}$$

where γ_0 is given by Eq. (16). The main result of this section is that one must forfeit at least this much information about the photons' paths in order to obtain an interference pattern of sharpness S. That is,

$$H \geqslant II(S). \tag{18}$$

Let us now apply this result to our original experiment (experiment 1), with the smudging parameter u having the same value as before. The interference pattern is [Eq. (2)]

$$\begin{aligned}\mathcal{F}(\xi) &= 1 + e^{-u^2}\cos 2k_0\xi \\ &= 1 + (0.796)\cos 2k_0\xi.\end{aligned} \tag{19}$$

That is, $S = 0.796$. The value of $H(S)$, given by

Eqs. (17) and (16), is then $H(S) = 0.497$. This number becomes more meaningful if we compare it to the total amount of information $H_0 = \ln 2$ available about each photon:

$$H(S)/H_0 = 0.717.$$

Thus, according to our result, in order to obtain the interference paltern (19), we must sacrifice at least 71.7% of the available information regarding the photons' paths.

This is the minimum amount of information we must sacrifice. How much information do we in fact give up when we perform Einstein's experiment? The easiest way to answer this is to return to the κ notation. According to Eq. (4), the probability $p_A(\kappa)$ that a photon in the subensemble κ will pass through slit A is

$$p_A(\kappa) = \frac{\exp\left[-a^2(\kappa + k_0)^2\right]}{\exp\left[-a^2(\kappa + k_0)^2\right] + \exp\left[-a^2(\kappa - k_0)^2\right]},$$

and $p_B(\kappa) = 1 - p_A(\kappa)$. The average information we lack per photon is

$$H = \int_{-\infty}^{\infty} d\kappa \mathfrak{D}(\kappa)\left[p_A(\kappa)\ln p_A(\kappa) + p_B(\kappa)\ln p_B(\kappa)\right]$$

where the distribution $\mathfrak{D}$ of measured momentum κ is given by Eq. (3). Upon evaluating this integral numerically, we find that

$$H/H_0 = 0.728.$$

This is only slightly greater than the minimum value $H(S)'H_0 = 0.717$, associated with this interference pattern. Thus, Einstein's experiment gives almost as much information as one could possibly get [which, by the way, is not very much in this case-only 28.3% (i.e., $1 - 71.7\%$) of the available information; this is perhaps in better agreement with what we might expect for this interference pattern, as compared to the expression "75% accuracy" which we used earlier]. But the point is that the amount of information one can get is limited by $H(S)$.

Let us conclude this section with a clear statement of the complementarity principle in the language of information theory, as it applies to the double-slit experiment. The sharpness of the interference pattern can be regarded as a measure of how wavelike the light is, and the amount of information we have obtained about the photons' trajectories can be regarded as a measure of how particlelike it is. Equation (14) can be expressed in words as follows: (Information lost about the photons' paths) $\geqslant$ (information $H(S)$ lost in pure-state experiment giving the same interference pattern). $H(S)$ [given by Eqs. (17) and (16)] increases monotonically as the sharpness increases. The above inequality is thus a pre-
cise statement of the following fact: The more clearly we wish to observe the wave nature of light, the more information we must give up about its particle properties.

26.12.6 Acknowledgments

We would like to thank Professor John Archibald Wheeler, who encouraged us to pursuc this project, for many stimulating discussions and for reading the manuscript. We would also like to thank Dilip K. Kondepudi for sharing with us some of his ideas on the double-slit experiment.

26.12.7 Appendix A: Multiplate Double-slit Experiment

As we have discussed in the introduction, Einstein proposed to modify the double-slit experiment in such a way that in principle one should be able to determine through which slit the photon passed. In this appendix we shall propose an arrangement where one would be able to carry out an equivalent experiment in practice

The major difficulty encountered in an attempt to realize Einstein's proposal is the error in the determination of the lateral kick. This measurement may be performed by releasing any of the three screens involved (we do not consider any causality effects in this appendix), and measuring the momentum of the screen after its interaction with the photon. But regardless of the particular screen, the square average momentum of the random, noiselike Brownian motion is larger than the value of the kick we want to determine. For the case where the photographic plate is released Wheeler [13] recently calculated that the resulting fluctuations in the value of the momentum are 12 orders of magnitude larger than the signal itself. We are consequently forced to look for some alternative indicator of the particle path that would replace the momentum kick.

The direction was all that the kick could have told us. Can we determine the direction of the photon in a straightforward manner? To do it we propose the experimental arrangement envisaged in Fig. 4. There, the usual photographic plate is replaced by the set of nontransparent, thin "photoplates" covered with the photographic emulsion on both sides. In such a "multiplate double-slit" experiment, when the photon blackens a grain of sliver bromide on the top (bottom) of one of the photoplates, we expect that it came from the top (bottom) slit. The analysis of the experiment is simplest when the photoplates are occupying the region $\Delta\xi \ll s$, that is, when they lie close to the optical axis of the double-slit apparatus. We shall assume that this is true in the

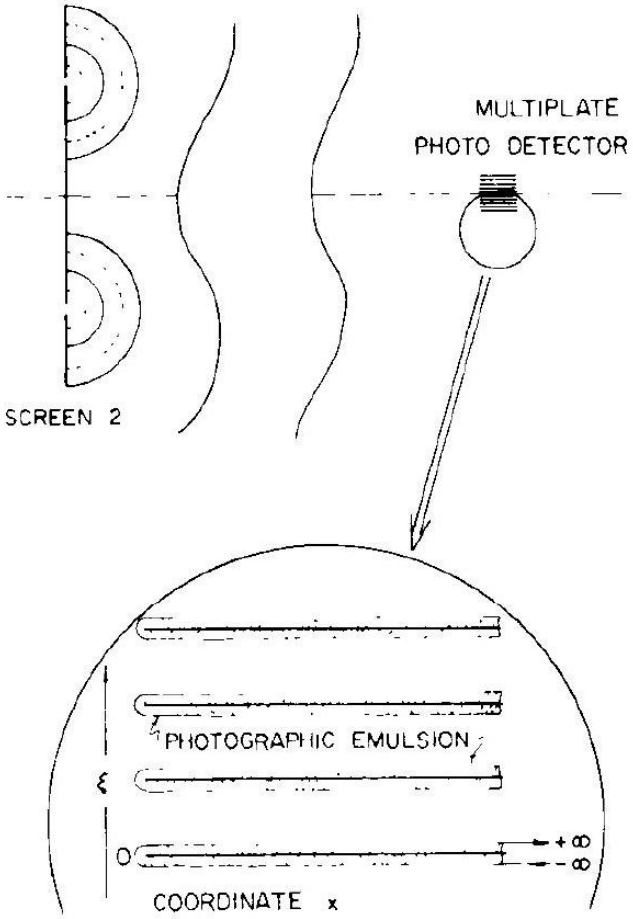


FIG. 4. Multiplate double-slit experiment.

rest of this section unless otherwise stated.

Let us now consider only those plates in the positions where previously, with the help of the normal photographic plate, maxima and minima of the perfect interference pattern

$$\mathfrak{F}(\xi) \propto 1 + \cos 2k_0\xi$$

were observed. Will the plates placed at $\xi = 2n\pi/2k_0$ become dark while the ones at $\xi = [(2n+1)\pi]/2k_0$ remain untouched by the radiation? Shall we recover the perfect interference pattern? If so, quantum mechanics would prove inconsistent: The same photon goes through two slits producing an interference pattern and yet it comes from the top (bottom) slit.

What other outcomes of the experiment are conceivable? Let us examine more carefully the possible fate of photons landing on the photoplates to establish if: (1) The interference pattern may disappear -and all the plates will be "grey." (2) The fact that the photon lands on the top (bottom) of the photoplate does not yet allow us to be sure from which slit it came.

While the experiment remains to be done, one really expects (1) to occur. The reason for it in a carefully performed multiplate double-slit experiment is clear enough: The photons coming from two different slits never meet on the same side of the photoplate-they can never interfere. We can conclude this already from the wave optics interpretation, unless the wave representing the

electrical field of the photon can get in some fashion from the bottom slit to the top side of the photoplate.

If this "landing on the wrong side" does occur, then we have the situation described by (2). Physical reasons for that effect can be found in the reflections that direct the ray coming from

the top slit to the bottom side of the photoplate [see Fig. 5(a)]. Consequently, the probability of detecting a photon from a certain slit changes accordingly. We can use $p_A(x)$ as in Sec. III, to denote the probability that a photon from the top slit will arrive at the position x, where x is defined in Fig. 5(a). As before, we assume $p_A(x) + p_B(x) = 1$. We can also assume that the phases of the photons arriving at the given x are not randomized through the undergone reflection processes.

With this in mind one does not encounter any difficulties in carrying out an analysis similar to the one performed in Sec. III. The only important change is the different shape of $p_A(x)$ and $\rho_B(x)$, which is qualitatively shown in Fig. 5(b). What we shall measure here can be described in terms of the partial interference pattern and total interference pattern. For when we record the intensity at a certain position x on each plate, we sample at a set of discrete points $\{\xi_i\}$ (which are the positions of the photoplates) the partial interference pattern $i_x(\xi)$. As in Sec. III, from the knowledge of $p_A(x)$ and $p_B(x)$, we have

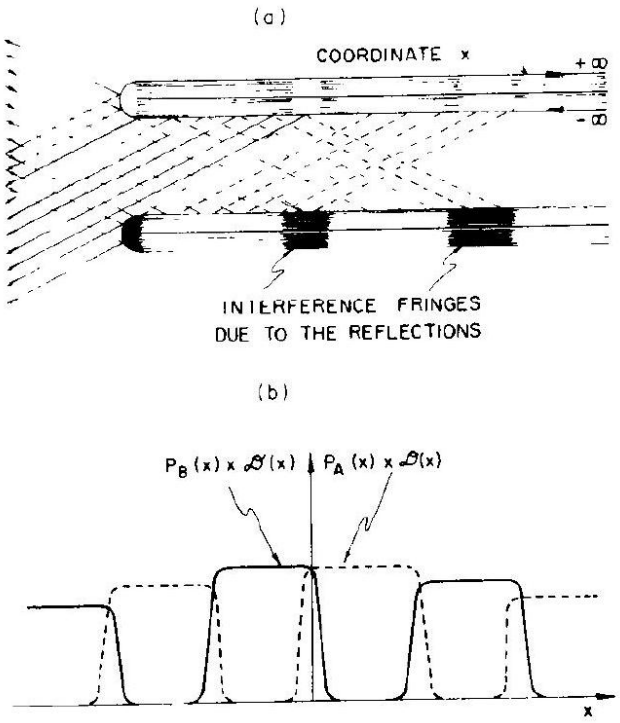


FIG. 5. Origin of the residual interference pattern in the multiplate double-slit experiment. (a) The paths of the photons and the resulting interference pattern. (b) Probabilities of arrival from one of the slits as a function of x.

$$i_x(\xi) = 1 + p_A^{1/2}(x)p_B^{1/2}(x)\cos 2k_0\xi$$

This formula is true since all the photons landing at a certain x have the identical probabilities $p_A(x)$ and $p_B(x)$, and for that reason constitute one "subensemble" in the sense of Sec. III. Thus, we have succeeded in designing a measurement that gives directly the partial-interference pattern.

To obtain the total interference pattern, $\mathcal{F}(\xi)$, we use formula (6):

$$\mathcal{F}(\xi) = \int_{-\infty}^{\infty} dx\rho(x)i_x(\xi) \tag{A1}$$

That is, the total number of grains blackened on the photoplate at a position ξ gives the value of the total interference pattern $\mathcal{F}(\xi)$. The $\rho(x)$ used in Eq. (A1) is the weight function

proportional to the total number of photons that land at a certain x and plays the same role as $D(K)$ in formula (6).

To show that the discussed proposal is practical and realizable, let us go through the calculations in an example. The separation of photoplates δ should not be larger than the distance between the maximum and minimum expected in the interference pattern-in fact it is advantageous to sample the pattern only at these points: This yields for δ :

$$\delta - \pi/k_0.$$

We have assumed previously that $\delta/\mathrm{s} \ll 1$. This assumption is not crucial. We have used it solely to ascertain that in the set of photoplates one side of the photoplate can see only one slit. However, even if $\delta \sim s$, we can still make sure that this last statement is true by orienting the photoplates sc that the plane in which each one of them lies always intercepts the double-slit screen half-way between the two slits. Still, it is easier to do with s bigger than δ.

Taking $\lambda = 10\mu$ m (there are lasers which have wavelength of this order), we get for $L =$ 100 cm and $s = 5$ mm the photoplate separation $\delta = 0.85$ mm. This is well within reach of experimental possibilities.

We have seen here an experiment that attempts to determine the slit through which each photon passed while trying to retain the interference pattern - the same purpose for which the experiment described in the introduction was designed. However, no data clarifying the Einstein-Podolsky-Rosen paradox as discussed in Sec. IV can be obtained here, since both the path determination and contribution to the interference pattern follow from a single event-photoinduced transition in a silver-bromide grain. Still, our proposal is the only practical version of Einstein's double-slit experiment we are aware of.

26.12.8 Appendix B: Outline of a Proof That the Pure State Minimizes the Loss of Information

For a given value of S, what distribution ρ minimizes H ? This question can be simplified by the following definitions:

$$\begin{aligned} s(\gamma) &= \gamma^{1/2}(1-\gamma)^{1/2}, \\ h(\gamma) &= -[\gamma \ln \gamma + (1-\gamma)\ln(1-\gamma)], \\ \hat{\rho}(\gamma) &= \rho(\gamma) + \rho(1-\gamma), \end{aligned}$$

restricted to the interval $0 \leqslant \gamma \leqslant \frac{1}{2}$. Then

$$S = \int_0^{1/2} d\gamma \hat{\rho}(\gamma) s(\gamma) \tag{B1}$$

$$H = \int_0^{-1/2} d\gamma \hat{\rho}(\gamma) \tag{B2}$$

What we wish to show is that the distribution $\hat{\rho}_0(\gamma) = \delta(\gamma - \gamma_0)$ minimizes H for a given value of S. This will imply in particular that the pure state $\rho_0 = \delta(\gamma - \gamma_0)$ minimizes H. [So does any other ρ which gives the same $\hat{\rho}$. These other ρ 's are all of the form

$$\begin{aligned} &\rho(\gamma) = \alpha\delta(\gamma - \gamma_0) + (1-\alpha)\delta(\gamma - (1-\gamma_0)), \\ &0 \leqslant \alpha \leqslant 1.] \end{aligned}$$

Step 1. One can prove that s and h are monotonically increasing in the interval $0 \leqslant \gamma \leqslant \frac{1}{2}$, and that $s''/s' \leqslant h''/h'$ in this interval. (A prime denotes differentiation with respect to γ.)

Step 2. Let us compare the distribution $\hat{\rho}_0(\gamma) = \delta(\gamma - \gamma_0)$ with the trial distribution $\hat{\rho}_1(\gamma) = \eta_1 \delta(\gamma - \gamma_1) + \eta_2 \delta(\gamma - \gamma_2)$, in which $\eta_1 + \eta_2 = 1$, and the parameters are assumed to be adjusted so that both distributions give the same value of S;
that is [Eq. (B1)],

$$s(\gamma_0) = \eta_1 s(\gamma_1) + \eta_2 s(\gamma_2) \tag{B3}$$

We will show that $\hat{\rho}_0$ gives a smaller value of H than $\hat{\rho}_1$ does; that is [Eq. (B2)],

$$h(\gamma_0) \leqslant \eta_1 h(\gamma_1) + \eta_2 h(\gamma_2). \tag{B4}$$

To prove this, it is helpful to define $\bar{h}(\gamma)$ by
$\bar{h}(\gamma) = \frac{[s(\gamma_2)-s(\gamma_1)]h(\gamma)+s(\gamma_1)h(\gamma_2)-s(\gamma_2)h(\gamma_1)}{h(\gamma_2)-h(\gamma_1)}$.
The following things are true about $\bar{h}$:
(i) $\bar{h}(\gamma_1) = s(\gamma_1)$ and $\bar{h}(\gamma_2) = s(\gamma_2)$.
(ii) $\frac{\bar{h}''}{\bar{h}'} = \frac{h''}{h'} \geqslant \frac{s''}{s'}$ for $0 \leqslant \gamma \leqslant \frac{1}{2}$.
(iii) By (i) and Eq. (B3), $s(\gamma_0) = \eta_1 \hbar(\gamma_1) + \eta_2 \hbar(\gamma_2)$.
(iv) To prove Eq. (B4), it is sufficient to prove that

$$\bar{h}(\gamma_0) \leqslant \eta_1 \bar{h}(\gamma_1) + \eta_2 \bar{h}(\gamma_2).$$

From (iii) and (iv) it is clear that what we have to prove is that $\bar{h}(\gamma_0) \leqslant s(\gamma_0)$. In fact it is not hard to show from properties (i) and (ii) that $\bar{h}(\gamma) \leqslant s(\gamma)$ for all γ between γ_1 and γ_2, and thus for γ_0 in particular.

Step 3. We have seen in Step 2 that the distribution $\hat{\rho}_0 = \delta(\gamma - \gamma_0)$ is better at minimizing H than any sum of two δ functions. This result can be extended by induction to any sum of $n\delta$ functions.

Step 4. For the purpose of calculating S and H, any distribution can be approximated arbitrarily closely by a sum of $n\delta$ functions. Therefore, the distribution $\hat{\rho}_0 = \delta(\gamma - \gamma_0)$ minimizes H with respect to all possible distributions.

[1] M. Jammer, The Philosophy of Quantum Mechanics (Wiley, New York, 1974), pp. 121-132.
[2] F. J. Belinfante, Measurement and Time Reversal in Objective Quantum Theory (Pergamon, New York, 1975), p. 32.
[3] R. P. Feynman, R. B. Leighton, and M. Sands, The Feynman Lectures on Physics (Wesley, Reading, Mass., 1965), Vol. 3, p. 1-1.
[4] M. Jammer, Ref. 1, pp. 160-247.
[5] F. J. Belinfante, Ref. 2, p. ix.
[6] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. 47, 777 (1935).
7B. D'Espagnat, Conceptual Foundations of Quantum Mechanics (Benjamin, Reading, Mass., 1976), 2nd edition.
[8] C. E. Shannon, Bell Syst. Techn. J. 27, 379 (1948).
[9] J. R. Pierce, Symbols, Signals and Noise (Harper, New York, 1961).
[10]H. Everett III, in The Many-Worlds Interpretation of Quantum Mechanics, edited by B. DeWitt and N. Graham (Princeton Univ. Press, Princeton, New Jersey, 1973).
[11]H. Weyl, The Theory of Groups and Quantum Mechanics (Methuen, London, 1931).
[12] P. Jacquinot and B. Roizen-Dossier, in Progress in Optics, edited by E. Wolf (North-Holland, Amsterdam, 1964), Vol. 3.
[13] J. A. Wheeler, in Mathematical Foundations of QuantumTheory: Proceedings of the New Orleans Conference on the Mathematical Foundations of Quantum Theory, edited by A. R. Marlow (Academic, New York, 1978).

26.13 III.12 Complementarity in the Double-slit Experiment: on Simple Realizable Systems for Observing Intermediate Particle-wave Behavior

Abstract

In the course of a detailed analysis of observable intermediate particle-wave aspects of light, Wootters and Zurek invented an ingenious but technically difficult practical apparatus for performing Einstein's version of the double-slit experiment. The present note discusses two very simple alternative systems for displaying the Bohr-Einstein particle-wave extremes or, if desired, any intermediate trajectory-interference manifestation associated with the double-slit experiment.

In a recent analysis of Einstein's version of the double-slit experiment, Wootters and Zurek [1] presented a detailed treatment of the potentially observable manifestations of particle and wave characteristics of light. This approach led them to a quantitative expression of Bohr's complementarity principle appropriate for such experiments. Einstein had originally proposed that the lateral kick imparted by a photon to an interference screen could be used to identify which slit the photon traveled through on its way to the screen. Pointing out that thermal noise in practical experiments would utterly obscure such photon-induced recoils, Wheeler [2] recently reformulated the Einstein experiment in such a way that simple optical discriminat ion replaced measurements of photon kicks. In Wheeler's revised experiment, the operator is free to choose (after the photon has passed the slits, if he wishes) either to observe which slit has been traversed or to accumulate interference fringes. Wootters and Zurek showed how to modify the double-slit experiment to permit intermediate choices. In their thought experiment strongly visible interference fringes are displayed under conditions allowing "trajectories of the photons" to be "determined with fairly high accuracy." Although their theoretical analysis was developed in terms of measurements of Einstein photon kicks, Wootters and Zurek also proposed an ingenious practical version of the experiment not requiring measurements of recoil. Instead of adapting the Wheeler version, however, they introduced a new type of multiplate detector.

It seems worthwhile to point out that a small modification of Wheeler's apparatus leads to an even simpler demonstration of intermediate "par-ticle-wave" behavior. This modification is illustrated in Fig. 1. In Wheeler's design the interference screen is placed at the focal plane of the lens at a distance L from the slits, where the Fraunhofer pattern can be observed. If, instead, it is desired to observe the trajectory of a particular
photon, the screen is turned aside and the photon activates one or the other counter. [3] All that is needed to observe intermediate behavior is to move the interference screen to a new distance $l = L + z$, on either side of the focus, where the Fresnel pattern can be viewed. It is convenient to analyze a system with equivalent slits incorporating Wheeler's Gaussian transmission filters. Such filters circumvent the subsidiary diffraction spots characteristic of slits with abrupt edges. Elementary diffraction theory for a case $l \gg d \gg \lambda$ yields the intensity

$$I(y) = K[F(y)]^2 \cosh(ay)[1 + V(y) \cos by] \tag{1}$$

where $F(y)$ is the slit form factor $\exp(-y^2/2\sigma^2)$, $V(y)$ is the Michelson "fringe visibility" (parameter S of Wootters and Zurek) given by sech(ay), and K, a, b, and σ are identified in Ref. 4.

Although the fringe visibility damps as y increases, it is easy to choose conditions making the variation of $V(y)$ small across a span of many fringes. As is true also for the Wootters and Zurek system, fringe visibility is related to the slit transmission probabilities $P_A(y)$ and $P_B(y)$ for radiation reaching coordinate y via

$$V(y) = 2\,[P_A(y)P_B(y)]^{1/2}\,. \tag{2}$$

Therefore, if the slit discrimination ratio $P_A : P_B$ is selected to be 4 : 1, for example, the resultant

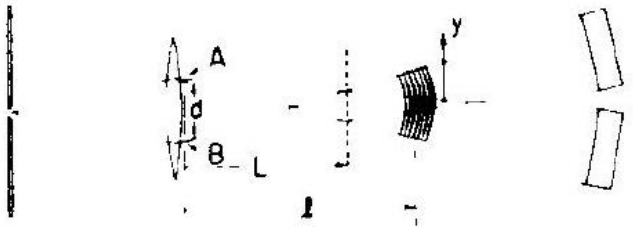


FIG. 1. Modification of Wheeler's version of Einstein's double-slit experiment. Fraunhofer fringes can be accumulated on a screen at L, or counters at right can detect which slit a photon came through. Alternatively, an observation region y at $l \neq L$ can be selected to yield any desired slit transmission probability ratio, $P_{A : P_{B}}$, and fringe visibility. See text.}

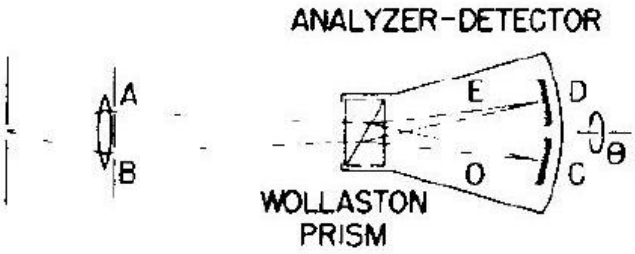


FIG. 2. Double-slit apparatus with controllable trajectory/interference characteristics. Slits A and B transmit light polarized at $+45^{\circ}$ and -45°, respectively. Any desired slit transmission ratio $P_A : P_B$ and corresponding fringe visibility received at the detectors can be chosen by adjusting the analyzer-detector orientation. O and E represent ordinary and extraordinary rays.}

fringe visibility is only 20% lower than that of an ideal two-slit pattern. Although such a ratio suggests a fairly high probability of a trajectory through slit A, it cannot, of course, be rigidly interpreted in terms of individual photons going through slit A four times out of five. Equation (2) obviously reduces to the Bohr-Einstein extremes as V, P_A, or P_B approach unity. At intermediate values of these variables, Eq. (2) offers a quantitative expression of complementarity for intermediate cases. Expectation values of V (wave) and P_A (particle) cannot both be unity simultaneously; the sacrifice of knowledge of one for the other is plain.

The extreme simplicity of the foregoing experiment may not be an adequate compensation for its unattractive but characteristic variation of $P_A : P_B$ across the diffraction pattern. Therefore, an alternate apparatus designed to produce patterns with uniform, controllable $P_A : P_B$ ratios is sketched in Fig. 2. In this apparatus, slits A and B transmit light polarized at $+45^{\circ}$ and -45°, respectively. When the analyzer-recorder is oriented as illustrated, two-slit patterns of unit visibility arrive at C and D (one pattern with a light fringe and one with a dark fringe at the center). rotation of the analyzer system by 45° about the optic axis produces a single-slit pattern from A at C and a corresponding pattern from B at D. Intermediate rotations θ generate intermediate

fringe visibilities ($V = \cos 2\theta$) and intermediate transmission probabilities P_A and P_B. Again, the visibility is related to transmission probabilities by Eq. (2) but the ratio $P_A : P_B$ now depends only on the orientation θ. In principle, by adjusting θ, a choice can be made (after the photon has passed the slits, if desired) of what fraction of it (89%, say) shall have passed through one slit and what fraction through the other. The experimenter cannot, of course, choose which slit shall have transmitted 89%-that is left to chance-but only that one of the slits shall have transmitted 89%. and one, 11%. The 11%, although small, is quite crucial to the 63% fringe visibility.

In each of the two experiments sketched above, the Fresnel and the polarization, Wootters and Zurek reflectionless multiplate detectors could be introduced to determine directly the $P_A : P_B$ ratio inferred only indirectly in the foregoing. Naturally, such direct observations would render the interference fringes unobservable. Each of the experiments can be adjusted to manifest a variable degree of wave-particle behavior analogous to that discussed at length by Wootters and Zurek. As thought experiments the present designs offer no new lessons. As realizable experiments, however, they offer quite the simplest arrangements possible.

This research was supported by a grant from the National Science Foundation.

26.14 III.13 A "delayed-choice" Quantum Mechanics Experiment by Wickes, Alley, Jakubowicz

We describe an experiment currently being assembled to test the quantum-mechanical assertion that the results of a split-beam interference measurement are unchanged even if the decision to recombine the two light beams is delayed until after each photon interacts with the beam splitter and enters a superposition state.

In a traditional optical double-slit interference experiment (Fig. 1), photons from a distant point-source are incident upon a screen containing two small apertures. With a lens behind the screen, an image of the source is formed on, for example, a photographic plate situated in the focal plane of the lens. The size and shape of the image depend upon the apertures, but the image will be crossed by interference fringes of angular frequency λ/D, where D is the separation of the apertures and λ is the wavelength of the light. Such an experiment isolates the wave character of the incident radiation: the interference fringes can be best understood by describing the energy contained in the radiation as passing through both apertures, even if the intensity is reduced so that usually only one photon at a time enters the system.

[81] W. K. Wootters and W. H. Zurek, Phys. Rev. D19, 473 (1979).

[2] J. A. Wheeler, in Mathematical Foundations of Quantum Theory: Proceedings of the New Orleans Conference on the Mathematical Foundations of Quantum Theory, edited by A. R. Marlow (Academic, New York, 1978).

[3] A greater discrimination can be secured by placing a

[8]lens at or beyond the interference screen to project images of the slits upon the counters.

[4] Let the slit amplitude transmission function be $\exp\left(-x^2/\ 2{x_0}^2\ \right)$, where x is the vertical distance from the slit center. Then $\sigma^2 = l^2{x_0}^2\left[k^{-2}{x_0}^{-4} + \left(l^{-1} - L^{-1}\right)^2\right]$, $a = ld\left(l^{-1}\ -L^{-1}\right)/\sigma^2$, and $b = ld/k{x_0}^2\sigma^2$. The symbol K represents a collection of constants of no concern here.

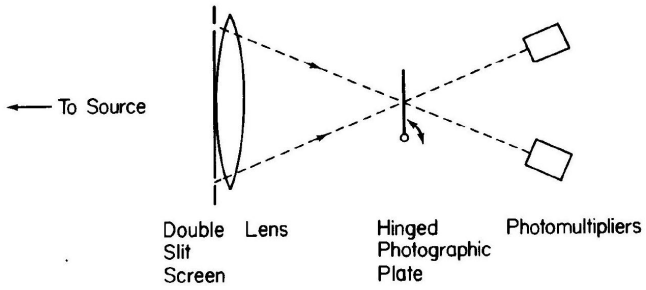


figure 1. Ideal Double-Slit Experiment

If the photographic plate is replaced by a pair of photomultipliers situated so that each one receives light from only one of the apertures, then the experiment emphasizes the particle nature of the light. If, for example, one of the apertures is covered, there is no effect on the count rate observed with the photomultiplier associated with the other aperture. This effect implies that each photon passes through one aperture or the other, never both.

This reasoning suggests that the configuration of the apparatus, and hence, the choice of an experimenter, determines whether the photons exhibit particle-like or wave-like behavior. Acceptance of this apparent paradox is central to the Copenhagen interpretation of quantum mechanics. Bohr (1949) moreover asserts that the outcome of a double-slit experiment will not change even if the apparatus is changed after the photon is already in flight. The experiment we propose will test this prediction.

In an idealized "delayed choice" double-slit experiment (Wheeler, 1978, 1979), the choice of whether the experiment is to demonstrate the wave properties (interference fringes on a photographic plate) or the particle properties (individual events in photomultipliers) is delayed until after a particular photon has passed the planc of the double slit. The light intensity is adjusted so that there is a low probability of more than one quantum being in the apparatus at any time. We might imagine that the photographic plate is hinged to swing rapidly into or out of the photon paths: if the plate intercepts the beams, an interference pattern is recorded, one grain at a time; if the plate is swung out of the way, photons passing through individual apertures are detected. If the interference pattern obtained is the same as obtained with a static plate, the quantum-mechanical prediction is confirmed. In what Wheeler (1979) calls a bad set of words, the behavior of the photons at the time of their interaction with the double slit, i.e., whether they pass through one aperture or both, is determined by our choice of photographic plate position after the interaction has taken place. There is no doubt that interference effects are obtained with a fixed system; however, an actual delayed-choice experiment of this type has not been performed. Various tests of hidden variable theories and of the EPR paradox have been proposed (Clauser et al., 1969; Wootters and Zurek, 1979) or carried out (Faraci, 1974; Freedman and Clauser, 1972; Kasday, 1971). Aspect (1975, 1976) is undertaking an experiment to test Einstein separability by studying the polarization of correlated photons separated by spacelike intervals. The delayed-choice experiment considered here looks at the behavior of single photons with a choice of trajectories to a single recombination region in space-time rather than at pairs of photons at distant points.

For any practical realization of a delayed-choice experiment, devices analogous to the hinged photographic plate are not possible because of the high speed of propagation of the photons. It is conceptually equivalent and technologically feasible to change the beam paths, switching among stationary detectors. In our configuration, to facilitate the beam switching the "double slit" is replaced by a beam splitter, resulting in an arrangement similar to the split-beam apparatus described by Wheeler (1978).

In the proposed system (Fig. 2), the detection of both "particles" and "waves" is accom-

plished by photomultipliers in which detection events can be localized in time. We will use RCA 31024 photomultipliers, which have a pulse jitter of approximately 500 ps for detection of single photons. Discriminated photon

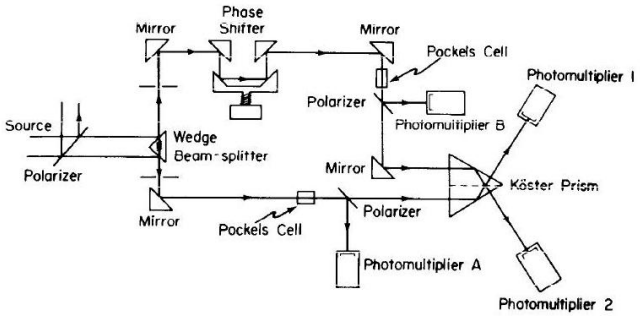


FIGURE 2. The "Delayed Choice" Interferometer

events will be recorded with the University of Maryland Lunar Ranging Program event timer (Currie et al., 1972; Steggerda, 1973), modified to accept inputs from four independent photomultipliers. The event timer will record the epoch of each photon event to an accuracy of $200 - 300$ps, as well as identify the appropriate detector. The delayed-choice switching is implemented in both anns of the apparatus by a combination of a Pockels cell and a thin-film polarizer. Upon application of a high voltage, the Pockels cells produce a 90° rotation of the plane of polarization of transmitted light. If the light from the original source is plane polarized, then the state of the Pockels cells at the time the photons pass through them will determine whether the photons are transmitted by the thin-film polarizers into the Köster prism, or reflected into photomultipliers **A** and **B**, depending upon the relative orientations of the source polarizer and the thin-film polarizers. This type of switching is routinely employed in modern short-pulse laser systems, with a rise time of the Pockels cells switching of about $2 - 3$ ns. The cumulative uncertainty in the overall system timing is thus less than 3 ns ; the photon paths from beam splitter to Pockels cells are about 15 ns light travel time.

Photomultipliers A and B play the role of "particle" detectors, since each can receive light from only one arm of the apparatus and thus is isolated from any wave interference effects. Photomultipliers 1 and 2 then serve to detect "wave" properties through the interference of the beams recombined within the Köster prism. In Figure 2, the dotted line in the Köster prism represents a beam splitter surface. The silvering of that surface is adjusted to provide a net 90° phase difference between the reflected and transmitted rays, so that if the two waves from the two arms of the apparatus entering the prism differ in phase by 90°, there will be destructive interference in the two waves leaving the prism on one side, and constructive interference on the other side. The initial 90° phase difference is supplied by the adjustable phase shifter situated in one arm of the system. The
presence of interference is thus simply indicated by the relative count rates in photomultipliers 1 and 2. In the absence of interference, for example, if one arm or the other is blocked, the two photomultipliers will exhibit identical count rates. Perfect interference would be indicated by an absence of counts in one detector

An advantage other than simplicity of using photomultipliers to detect interference effects is that there is no necessity then to control in advance the emission times of the photons entering the apparatus. Since the arrival time of each detected photon is recorded, its distance from the Pockels cells can be computed backwards from that time rather than forwards from an emission time. We may therefore use a low intensity thermal source, emitting photons at random, and may also switch the Pockels cells at random (or periodically, which is more convenient). The recorded events can later be sorted according to the computed position of each detected photon

at the time of a Pockels cells switch. The only events of interest are those for which the photons are "found" to have been between the beam splitter and the Pockels cells at the time of the switch; these events are then analyzed for possible delayed-choice effects on their interference properties as reflected in the relative number of these events found with photomultipliers 1 and 2 .

As a second approach, we plan also to use a mode-locked neodymium YAG laser as a light source. This emits pulses with a time duration of 100 ps , corresponding to a wave packet with spatial extension of 3 cin. In this case, the time can be known at which a suitable attenuated pulse containing energy equivalent to one photon enters the apparatus.

Any interpretation of the results of this experiment will depend, of course, on whether it is sensibie to speak of the "position" of individual photons, especially as regards the extrapolation backwards in time from the detection of photomultiplier pulses. It should be emphasized that there is no requirement to identify the photons entering the Köster prism as having been in one arm or the other of the apparatus; we are only interested in whether the photons, considered as particles, wave packets, etc., were between the initial beam splitter and the Pockels cells at the time when the cells changed state, with no consideration of whether the photons were "in" one arm or the other or both. That such a "one-dimensional" positioning is meaningful is clear from experiments such as the lunar ranging work (Alley, 1972; Bender et al., 1973; Silverberg, 1974; Williams et al., 1976), where a 3 ns pulse of laser radiation is emitted, sent to a distant corner reflector target, and returned. The return detections, which require single photon sensitivity, occur within a well-defined time window corresponding to the emission time plus round trip travel time. We could, in principle, calculate the emission epoch from the reception time with equally consistent results. According to the uncertainty principle, the uncertainty in a photon's position along the direction of propagation is given by $\lambda^2/\Delta\lambda$, where λ and $\Delta\lambda$ are respectively the central wavelength and bandwidth of the optical bandpass filter at the entrance to the delayed-choice apparatus. Choosing $\lambda/\Delta\lambda$ to be $\simeq 50$ gives a position uncertainty of $\simeq 50\lambda$, which
is negligible compared to the dimensions of the apparatus while still permitting small path length differences in the two arms without eliminating interference.

All measurements for calibration purposes such as determining the overall photon count rate, relative transmissions of the two arms overall and of individual components, photomultiplier efficiencies and dark rates, and adjustments of the phase shifter, can be made with a static system. The basic split-beam/Köster prism interferometer is the principal part of an existing long baseline stellar interferometer (Liewer, 1979), so that the optical stability of and detection of interference with the system have already been verified. This experiment is further forgiving in that by asking only one simple question (at least initially), i.e., does the delayed-choice switching of the Pockeis ceils affect the wave/particle properties exhibited by photons in a static system, there is no necessity for ideal behavior of components such as the thin-film polarizers, the initial beam splitter, or the Köster prism. The initial experiment will be to detect gross effects; refinements can foliow if the resuits are interesting.

The most "interesting" result would be an observable delayed-choice effect on the photons' interference. At present, it is safe to say that few physicists would expect such an effect. However, until questions of superluminal connections (Stapp, 1977), hidden variable theories (see d'Espagnat, 1979, for a review), or the continuing problem of interpretation of the wave function (Wheeler, 1977) are satisfactorily answered, we believe that it is desirable to continue to test and probe all fundamental predictions of quantum mechanics as it becomes technologically possible to do so.

The undertaking of this experiment was inspired by an Einstein Centennial Address delivered at the University of Maryland by J. A. Wheeler. We are grateful to A. Shimony and to A. Wightman for their encouragement.

27 IV. Field Measurements

27.1 IV.1 Extension of the Uncertainty Principle to Relativistic Quantum Theory by Landau, Peierls

It is shown by considering possible methods of measurement that all the physical quantities occurring in wave mechanics can in general no longer be defined in the relativistic rannge. This is related to the well-known failure of the methods of wave mechanics in that range.

27.1.1 1. Introduction

It is known that the application of the methods of wave mechanics to problems in which the speed of light cannot be regarded as infinite leads to absurd results. In the first place, states with negative mass appear in Dirac's relativistic equation [1]. This difficulty arises because the relation between momentum and energy in relativity theory is quadratic, so that two energy states are possible for a given momentum. In contrast to classical ($h = 0$) relativity theory, where the continuous change of all quantities means that transitions between the two kinds of state are impossible, such transitions cannot reasonably be forbidden in quantum theory.

In the second place, the interaction of a charged particle with the field produced hy itself is inevitably divergent [2].

The infinite zero-point energy of the radiation field which occurs on quantisation of the field [3] can be avoided by the use of suitable variables [4], but it still has the effect that the energy-density matrix elements become infinite. This is very closely related to the self-energy difficulty mentioned above (see also ref. 5).

This complete failure of the theory suggests that in the range considered the physical requirements for the applicability of the methods of wave mechanics are no longer satisfied. The present paper investigates this problem. †

27.1.2 2. The Concept of Measurement in Wave Mechanics

The significance of any physical theory is to derive from the result of an experiment conclusions regarding the results of subsequent experiments. Thus the relations between measurements and the physical states of a system are

L. Landau und R. Peierls, Erweiterung des Unbestimmtheitsprinzips fr die relativistische Quantentheorie, Z. Phys. 69, 56 (1931).

† The uncertainty relations on which our conclusions are based are derived mainly from discussions in Copenhagen. Professor Bohr's attitude to these relations will be described in an article to appear shortly in Nature.

‡ This section is essentially a deveiopment of ideas put forward by N . Bohr in his lecture at Como [6].

Translation originally published in Collected Papers of Landuu, D. ter Haar, ed., pp. 40-51, Gordon and Breach, New York (1965).

of two kinds. Firstly, the measurement determines the state of the system after the measurement is made, and secondly it examines the state of the system which existed before the measurement. In classical ($n = 0$) mechanics this distimetion is of no importance, since the states of the system before and after the measurement can be regarded as identical.

In wave mechanics, however, the situation is quite different, since the measurement always causes a change in the state of the system, and this change is in principle impossible to determine. If the measurement had no other property, the wave-mechanics description would be neither possible nor meaningful. It is necessary to make use of another physical property of

measurements, which is usually described as repeatability. This signifies that, when the same measurement is immediately repeated, the same result is certainly obtained. In this form, however, the hypothesis is physically incorrect in most cages, as will be shown in more detail below; and in this strict form it is not necessary for wave mechanics. The important point is that for any system there should exist predicidule measurements. This means measurements such that for overy result there is a state of the system in which this measurement certainly gives that result. For, if this requirement were not fulfilled, the state of the system after a measurement couid not be described by a ψ function. This may be seen as follows. We can describe the state of the system and the measuring apparatus together by a wave function which, before the measurement, consists of a product $\psi\varphi_0$. Fiere ψ is the initialiy arbitrary wave function of the system, and $\%_0$ the known wave function of the measuring apparatus. After the interaction, the wave function will in general no longer be a product. If we expand it in terms of the eigenfunctions of the measuring apparatus, in the form $\sum \Psi_n\varphi_n$, then Ψ_n describes the state in which the system remains after the measurement. In general, the form of ψ_n depends on that of ψ. If the wave function of the system is to be deduced from an observation of the measuring apparatus, ψ_n must be independent of ψ apart from a constant factor, i.e. $\psi_n = a_n u_n$, with u_n normalised to unity. From the linearity of the wave equation it follows that a_n depends linearly on ψ, i.e. can be written in the form $\int \psi v_n^* \, \mathrm{d}\tau$, with v_n any function dependent on the process of measurement. Then $|a_n|^2$ is the probability that the measurement gives the nth result. The sum of all these probabilities must be equal to unity, i.e. $\Sigma\,|a_n|^2 = 1$ independent of ψ (rpovided that ψ is normalised):

$$\sum a_n a_n^* = \int \sum a_n v_n \psi^* \, \mathrm{d}\tau$$

This expression must therefore always equal unity if $\int \psi\psi^* \, \mathrm{d}\tau = 1$, i.e. we must have

$$\sum a_n v_n = \psi$$

(The v_n form a complete orthogonal system). From this, however, it follows that the measurement is predictable if we take ψ to have the particular value of one of the v_n; then only one of the a_n is not zero. The repeatability of the Gre 2a
measurement would signify that the v_n and the u_n are identical, and this is not in general true. †

If, however, the wave function of the system can not be determined by any measurement, it can have no physical meaning. The use of wave functions would then be as pointless as, for example, the use of the concept of paths in quantum mochanics. Thus the existence of predictable measurements is an absolutely necessary condition for the validity of wave mechanics.

The condition of repeatability cannot in general be satisfied. This is particularly seen if the time necessary for the measurement is baken into account. This time is restricted by the relation $\Delta E \Delta t > \hbar$, which has very often been stated, but which has been correctly interpreted only by Bohr [6]. Clearly it dues noi signify that the energy can not be known exactily at a given time (for in that case the concept of energy would have no meaning), nor does it mean that the energy can not be measured with arbitrary accuracy within a short time. We must take into account the change caused by the process of measurement even in the case of a predictable measurement, i.e of the difference between the result of the measurement (v_n) and the state after the measurement (u_n). The relation then signifies that this difference causes an energy uncertainty of the order of $\hbar/\Delta t$, so that in time Δt no measurement can be performed for which the energy uncertainty in both states is less than $\hbar/\Delta t$.
This follows from a consideration of the time evolution of the interaction process. The method of the variation of constants shows that transitions within short times occur not only between

states which satisfy the condition $E+\varepsilon = E'+\varepsilon'$ (E and E' being the energy of the system before and after the transition, ε and ε' that of the apparatus). These states are given preference by resonance only after a long time, the corresponding transition probabilities increasing greatly with time. In practice, after a time Δt, only transitions for which $|E+\varepsilon-E'-\varepsilon'| \lesssim \hbar/\Delta t$ are of importance. This fact does not, of course, contradict the strict validity of the law of conservation of energy in wave mechanics, but the energy of interaction between the system and the apparatus is also indeterminate by the same amount. In the most favourable case, where ε and ε' are precisely known, the uncertainty must be $\Delta(E-E') > \hbar/\Delta t$.
This relation has important consequences as regards the measurement of momentum. Any measurement of momentum is made by allowing the body to collide with another. In measuring a component of momentum (most simply done by collision with a plane mirror) the law of conservation of momentum is to be applied rigorously, but that of conservation of energy applies only to within $\hbar/\Delta t$, because of the unknown interaction energy. Thus to determine the
† In a measurement which occupies a short time it can easily be shown that the u_n are identical with the v_n only when the corresponding operator commutes with the energy of interaction between the system and the apparatus. In wave mechanics (neglecting relativity) this interaction energy is always a function of the co-ordinate. The only quantity for which a repeatable measurement is possible is therefore the co-ordinate. Measurements of the co-ordinate always actually have this property. It is also seen that the u_n need not in general be orthogonal, i.e. the measurement does not in general diagonalise an operator. This physical circumstance also is usually overlooked in the presentation of transformation theory. in the presentation of transformation theory.
particle momentum $\boldsymbol{P}$ we have the equations

$$\boldsymbol{p}+\boldsymbol{P}-\boldsymbol{p}'-\boldsymbol{P}'=0$$
$$|\varepsilon+\boldsymbol{\Sigma}-\varepsilon'-\boldsymbol{E}'| \gtrsim \frac{\hbar}{\Delta t}$$

$\boldsymbol{p}, \boldsymbol{p}', \varepsilon, \varepsilon'$, i.e. the motion of the measuring apparatus before and after the collision, may be regarded as known. Then $\Delta P = \Delta P'$ and, since $\Delta E = v\Delta P$,

$$(v-v')\,\Delta P > \frac{\hbar}{\Delta t}. \tag{1}$$

Thus any measurement of momentum necessarily involves a definite change of momentum (in addition to the unknown ehange which restricts the accuracy of the measurement). † This fact was first recognised by Bohr [6]. The non-repeatability of the momentum measurement in a short time is thus shown with particular clarity. Momentum measurements which last a long time, on the other hand, are meaningful only for free particles.

27.1.3 3. Momentum Measurement in the Relativistic Case

We now wish to make use of relativity, i.e. of the finite speed of propagation. There exists as yet no satisfactory relativistic quantum theory, but it is clear that here also we certainly cannot go beyond the limits imposed on the accuracy of measurement by the general principles of wave mechanics.
The scope of the relation just derived for momentum measurement is considerably extended by relativity. In the non-relativistic theory, the definite change of velocity could be made arbitrarily large, and so the momentum could be measured with arbitrary accuracy even in a short time. If, however, we take into account the fact that the velocity cannot exceed c, then $v-v'$ can be at most of the order of c, so that equation (1) gives

$$\Delta P \Delta t > \frac{\hbar}{c}. \tag{2}$$

The inequality (2) is particularly casy to derive for the state after the measurements. If we assume that the particle had a definite position before the measurement, then after a time Δt, on account of the finite velocity limit, the position is still known with accuracy $c\Delta t$. If the momentum after this time were determined more accurately than as given by (2), this would contradict the result $\Delta P \Delta q > \hbar$.

† Here an important point is that not every Hamilton's function can actually occur in nature; as already mentioned, the interaction function is always a function of the co-ordinates and so does not commute with the momentum. If the form of the Hamilton's function could be chosen at bitrarily, the momentum could be measured in an arbitrarily short time without change of velocity; this is a trivial deduction from the fact that co-ordinates and momenta are then equiablent.

On account of (2) the concept of momentum has a precise significance only over long times. Thus, in cases where the momentum changes appreciably within such times, the use of the concept of momentum is purposeless.

In the measurement of momentum of a charged hody, in addition to the above-mentioned inaccuracy, a further perturbation of the measurement arises because the body will emit radiation in the necessary change of velocity. We shall consider only the case where the velocity of the body before the measurement is certainly small compared with c. In this case it is favourable to conduct the measurement so that after the measurement the velocity is again considerably less than c. For, if the velocity approaches c, the relation (1) gives very little benefit, while the accuracy is greatly reduced by the emission of radiation. Thus the non-relativistic formula for radiation damping can be used. The energy omitted is then

$$\frac{e^2}{c^3} \int \dot{v}^2 \, \mathrm{d}t,$$

where e is the charge on the body. This energy evidently has its least value for uniform acceleration, i.e. for $\dot{v} = (v' - v)/\Delta t$, so that the energy emitted is

$$\frac{e^2}{c^3} \frac{(v' - v)^2}{\Delta t}.$$

This unknown change of energy has to be taken into account in the energy balance, and there thus arises in the momentum a further inaccuracy:

$$(v' - v)\, \Delta P > \frac{e^2}{c^3} \frac{(v' - v)^2}{\Delta t},$$

or

$$\Delta P \Delta t > \frac{e^2}{c^3} (v' - v) \tag{3}$$

For electrons this inequality gives no new information, since even in the most unfavourable case where $v \sim v' + c$ it gives only $\Delta P \Delta t > e^2/c^2$, and this is weaker than (2), since $e^2 < \hbar c$. For macroscopic bodies, however, the relation (3) is significant. Multiplication by (i) gives

$$\Delta P \Delta t > \frac{\hbar}{c} \sqrt{\frac{e^2}{\hbar c}}, \tag{4}$$

and in this form we shall make use of it later. The inequality (4) is, of course, valid independently of the method of measurement used, and in particular when the measurement

is made by means of the charge on the body, as in the case of the Compton effect, where, in addition to the Compton scattered radiation used in the measurement, there is a further radiation corresponding to that discussed above, obtained when higher approximations are taken into account in the perturbation calculation for the interaction between the radiation and the particle [7]. (In the ordinary Compton effect with electrons this effect is of no importance, on account of the smallness of $e^2/\hbar c$.)

27.1.4 4. Field Measurement

The simplest method of measuring an electric field is to observe the acceleration of a charged test body. In order to avoid interference by magnetic fields, we use a body of very large mass and very small velocity. Let the momentum of the body before the measurement be known, and let the momentum afterwards be measured, again with accuracy ΔP. From this we car deduce the electric field strength with accuracy such that

$$e\Delta\mathscr{E}\Delta t > \Delta P. \tag{5}$$

In addition, however, the condition (4) must be satisfied in the momentum measurement. Multiplication of equations (4) and (5) gives

$$\Delta\mathscr{E} > \frac{\sqrt{\hbar c}}{(c\Delta t)^2}. \tag{6}$$

For the magnetic field strength we easily obtain the same result by considering the motion of a magnetic needle:

$$\Delta\mathscr{H} > \frac{\sqrt{\hbar c}}{(c\Delta t)^2}. \tag{6a}$$

If it is desired to measure the electric and magnetic field strengths simultaneously, then, in addition to the effects already discussed, we have to take into account the effect on the needle of the magnetic field due to the charged body and vice verse. This magnetic field is, in order of magnitude,

$$\Delta\mathscr{H} > \frac{e}{(\Delta l)^2}\cdot\frac{v'}{c} \tag{7}$$

where Δe is the distance between the test body and the needle. If we multiply this inequality by equations (5) and (1), then (with $v = 0$) we have

$$\Delta\mathscr{E}\Delta\mathscr{H} > \frac{\hbar c}{(c\Delta t)^2}\cdot\frac{\mathbf{i}}{(\Delta c)^2}. \tag{6 b}$$

This condition differs from the product of (6) and (6a) in that $c\Delta t$ in the denominator is partly replaced by Δe.

If follows from (6), (6a) and (6b) that for $\Delta t = \infty$ the measurement can be made arbitrarily accurate for both $\mathscr{E}$ and $\mathscr{H}$. Thus static fields can be completely defined in the classical sense. †

In wave fields (that is, field which are further than $c/v = \lambda$ from the bodies which produce them), it is sufficient to use (6) and (6a), because as a result of the coupling of the space and time variation nothing is discovered about the

† Our thanks are due to Professor Bohr for pointing out this situation and the significance of time in general.

field if the region of measurement has an extent less than $c\Delta t$ for a given Δt. Thus here also

the measurements of $\mathscr{E}$ and $\mathscr{H}$ do not interfere, and to the extent that the ficld strengths can be measured in accordance with (6) and (6a) they can be measured simultaneously. Thus the field strengths are in accordance with the classical theory inasfar as they can be defined at all. In the quantum range, on the other hand, the field strengths are not measurable quantities. †

27.1.5 5. Measurements on Light Quanta

We shall now show that in a radiation field no measurements can be carried out with certainty within a short time, i.e measurements for which every possible result gives information about the state of the system. (Thus we do not consider such moasurements as, for example, a measurement of position by means of a collision which does not occur with probability unity within the period of observation, so that, although a deflection of the test body shows that the budy under measurement was at the point considered, the absence of such a deflection shows nothing.) The time necessary for the measurement depends on the state of the system. If the energy of the radiation field is approximately determined as E, we shall show that this time is greater than t/E. Since the field consists of light quanta, the greatest frequency occurring in the Fourier resolution of the field can be at most $E/\hbar$; if we carry out the measurements in times small compared with h/E, we remain within the period of oscillation, and so the field strength may be regarded as constant during the measurements. All measurements in such short times are therefore field measurements and are subject to the inaccuracy (6). Thus, in order than an effect should be detectable, the ficld strength must considerably exceed $\sqrt{\hbar c/(c\Lambda t)^2}$. The smallest wavelength occurring, on the other hand, is $\hbar c/E$, and so the field strength, if non-zero at any point, must be non-zero in a region of at least this extent. Consequently, the total field energy must be at least of the order $E > \mathscr{E}^2(\hbar c/E)^3 > (\hbar c)^4/E^3(c\Delta t)^4$, i.e.

$$\Delta t > \frac{\hbar}{E}, \tag{8}$$

in contradiction with our hypothesis. Thus measurements which do not satisfy equation (8) are impossible.

This result applies in particular, of course, when the radiation field consists of a single quantum of light. Within the time given by (8), a quantum of light is therefore undetectable, and in particular its position cannot be determined with any accuracy. In a measurement of position, the time to which that position refers is therefore indeterminate by more than $\hbar/E$. If the measurement of position is to be used to investigate a state, as discussed in section 2, we are interested in the position at a time up to which the state under investigation

† The inaccuracy for the field measurement with an electron found by Jordan and Fock [8] is greater than (6) and therefore proves only that the electron is not a suitable means of measuring the field.

(i.e. the state whose energy was of the order of E) existed. The measurement of position indicates such a quantity with inaccuracy, at best $\Delta q > \hbar c/E$.

It might be thought that the accuracy could be improved by measuring momentum at the same time as position (within the limits given by $\Delta P \Delta q > \hbar$, of course), and seeking to deduce how far and in which direction the light quantum has mean while travelled. A closer examination, however, shows that the resulting accuracy can be no better than $\hbar c/E$. Thus in every state it is meaningful to give the probability of presence of the light quantum only for regions large compared with the wavelength, and the position of the light quantum is a meaningful concept only in geometrical optics.

If the number of light quanta varies appreciably within the period of oscillation, the concept of light quanta itself is meaningless.

27.1.6 6. Measurements on Material Particles

Let us now investigate the corresponding relations for material particles. (We shall always speak of electrons, but the arguments of course apply for any kind of material particle.) Such particles can best be detected by means of collision processes, for example using the Compton effect. Thus the presence of an electron is demonstrated by making two momentum measurements on the light quantum and deducing from the change in momentum that a collision has occurred in between. Here, however, the course of the provess depends considerably on the length of the time interval between the two measurements. Over long times the Compton effect is obtained, i.e. the momentum of the light quantum changes either not at all or by an amount determined by the initial momenta, which can be made arbitrarily large by using very hard radiation. Over very short times, however, any changes of momentum may occur, provided that the law of conservation of momentum remains valid; the sum of the energies of the electron and the light quantum need be conserved only to within $\hbar/\Delta t$, as shown in section 2 . For the same reasons as in measurements on light quanta, the small momentum changes have much the greatest probability. An elementary calculation shows that the second behaviour begins when the time interval is no longer large compared with $\hbar/E$, where E is the approximate energy of the electron before the measurement.

Thus, if the duration of the process of measurement is made shorter than $\hbar/E$, the momentum of the light quantum (and therefore also that of the electron) changes by an arbitrary amount. Hence, from the fact that no measurable change of momentum has occurred, we cannot conclude that no collision has taken place. Physically this signifies that the measurement of the momentum of the light quantum destroys the initial state of the electron. We cannot ensure that the electron is found with probability unity at the first measurement: if it was in a volume δq before the measurement, a time $\delta q/c$ is necessary before we can be sure that the light has reached the electron. Since $\delta q/c > \hbar/c\delta P > \hbar/cP > \hbar/E$, we should therefore have to make several measurements before being able to detect the electron, and thus completely destroy its state before we find it. Measurements in times less than $\hbar/E$ are therefore useless.

We now again ask how accurately this measurement can be used to derive the position of the electron at a time up to which it was in its former state. To do this, of course, only the knowledge about the velocity which is compatible with the position measurement can be used, and not, for example, the velocity in the state before the measurement. If an exact measurement of position is made, no information is obtained as regards the velocity, which thus remains indeterminate within c. The co-ordinate can therefore be derived only with an error $\Delta q > \hbar c/E$. Elementary considerations show that no higher accuracy can be achieved by measuring the momentum and co-ordinate simultaneously with any accuracies compatible with $\Delta P \Delta q > \hbar$. Thus

$$\Delta q > \frac{\hbar c}{E} \tag{9}$$

represents the limit of the accuracy with which the position of the eiectron can reasonably be defined. If in particular, if the velocity of the electron is not very close to c, this becomes

$$\Delta q > \frac{\hbar}{mc}. \tag{10a}$$

The derivation of (10a) shows that it is valid only for electrons which are not moving too rapidly. The statement frequently found in the literature that $\hbar/mc$ is a general limit for the accuracy of measurements of position is based on incorrect arguments.

A superficial consideration might suggest that the uncertainty relations derived above are not relativisticaliy invariant. In reality, of course, there can be no contradiction with relativity, which has been taken into account throughout the derivations. The explanation is that the

inequalities themselves need not transform in a relativistically invariant manner, since the most favourable possible measurements of a quantity need not be so when they are viewed from a moving system of co-ordinates. Thus we have only to require that the limit of accuracy should not be exceeded when such a measurement is viewed from a moving system of co-ordinates. This requirement is, of course, always satisfied.

Particular care is needed in this respect with position measurements, for here the statement of the problem is itself not relativistically invariant, but distinguishes a time axis, since we ask for the co-ordinate at a time up to which the unperturbed state existed.

27.1.7 7. Mathematical Failure of the Methods of Wave Mechanics

The above-stated unmeasurability of all wave-mechanical quantities also appears, of course, in the formalism which results when we attempt to apply the methods of wave mechanics to the relativistic case.

The most fundamental quantity in the theory, both for electrons and for light quanta, is the momentum; this is of course due to the fact that if it remains constant in time it can be defined with arbitrary accuracy, although very long times are needed for its measurement. This latter fact does not, of course, appear in the wave-mechanics formalism, and in consequence the statements of the theory regarding short times have no meaning.

The unmeasurability of the position, on the other hand, is directly expressed in the formalism. For electrons this is because the Dirac equation also allows the physically meaningless solutions with negative energy. The result of a measurement can, of course, in reality only be a wave function composed only of states with positive energy. Such states cannot, however, form an arbitrary wave packet. It is easily seen that the dimensions of a wave packet in general cannot be less than $\hbar/mc$. There are, it is true, special wave packets of smaller size (namely those whose centre moves at almost the speed of light †), but the corresponding wave functions do not form a complete system, and the state before the measurement cannot in general be expanded in terms of them. This corresponds to the result shown earlier that in short times a determination of position may sometimes chance to be possible, but a measurement cannot be carried out with certainty.

The conditions for light quanta are still more extreme in that no mathematical expression can be given for the probability density. This is seen from the fact that, on account of polarisation properties, the wave function for a light quantum must be a tensor of rank two [4]. The probability density and current must form a four-vector, which is impossible, because they depend quadratically on the wave function. In geometrical optics it is, of course, possible to construct wave packets in which all effects vanish outside a certain region. But here also these wave functions do not form a complete system.

The unmeasurability of the field strength is shown by the fact that in empty space (no light quanta) the field strength operator [2,4] is not zero, but even the expectation of the square of the field strength is infinite. This is related to the fact that for $\Delta t = 0$ we have from (6) an infinite indeterminacy of the field strength.

27.1.8 8. Conclusions

We have seen that no predictable measurements can exist for the fundamental quantities of wave mechanics (except when these quantities are constant in time, and then an infinitely long time is needed for an exactly predictable measurement). It cannot, of course, be formally demonstrated that there are not in nature some particularly complicated quantities for which predictable measurements are possible, but such a speculation need not be discussed. The assumptions of wave mechanics which have been shown to be necessary in section 2 are therefore

not fulfilled in the relativistic range, and the application of wave mechanics methods to this range goes beyond their scope. It is

† Our thanks are due to Professor O. Klein for pointing this out.

therefore not surprising that the formalism leads to various infinities; it would be surprising if the formalism bore any resemblance to reality.

The applicability of wave mechanics is restricted to processes where the state of the system varies sufficiently slowly. In cases where theordinary Schrödinger's equation is applicable this is of course not always true. For radiation alone wave mechanics is never meaningful, since the limit $c = \infty$ has no meaning.

In the correct relativistic quantum theory (which does not yet exist), there will therefore be no physical quantities and no measurements in the sense of wave mechanics. One can, of course, cause the system to interact with some apparatus and ask what happens to the latter. The theory will give a probability for the result of this experiment, but this cannot be interpreted as the probability of a parameter of the system under investigation, since it can in no way be ensured that the probability of a given result is unity and that of all other results is zero. In addition, it is in principle impossible to make the duration of such an experiment arbitrarily short.

This view is confirmed by the known fact that the β-spectra of radioactive nuclei are continuous, although the uniform lifetime indicates that the nuclei are not in different states. For, if all the β-particles had the same energy, the process could be regarded as a predictable measurement.

This fact presents an insuperable difficulty in wave mechanics because, as Bohr has emphasised, it means that the law of conservation of energy is probably invalid for nuclear electrons. This law is indissolubly connected with the foundations of wave mechanics. In relativistic quantum theory, however, the preceding discussion shows that the concept of energy need not be mechanically definable. It is of course definable in a certain sense in terms of the total mass of the nucleus, because the nucleus in its motion as a whole satisfies wave mechanics, but this does not imply a predictable measurement of quantities related to the internal state of the nucleus.

If the law of conservation of energy is not valid, then in radioactive processes the mass of the whole system will of course change, but this change cannot be followed in the course of time, since the mass cannot be measured in an arbitrarily short time. If we consider the process of measurement of the mass as in section 3, the time needed for the measurement is such that

$$\Delta m \Delta t > \frac{\dot{h}}{c^2}$$

The preceding discussion is not contradicted by the fact that the spectra of protons and α-particles are discrete. On account of their large mass (low velocity) these particles obey wave mechanics even in the nucleus, rather as the nuclei in a molecule can be essentially described in classical terms despite their strong interaction with the electrons, for which classical mechanics fails completely.

One of us (Landau) thanks the Rockefeller Foundation for making it possible for him to work in Copenhagen and in Zrich.

References

1. P. A. M. Dirac. Proc. Roy. Soc. A 117, 610 (1928).

2. W. Heisenberg and W. Pauli, Z. Phys, 56, 1 (1929); 59,168 (1930).

3. P. Jordan and W. Pauli, Z. Phys. 47, 151 (1928).

4. L. Landat and R. Prrarls, Z. Phyy. 62, 188 (1930); Colleuted Fapers No 3, p. i9.

5. L. Rosenfeld, Z. Phys. 65, 589 (1930).

6. N. Bonn, Nuiurwiss. 16, 245 (1928).

7. P. Jordan and V. Fock, Z. Phys. 66, 206 (1930).

27.2 IV.2 The Measurability of the Electromagnetic Field

Commentary of Rosenfeld (1955)

When I arrived at the Institute on the last day of February, 1931, for my annual stay, the first person I saw was Gamow. As I asked him about the news, he replied in his own picturesque way by showing me a neal pen drawing he had just made* It represented Landau, tightly bound to a chair and gagged, while Bohr, standing before him with upraised forennger, was saying: "Bitte, bitte, Landau, muss ich † nur ein Wort sagen!" I learned that Landau and Peierls had just come a few days before with some new paper of theirs which they wanted to show Bohr, "but" (Gamow added airily) "he does not seem to agree-and this is the kind of discussion which has been going on all the time." Peierls had left the day before, "in a state of complete exhaustion," Gamow said. Landau stayed for a few weeks longer, and I had the opportunity of ascertaining that Gamow's representation of the situation was only exaggerated to the extent usually conceded to artistic fantasy.

There was indecd reason for excitement, for the point raised by Landau and Peierls was a very fundamental one. They questioned the logical consistency of quantum electrodynamics by contending that the very concept of elec-

- I am afraid this work of art has been allowed to disintegrate before its historical value could be realized.

This is a familiar danicism of Bohr's for "darf ich."

tromagnetic field is not susceptible, in quantum theory, to any physical determination by means of measurements. The measurement of a field component requires determinations of the momentum of a charged test-body; and the reaction from the field radiated by the test-body in the course of these operations would (except in trivial cases) lead to a limitation of the accuracy of the field measurement, entirely at variance with the premises of the theory. In fact, the quantization of the field only entails reciprocal limitations of the measurements of pairs of components, arising from their non-commutability, but no limitation whatsoever to the definition of any single field component. On the other hand, one had to face another inescapable consequence of the field quantization, the occurrence of irregular fluctuations in the value of any field component; the existence of this fluctuating "zero-field" (as it was called because it persists even in a vacuum) was known to be responsible for one of the divergent contributions to the self-energy of charged particles, but its meaning was very obscure. Landau and Peierls, somewhat illogically, tried to bring it in relation with their alleged limitation of measurability of the field, and this only further confused an already tangled issue.

Bohr's state of mind when he attacked the problem reminded me of an anecdote about Pasteur. When the latter set about investigating the silk-

worm sickness, he went to Avignon to consult rabre. "I should like to see cocoons," he said, "I have never seen any, I know them only by name." Fabre gave him a handful: "he took one, turned it between his fingers, examined it curiously as we would some singular object brought from the other end of the world. He shook it near his ear. 'It rattles,' he said, much surprised, 'there is something inside.'" My first task was to lecture Bohr on the fundamentals of field quantization; the mathematical structure of the commudation relations and the underlying physical assumptions of the theory were subjected to unrelenting scrutiny. After a very short

time, needless to say, the roles were inverted and he was pointing out to me essential features to which nobody had as yet paid sufficient attention.

His first remark, which threw decisive light on the problem, was that field components taken at definite spacetime points are used in the formalism as idealizations without immediate physical meaning; the only meaningful statements of the theory concern averages of such field components over finite space-time regions. This meant that in studying the measurability of field components we must use as testbodies finite distributions of charge and
current, and not point charges as had been loosely done so far. The consideration of finite test-bodies immediately disposed of Landau and Peierls' argument concerning the perturbation of the momentum measurements by the radiation reaction: it is easily seen that this reaction is so much reduced, for finite test-bodies, as to be always negligible.

On the other hand, the construction and manipulation of extended testbodies proved a most perplexing affair. . . . in fact, it seemed as if we had hii upon mode of measurement exactly suited to give the best combined accuracy, for pairs of field determinations, compatible with the theoretical limitation. We little imagined that it would still take us almost two years to reach that goal

At the end of our laborious inquiry, we had completely vindicated the consistency of quantum electrodynamics, at least in its simplest form. Our increased insight invited a reassessment of the scope of the analysis we had just completed. We had set out on the suspicion of grave defects in the logical structure of the theory, and used the direct method of testing definitions of concepts by investigating the concrete measuring processes they embody.

27.3 IV. 2 on the Question of the Measurability of Electromagnetic Field Quantities by Bohr, Rosenfeld

27.3.1 1. Introduction

The question of limitations on the measurability of electromagnetic fieid quantities, rooted in the quantum of action, has acquired particular interest in the course of the discussion of the still unsolved difficulties in relativistic atomic mechanics. On the basis of exploratory considerations, Heisenberg [1] atiempied to demonstrate that the connection between the limitation on the measurability of field quantities and the quantum theory of fields is similar to the relationship between the complementary limitations on the measurability of kinematical and dynamical quantities expressed in the indeterminacy principle and the non-relativistic formalism of quantum mechanics. However in the course of a critical investigation of the foundations of the relativistic generalization of this formalism, Landau and Peierls [2] came to the conclusion that the measurability of field quantities is subjected to further restrictions which go essentially beyond the presuppositions of quantum field theory, and which therefore deprive this theory of any physical basis.

At first glance, one might see in this contradiction a serious dilemma. On the one hand, the quantum theory of fields surely ought to be considered a consistent re-interpretation of classical electromagnetic theory in the sense of the correspondence argument, just as quantum mechanics represents a reformulation of classical mechanics adapted to the existence of the quantum of action. On the other hand, quantum electrodynamics has essentially increased the difficulties, already encountered in classical electron theory, of a harmonious blending of field theory and atomic theory. However, closer consideration shows that the various problems involved here can be to a large extent separated from each other, since the quantum-electromagnetic formalism in itself is independent of all ideas concerning the atomic constitution of matter. This is evident from the fact that in addition to the velocity of light only the quantum of action

Originally published under the title, "Zur Frage der Messbarkeit der elektromagnetischen

Feldgrössen," Mat.-fys. Medd. Dan. Vid. Selsk., 12, no. 8 (1933); this translation into English by Aage Petersen is taken from Selected Papers of Lon Rosenfeld, Cohen and Stachel, eds. (1979), Reidel,
enters the formalism as a universal constant; for these two constants obviously do not suffice to determine any specific space-time dimensions. In the quantum theory of atomic structure such a determination will be obtained only by the inclusion of the electric charge and the rest masses of the elementary particles.

Just the insufficient distinction between field theory and atomic theory is the principal reason for the conflicting results of previous investigations of the measurability of ficld quantities in which single electrically charged mass points were used as test bodies. The utilization of classical electron theory, in the sense of the correspondence argument, which underlies current atomic mechanics, rests above all on the smallness of the elementary charge in comparison with the square root of the product of the quantum of action and the velocity of light, which makes it possible to treat all radiation reactions as small compared to the ponderomotive forces exerted on the particles. However, in measurements of tield quantities it turns out to be essential to be able to adjust the charge of the test bodies to an extent which would be in conflict with the latter presupposition if one were to consider these bodies as point charges. As we shall see, however, these difficulties disappear if one uses test bodies whose linear extensions are chosen sufficientily large, compared to atomic dimensions, that their charge density can be considered approximately constant over the whole body.

In this connection, it is also of essential importance that the customary description of an electric field in terms of the field components at each space-time point, which characterizes classical field theory and according to which the field should be measurable by means of point charges in the sense of the electron theory, is an idealization which has only a restricted applicability in quantum theory. This circumstance finds its proper expression in the quantum-electromagnetic formalism, in which the field quantities are no longer represented by true point functions but by functions of space-time regions, which formally correspond to the average values of the idealized field components over the regions in question. The formalism only allows the derivation of unambiguous predictions about the measurability of such region-functions, and our task will thus consist in investigating whether the complementary limitations on the measurability of field quantities, defined in this way, are in accordance with the physical possibilities of measurement.

Insofar as we can disregard all restrictions arising from the atomistic structure of the measuring instruments, it is actually possible to demonstrate a complete accord in this respect. Besides a thorough investigation of the construction and handling of the test bodies, this demonstration requires, however, consideration of certain new features of the complementary mode of description, which come to light in the discussion of the measurability question, but which were not included in the customary formulation of the indeterminacy principle in connection with nonrelativistic quantum mechanics. Not only is it an essential complication of the problem of field measurements that, when comparing field averages over different space-time regions, we cannot in an unambiguous way speak about a temporal sequence of the measurement processes; but even the interpretation of individual measurement results requires a still greater caution in the case of field measurements than in the usual quantummechanical measurement probiem.

Characteristic of the latter problem is the possibility of attributing to each individual measurement result a well-defined meaning in the sense of classical mechanics, while the quantum-imposed interaction, uncontrollable in principle, between instrument and object is fully taken into account through the influence of each measuring process on the statistical expectations testable in succeeding measurements. In contrast, in measurements of field quantities, indeed, every measuring result is well defined on the basis of the classical field concept; but, the limited applicability of classical field theory to the description of the unavoidable electromagnetic

field effects of the test bodies during the measurement implies, as we shall see, that these field effects to a certain degree influence the measurement result itself in a way which cannot be compensated for. However, a closer investigation of the fundamentally statistical character of the consequences of the quantum-electromagnetic formalism shows that this influence on the object of measurement by the measuring process in no way impairs the possibility of testing such consequences, but rather is to be regarded as an essential featurc of the intimate adaptation of quantum field theory to the measurability problem.

Before we turn to a detailed exposition of the considerations indicated above, we want to stress once more that the fundamental difficulties which confront the consistent utilization of field theory in atomic theory remain entirely untouched by the present investigation. Indeed, consideration of
the atomistic constitution of all measuring instruments would be essential for an assessment of the connection between these difficulties and the well-known paradoxes of the measurement probiem in relativistic quantum mechanics. Also particularly relevant in this context is the limitation which the finite value of the elementary charge compared to the square root of the product of the velocity of light and the quantum of action places on atomic mechanics based on the correspondence argument. [3]

27.3.2 2. Measurability of Fields According to Quantum Theory

The quantum electromagnetic formalism found its starting point in the quantum theory of radiation developed by Dirac, which is characterized by the introduction of a noncommutativity, consistent with the quan-tum-mechanical commutation relations, of canonically conjugate amplitudes of vibration of a radiation field. On the basis of this theory, Jordan and Pauli set up commutation relations between the electromagnetic field components for the case of charge-free fields, and the formalism was then brought to a certain completion by Heisenberg and Pauli who treated the interaction between field and material charges on contespondence lines. However, the consistent application of the theory to atomic problems is essentially impaired by the occurrence of the well-known paradoxes of the infinite self-energy of the elementary particles, which were not removed by Dirac's proposed modifications in the representation of the formalism. [4] Yet, in our discussion of the limitations of the measurability of field quantities these difficulties play no role, since for this purpose the atomistic structure of matter is not an essential issue. It is true that the measurement of fields requires the use of material charged test bodies, but their unambiguous application as measuring instruments depends exactly on the extent to which we can treat their response to the fields as well as their influence as field sources on the basis of classical electrodynamics.

In these circumstances we may restrict ourselves to the pure field theory, and thus take the commutation relations for charge-free fields as our starting point for the investigation of the consequences of the quantum electromagnetic formalism with respect to the measurability of field quantitics. Using the usual notation, $[p, q] = pq \quad qp$, we thus have the
following typical relations between the field components in two spacetime points (x_1, y_1, z_1, t_1) and (x_2, y_2, z_2, t_2), from which the remaining commutation relations are obtained by cyclic permutation: [5]

$$\left\{\begin{array}{l} \left[\mathfrak{F}_x^{(1)}, \mathfrak{E}_x^{(2)}\right] = \left[\mathfrak{S}_x^{(1)}, \mathfrak{S}_x^{(2)}\right] = \sqrt{-1}\hbar\left(A_{xx}^{(12)} - A_{xx}^{(21)}\right) \\ \left[\mathfrak{F}_x^{(1)}, \mathfrak{E}_y^{(2)}\right] = \left[\mathfrak{S}_x^{(1)}, \mathfrak{S}_y^{(2)}\right] = \sqrt{-1}\hbar\left(A_{xy}^{(12)} - A_{xy}^{(21)}\right) \\ \left[\mathfrak{C}_x^{(1)}, \mathfrak{S}_x^{(2)}\right] = 0 \\ \left[\mathfrak{C}_x^{(1)}, \mathfrak{S}_y^{(2)}\right] = -\left[\mathfrak{S}_x^{(1)}, \mathfrak{C}_y^{(2)}\right] = \sqrt{-1}\hbar\left(B_{xy}^{(12)} - B_{xy}^{(21)}\right) \end{array}\right. \tag{1}$$

Here, $\mathfrak{F}_x^{(1)}, \mathfrak{F}_y^{(1)}, \mathfrak{F}_z^{(1)}, \mathfrak{Y}_x^{(1)}, \mathfrak{Y}_y^{(1)}, \mathfrak{G}_z^{(1)}$ are the electric and magnetic field components at the space-time point (x_1, y_1, z_1, t_1) while the foilowing abbreviations have been used:

$$\left\{\begin{array}{l} A_{xx}^{(12)} = -\left(\frac{\partial^2}{\partial x_1 \partial x_2} - \frac{1}{c^2}\frac{\partial^2}{\partial t_1 \partial t_2}\right)\left\{\frac{1}{r}\delta \,\middle|\, t_2 - t_1 - \frac{r}{c}\right)\right\} \\ A_{xy}^{(12)} = -\frac{\partial^2}{\partial x_1 \partial y_2}\left\{\frac{1}{r}\delta\left(t_2 - t_1 - \frac{r}{c}\right)\right\} \\ B_{xy}^{(12)} = -\frac{1}{c}\frac{\partial}{\partial t_1 \partial z_2}\left\{\frac{1}{r}\delta\left(t_2 - t_1 - \frac{r}{c}\right)\right\} \end{array}\right. \tag{2}$$

Further, $\hbar$ is Planck's constant divided by $2\pi, c$ the velocity of light, and r the spatial separation between the two points. Finally, δ denotes the symbolic function introduced by Dirac which, as is well known, is characterized by the property

$$\int_{t'}^{t''} \delta(t - t_0)\,\mathrm{d}t = \left\{\begin{array}{l} 1 \text{ for } t' < t_0 < t'' \\ 0 \text{ for } t_0 < t' \text{ or } t_0 > t'' \end{array}\right. \tag{3}$$

and which is formally differentiated like an ordinary function.
The occurrence of the δ-function, defined in (3), in the commutation relations (1) brings to the fore the fact mentioned above that the quantum theoretical field quantities are not to be considered as true point functions but that unambiguous meaning can be attached only to space-time integrals of the field components. With a view to the simplest possibility of testing the formalism we shall consider only averages of field components over simply connected space-time regions whose spatial exten-
sion remains constant during a given time interval. Thus, for example, if the volume of such a region G is denoted by V and the corresponding time interval is T, we define the average value of $\mathbb{E}_x$ by the formula

$$\mathbb{E}_x^{(G)} = \frac{1}{VT}\int_T \mathrm{d}t \int_V \mathfrak{E}_x \,\mathrm{d}v. \tag{4}$$

For the average values of two field components over two given spacetime regions I and II there exist commutation relations which follow immediately from (1) by integration over the two regions and division by the product of their four-dimensional extensions. Thus, the value of the bracket symbols $\left[\mathscr{E}_x^{(')}, \mathscr{E}_x^{('\mathrm{I}'}\right], \ldots$ are obtained from (1) simply by replacing the quantities $A^{(12)}, B^{(12)}$ by their average values over the two regions

$$\begin{aligned} \bar{A}_{\mathrm{xx}}^{(\mathrm{I,II})} &= -\frac{1}{V_\mathrm{i} V_\mathrm{II} T_\mathrm{i} T_\mathrm{II}}\int_{T_\mathrm{I}} \mathrm{d}t_1 \int_{T_\mathrm{II}} \mathrm{d}t_2 \int_{V_1} \mathrm{d}v_1 \int_{V_\mathrm{II}} \mathrm{d}v_2 \left(\frac{\partial^2}{\partial x_1 \partial x_2} - \frac{1}{c^2}\frac{\partial^2}{\partial t_1 \partial t_2}\right)\left\{\frac{1}{r}\delta\left|t_2 - t_\mathrm{i} - \frac{r}{c}\right|\right\} \\ \bar{A}_{xy}^{(\mathrm{I,II})} &= -\frac{1}{V_\mathrm{I} V_\mathrm{II} T_1 T_\mathrm{II}}\int_{T_1} \mathrm{d}t_1 \int_{T_\mathrm{II}} \mathrm{d}t_2 \int_{V_1} \mathrm{d}v_1 \int_{V_\mathrm{II}} \mathrm{d}v_2 \frac{\partial^2}{\partial x_1 \partial y_2}\left\{\frac{1}{r}\delta\left(t_2 - t_1 - \frac{r}{c}\right)\right\} \\ \bar{B}_{xy}^{(\mathrm{III})} &= -\frac{1}{V_\mathrm{I} V_\mathrm{II} T_\mathrm{I} T_\mathrm{II}}\int_{T_1} \mathrm{d}t_1 \int_{T_\mathrm{II}} \mathrm{d}t_2 \int_{V_1} \mathrm{d}v_1 \int_{V_{11}} \mathrm{d}v_2 \frac{1}{c}\frac{\partial^2}{\partial t_1 \partial z_2}\left\{\frac{1}{r}\delta\left(t_2 - t_1 - \frac{r}{c}\right)\right\} \end{aligned} \tag{5}$$

In exactly the same way as the Heisenberg relation for two canonically conjugate mechanical quantities
(6) $\Delta p \Delta q \sim \hbar$,
which is the basis for the uncertainty principle, can be derived from the general quantum mechanical commutation relation
$[q, p] = \sqrt{-1}h$,
one obtains for the products of the complementary uncertainties of the field averages in question the following typical formulae:

$$\Delta\overline{\mathfrak{G}}_x^{(\mathrm{I})}\Delta\overline{\mathfrak{F}}_x^{(\mathrm{II})} \sim \hbar\left|\bar{A}_{xx}^{(\mathrm{I,II})} - \tilde{A}_{xx}^{(\mathrm{II,I})}\right|, \Delta\overline{\mathfrak{G}}_x^{(\mathrm{I})}\Delta\overline{\mathfrak{G}}_y^{(\mathrm{II})} \sim \hbar\left|\bar{A}_{xy}^{(\mathrm{I,II})} - \bar{A}_{xy}^{(\mathrm{II,I})}\right|$$
$$\Delta\overline{\mathfrak{F}}_x^{(\mathrm{I})}\Delta\overline{\mathfrak{G}}_x^{(\mathrm{II})} = 0, \qquad \Delta\overline{\mathfrak{G}}_x^{(\mathrm{I})}\Delta\overline{\mathfrak{G}}_y^{(\mathrm{II})} \sim \hbar\left|\bar{B}_{xy}^{(\mathrm{I,II})} - \bar{B}_{xy}^{(\mathrm{II,I})}\right|. \tag{8}$$

Several results of importance for our problem follow immediately from the expressions (5) and (8). Above all, we see that, in accord with the property of the δ-function expressed in (3), the quantities $\bar{A}^{(1,11)}, B^{(1,11)}$ change continuously as a result of a continuous displacement of the boundaries of regions I and II, as long as the extension of these regions, i.e. the values of V_1, T_2, V_2, T_2, remain different from zero. In particular, the differences $\bar{A}^{(\mathrm{I}\,,\,\mathrm{II}\,)} - \bar{A}^{(\mathrm{II},\,\mathrm{I})}$ and $\bar{B}^{(\mathrm{I},\,\mathrm{II}\,)} - \bar{B}^{(\mathrm{II},\,\mathrm{I})}$ vanish without discontinuity when the boundaries of the two regions gradually are made to coincide. From this it follows that the averages of all field components over the same spacetime region commute, and thus should be exactly measurable, independently of one another. In fact, this consequence of the theory, which goes essentially beyond the presupposition of unrestricted measurability of each single field quantity, appears as a special case of two more general theorems which follow from the symmetry properties of the quantities $\bar{A}^{(\mathrm{I,II})}$ and $\bar{B}^{(\mathrm{I,II})}$. For the fact that the expressions $A^{(12)} - A^{(21)}$ change their sign when the times t_1 and t_2 are interchanged, implies that the averages of two components of the same kind (i.e. two electric or two magnetic components) over two arbitrary space-time regions always commute if the associated time intervals coincide. Further, the corresponding antisymmetry of the expressions $B^{(12)}$ and $B^{(21)}$ with respect to interchange of the spatial points (x_1, y_1, z_1) and (x_2, y_2, z_2) implies that the averages of two components of different kind, e.g. $\mathscr{E}_x$ and $\mathfrak{S}_y$, over two arbitrary time intervals commute when the corresponding spatial regions coincide.

At first sight these results might seem incompatible with the commutation relations between averages of field quantities at one and the same time and over finite space regions, which can be derived from the Heisen-berg-Pauli representation of the formalism and are discussed in the book by Heisenberg previously cited. While it is stated there too that averages of components of the same kind commute, it is deduced that components of different kind over one and the same region of space do not commute. However, this contradiction is solved easily by noting that Heisenberg's
treatment involves a limiting process in which two originally noncoinciding space-time regions are brought into coincidence oniy after their temporal extension has been contracted to one and the same instant of time. For from the symmetry of the expression (2) for $B_{xy}^{(12)}$ with respect to t_1 and t_2, and from the property of the δ-function stated in (3), we find in the case of coinciding time intervals

$$\bar{B}_{xy}^{(1,1\mathrm{I})} - \bar{D}_{xy}^{(1\mathrm{I},1)} = \tfrac{2}{V_1 V_{\mathrm{II}} T^2} \cdot \tfrac{1}{c} \int_{V_1} \mathrm{d}v_1 \int_{V_{11}} \mathrm{d}v_2 \tfrac{\partial}{\partial z_1}\left(\tfrac{1}{r}\right), \tag{9}$$

where we have put $T_{\mathrm{I}} = T_{\mathrm{II}} = T$ and where the double integration is over all pairs of points, one in each of the spatial regions, whose separation r is smaller than cT. If we now further assume that the two spatial regions have the same volume, $V_{\mathrm{I}} = V_{\mathrm{II}} = V$, and the same shape, but are displaced relative to each other in the z-dinection, then in the limit where cT can be considered negligible compared with the linear extensions of the space regions, the space integral in (9) gives by partial integration $\pm 2\pi c^2 T^2 F$, where F is the area enclosed by the projection on the xy-plane of the curve in which the surfaces of V_{I} and V_{II} intersect, and where the sign is + or depending on whether region II is displaced relative to region I in the positive or the negative z-direction. Thus, if the regions are displaced continuously through each other the difference $\bar{B}_{xy}^{(\mathrm{I,II})} - \bar{B}_{xy}^{(\mathrm{II,I})}$ undergoes a discontinuous change of $8\pi cF/V^2$, while both expressions $\bar{B}_{xv}^{(\mathrm{I,II})}$ and $\bar{B}_{xy}^{(II,1)}$ change their sign. Therefore, the commutation relation between the instantaneous spatial averages of $\mathbb{E}_x$ and $\mathfrak{S}_y$ in the limiting case under discussion displays an essential ambiguity, which is responsible for the apparent contradiction mentioned above.

Furthermore, as we shall see, the supposed demonstration, on the basis of previous investi-

gations of the physical possibilities of measurement, that there is a complementary limitation on the measurability of field components of different kinds in one and same region of space, aiso depends entirely on the use of point charges as test bodies, which does not permit a sufficiently sharp delimitation of the region of measurement. As we have already emphasized, only measurements employing test bodies with a charge distribution of tinite extension should be considered for the testing of the quantum-electromagnetic formalism, since every well-defined statement of this formalism refers to averages of field components over finite space-time regions. Yet this circumstance in no way prevents us from testing by field measurements all unambiguous conclusions that can be drawn from the Heisenberg-Pauli representation concerning the time dependence of spatial field averages. For this purpose we need only introduce averaging regions whose temporal extension T, multiplied by c, is sufficiently small compared to their linear spatial dimensions, the order of magnitude of which we shall in the following always denote by L.

In fact, the case $L > cT$ is particularly suited for a thorough testing of the consequences of the formalism in the properly quantum-theoretical domain. Of course, aIready in the domain of vaiidity of ciassical theory the case $L \leqslant cT$ is of little interest, since all the peculiarities of the wave fields inside the volume V are smoothed out to a large extent by the averaging procedure, because of the propagation during the time interval T. In addition to this smoothing out, there are, in the quantum domain, the peculiar fluctuation phenomena which derive from the basically statistical character of the formalism. As we shall see shortly, these fluctuations, while essentially entering the solutions of problems in the case $L \leqslant ct$, play a comparatively small role in the case $L > cT$.

The fuctuations in question are intimately related to the impossibility, which is characteristic of the quantum theory of fields, of visualizing the concept of light quanta in terms of classical concepts. In particular, they give expression to the mutual exclusiveness of an accurate knowledge of the light quantum composition of an clectromagnetic field and of knowledge of the average value of any of its components in a well-defined spacetime region. Let the density $\omega_i(\kappa_x, \kappa_y, \kappa_z)$ of light quanta with definite polarization parameter i and given momentum and energy, $\hbar\kappa_x, \hbar\kappa_y, h\kappa_z$ and $\hbar v = \hbar c\sqrt{\kappa_x^2 + \kappa_y^2 + \kappa_z^2}$ be known; then the expectation value of all field averages are indeed zero, but the mean square fluctuation of each field quantity, such as $\mathbb{F}_x^{(G)}$ defined in (4), is given by the easily derivable formula

$$\left\{\begin{array}{l} S(G) = \frac{1}{V^2T^2} \cdot \frac{\hbar}{3} \int_T \mathrm{d}t_1 \int_T \mathrm{d}t_2 \int_V \mathrm{d}v_1 \int_V \mathrm{d}v_2 \frac{\partial^2}{\partial t_1 \partial t_2} \int_{-\infty}^{\infty} \left(\sum_i \omega_i + 1\right) \\ \cos\left[\kappa_x (x_1 - x_2) + \kappa_y (y_1 - y_2) + \kappa_z (z_1 - z_2) - v(t_1 - t_2)\right] \\ / \frac{\mathrm{d}\kappa_x \ \mathrm{d}\kappa_y \ \mathrm{d}\kappa_z}{v} \end{array}\right. \tag{10}$$

From formula (10) we see that for a given light quantum composition the fluctuations in question can never vanish, since even when $\omega_i = 0$, i.e., in the complete absence of light quanta, they assume a finite positive value, which by an easy calculation can be put in the form

$$S_0(G) = \frac{2}{3\pi^2} \frac{\hbar c}{V^2} \int_V \mathrm{d}v_1 \int_V \mathrm{d}v_2 \frac{1}{r^2\left[(cT)^2 - r^2\right]} \tag{11}$$

For every other light quantum distribution defined by a given density ω_i, the mean square fluctuation of the average of a field component becomes larger than $S_0(G)$. However, the fluctuations of a field average expected according to the formalism can be arbitrarily small when a direct knowledge of field quantities, obtained by measurement for example, is assumed. In such a case the light quantum density ω_i is obviously not well defined, and we must content ourselves with statistical statements about this density.

Furthermore, it is of decisive importance for the discussion of the measurement possibilities that the expression (11) holds not only for the field fluctuations in a region free of light quanta, but also represents the mean square fiuctuation of each fieid average in the more general case

where only classically describable current and charge distributions occur as sources of the field. The state of the field is then uniquely defined by the requirement that the expectation value of every field quantity coincide with the classicaliy computed vaiue, and that the numbers of light quanta of given momentum and polarization be distributed around their mean value n_0, estimated by means of the correspondence argument, according to the probability law valid for independent events

(12) $\quad w(n) = \frac{n_0^n e^{-n_o}}{n!}$

An easy calculation shows that the field fluctuations in this state are given just by the expression (11). Moreover, in correspondence with the characteristics of black-body fluctuations, it follows that also in the general case of a field of given light quantum composition, the inclusion of field effects of any classically describable sources will have no influence on the fluctuation phenomena.

The square root of the expression (11) may be regarded as a critical
field strength, $\mathfrak{S}$, in the sense that only when considering field averages essentially larger than $\mathfrak{G}$ are we allowed to neglect the corresponding fluctuations. To assess the possibilities of testing the formalism in the properly quantum domain, still another critical field size, $\mathfrak{U}$, is relevant, which equals the square root of the products, given by (8), of the complementary uncertainties of two field averages over space-time regions that only partially coincide, being displaced relative to each other by spatial and temporal distances of order of magnitude L and T, respectively. For when the field strengths are essentially larger than $\mathfrak{U}$ we obviously enter the domain of validity of classical electromagnetic theory, where all quantum mechanical features of the formalism lose their significance. A simple estimate based on formulae (8) and (11), shows that in the case $L \leqslant cT$ both critical expressions $\mathfrak{U}$ and $\mathfrak{S}$ are of the same order of magnitude

$$\mathfrak{u} \sim \mathfrak{S} \sim \frac{\sqrt{\hbar c}}{L \cdot cT} \tag{13}$$

On the other hand, in the case $L > cT$ one has

$$\mathcal{U} \sim \sqrt{\frac{\hbar}{L^3 T}} \text{ and } \mathbb{S} \sim \frac{\sqrt{\hbar c}}{L^2} \tag{14}$$

so that in the limiting case $L \gg cT$ the critical field strength $\mathfrak{U}$ is much larger than $\mathfrak{S}$ and, therefore, in testing the characteristic consequences of the formalism we can to a large extent disregard the field fluctuations.

Before we turn to the comparison of the consequences of the quantum electromagnetic formalism discussed in this section, with the physical measurement possibilities for field quantities, we want to emphasize here once again that the consistent interpretability of this formalism is in no way endangered by such paradoxical features of its mathematical representation as the infinite zero-point energy. In particular, this latter paradox, which moreover can be removed by a formal change in the representation [6] that does not influence the physical interpretation, has no direct connection with the problem of measurability of field quantities. In fact, a field-theoretic determination of the electromagnetic energy in a given space-time domain would require knowledge of the values of the field components at each space-time point of a region, which are inaccessible to measurement. A physical measurement of the field energy can be carried out only by means of a suitable mechanical device that would
make it possible to separate the electromagnetic fields in a given region from the rest of the field, so that the energy contained in the region could be measured subsequently by application of the conservation law. However, because of the interaction with the measuring mechanism, any such separation of the fields would be accompanied by an uncontrollable change in the field energy in the region in question, the consideration of which is essential for clarification

of the well-known paradoxes that arise in the discussion of energy fluctuations in black-body radiation. [7]

27.3.3 3. Presuppositions for Physical Field Measurements

The measurement of electromagnetic field quantities rests by definition on the transfer of momentum to suitable electric or magnetic test bodies situated in the field. Quite apart from the caution required by quantum theory in appiying the customary idealization of field components defined in each space-time point, we are here always concerned with averages of these components over the finite time intervals necessary for the momentum transfer as well as over the spatial domains in which the electric charges or magnetic pole strengths of the test bodies in question are distributed. Obviously, even the assumption of a uniform charge distribution on a test body is an idealization, subject to a certain restriction because of the atomic constitution of all material bodies, but indispensable for the unambiguous definition of field quantities.

In order to have a definite case in mind we consider the measurement of the average of the electrical field component in the x-direction, $\mathfrak{E}_x$, over a space-time domain of volume V and duration T. For this purpose we therefore use a test body whose electric charge is uniformly distributed over the volume V with a density ρ, and determine the values p'_x and p''_x of this body's momentum components in the x-direction at the beginning t' and at the end t'' of the interval T. The average $\mathbb{E}_x$ we are looking for is then determined by the equation

$$(15) \qquad p''_x - p'_x = \rho \mathbb{E}_x V T,$$

where it is assumed that the time intervals required for the momentum measurements, whose order of magnitude we shall denote by Δt, can be regarded as negligibly small compared to T, and that we can disregard the displacements suffered by the test body due to the momentum measurements as well as the acceleration given to it during the time interval T by the field that is being measured, in comparison with the linear dimensions L of the spatial domain V.

By choosing a sufficiently heavy test body we can obviously make its acceleration due to the field arbitrarily small. In the momentum measurements, however, we encounter conditions which are independent of the mass of the test body. As a consequence of the indeterminacy principle, any measurement of the momentum component $\tilde{p}_x$ carried out with the accuracy Δp_x is accompanied by a loss Δx in the knowledge of the position of the body in question, the order of magnitude of which is given by the relation contained in (6)

$$(16) \qquad \Delta p_x \Delta x \sim \hbar.$$

Nevertheless, in itself this state of affairs does not imply any restriction on the accuracy to be achieved by the field measurement, because we still have at our disposal the value of the charge density. In fact, if we neglect Δt and Δx in comparison with T and L, we get from (15) and (16) for the order of magnitude of the accuracy $\Delta \dot{\mathbb{E}}_x$ of the field measurement

$$\Delta \bar{\tilde{\boldsymbol{r}}}_x \sim \frac{\hbar}{\rho \Delta x \cdot VT}, \tag{17}$$

which for any value of Δx, however small, can be made arbitrarily small by choosing a sufficiently large value of ρ.

Strictly speaking, the accuracy of the fieid measurement is also dependent on the absolute magnitude of the value of $\mathbb{F}_x$ itself, for with given ranges of Δt and Δx the value of $\mathbb{E}_\lambda$ ascertained from (15), even if Δp_x were zero, would be affected with an uncertainty arising from the latitude in the delineation of the domain of measurement which would surpass any limit as $\mathbb{C}_\lambda$ increases indefinitely. Yet, the latter circumstance merely reflects the general limitation on all physical measurements, for which a knowledge of the order of magnitude of the expected

effects is always required in order to choose the appropriate measuring instruments. In our problem an upper limit to the effects that we are interested in is set by the fact that as the magnitude of the field components increases we gradually reach the domain of validity of classical electromagnetic theory. As mentioned in the previous section, in the case $L > cT$, which is particularly suited for testing the quantum electromagnetic formalism, the expression

$$\mathrm{Q} = \sqrt{\frac{\hbar}{VT}},$$

which is equivalent to the right-hand side of the first formula (14), represents a critical field size in this respect. Substituting this into (17), the latier relation assumes the form
(19)

$$\Delta \mathbb{E}_x \sim \lambda Q$$

where

$$\lambda = \frac{Q}{\rho \Delta x} \tag{20}$$

is a dimensionless factor determining the accuracy of the field measurement.

The requirement that λ be small compared to unity and simultaneously Δx be small compared to L means that the total clectric charge of the test body must consist of a large number of elementary charges ε. In fact, according to (20) this number is given by

$$N = \frac{\rho V}{\varepsilon} = \frac{QV}{\lambda \varepsilon \Delta x} = \frac{1}{\lambda} \cdot \frac{L}{\Delta x} \cdot \sqrt{\frac{L}{cT}} \cdot \sqrt{\frac{\hbar c}{\varepsilon^2}} \tag{21}$$

and is very large when the above requirements are fulfilled and when $L > cT$ as assumed. The last factor is of course the reciprocal square root of the fine-structure constant whose smallness, as we already mentioned in the Introduction, is an essential presupposition for the correspondence approach to electron theory. As emphasized there, essential restrictions are imposed on a field measurement with an elementary charge as a test body, a fact which is also directly visible from (21) if one puts $N = 1$.[8] Moreover, the assumption of a large value of N is a necessary condition for the physical realization of a uniform distribution of the charge of the test body over the volume V; and as long as the linear dimensions of the test body are large compared to the atomic dimensions, its fulfillment obviously presents no difficulties in principle. It need hardly be mentioned that with this presupposition the assumption used above about the mass of the test body, equivalent to the requirement that this mass be very large compared to that of a light quantum of wave length L, always can be satisfied.

Thus far we have completely disregarded the electromagnetic field effects which accompany the acceleration of any test body during the momentum measurement. These effects superpose themselves on the original field and must be included in the field averages defined by equations of type (15). Hence, the main task of the following investigation will be to find a measuring arrangement in which the field effects of the test bodies can be controlled or compensated to the largest possible extent. Yet here we must first of all discuss the question of whether the reaction of the radiation fields produced by the acceleration of the test body in the momentum measurements could impair even the practicability of measuring the values occurring in (15) of the test body's momentum components at the beginning and end of the measuring interval It was just this possibility that led Landau and Peierls, in the work cited at the beginning, to doubt the reliability of the indeterminacy relation (16) for charged bodies and to conclude that it should be replaced by another even more restrictive relation in which the charge of the test body enters in an essential way. However, they likened the electromagnetic behavior of such a body to that of a point charge e, and consequently used the following expression for estimating

the order of magnitude of the test body's momentum changc, brought about by radiation recoil, during the time $4t$

(22) $\quad \delta_e p_x \sim \frac{e^2}{c^3}\frac{\Delta x}{\Delta t^2}$.

If, however, $\delta_e p_x$ is considered an additional indeterminacy of the momentum measurement, then if one puts $\rho V = e$ and does not distinguish between $\mathbb{E}_x$ and $\mathbb{E}_x$, one gets instead of (17)

$$\Delta_e \mathfrak{F}_x \sim \frac{\hbar}{eT\Delta x} + \frac{e\Delta x}{c^3 T\Delta t^2}, \tag{23}$$

whose minimum under variation of ε is obviously given by

$$\Delta_m \mathfrak{E}_x \sim \frac{\sqrt{hc}}{c^2 T\Delta t}. \tag{24}$$

If, still following Landau and Peierls, one does not distinguish between T and Δt, this expression agrees with the absolute limit on the measurability of field components that they gave, on which they based their criticism of the foundations of the quantum electromagnetic formalism.

However, the supposed difficulties of the momentum measurement disappear as soon as sufficient account is taken of the finite extension of the test body's electric charge. Using the idealization of a uniform, rigidiy displaceable charge distribution, to be more closely examined below, the electric field strengths in the region V during the acceleration of the test body within the time Δt can at most reach a value of the order of magnitude $\rho\Delta x$; since, according to Maxwell's equations, their time derivatives are at most of the same order of magnitude as that of the current density, given by $\rho(\Delta x/\Delta t)$. Hence, any electromagnetic reaction on the body during the measuring interval Δt can only contribute a momentum transfer of the order of magnitude

(25) $\quad \delta_\rho p_x \sim \rho^2 V\Delta x\Delta t$.

Thus, in view of (18) and (20), we get by comparison of (16) and (25)

$$\delta_\rho p_x \sim \Delta p_x \cdot \lambda^{-2}\frac{\Delta t}{T}, \tag{26}$$

which implies that for any desired accuracy of the field measurement, symbolized by a given value of λ, the influence of the electromagnetic reaction on the momentum measurement of the test body can be neglected if only $4t$ is chosen sufficiently small in comparison with T. It is precisely this circumstance that is decisive for assessing the accuracy of the field measurements; for it turns out to be impossible to directly take into account the influence of the radiation reaction on the momentum and energy balance in the individual momentum measurements. For example, Pauli's proposal [9] to measure subsequently by means of a special device the momentum and energy contained in the emitted radiation would already be impracticable because of the fact that, at least in the case $L > cT$ which is of particular importance for field measurements, the radiation fields that are produced in the momentum measurements at the beginning and at the end of the interval T cannot be separated from each other to the degree sufficient for this purpose. In fact, in the following sections we shall show quite generally that any attempt at such a control of the test body's field effects would essentially impair the realization of the field measurement in question.

Besides, not only for discussing the behavior of an individual test body during the measurement but also for assessing the mutual influence of
several test bodies, it is essential to treat these not as point charges but as continuous charge distributions. This is because the customary identification of the position indeterminacy of a test body, considered as a point charge, with the linear dimensions of the domain of measurement is an arbitrary assumption that is foreign to the measurability problem. For this reason.

not only do the estimates of the product of the uncertainties of $\mathfrak{F}_x$ and $\mathfrak{S}_y$ inside the same space-time domain, obtained by Heisenberg and by Landau and Peierls by considering point charges, deviate from the predictions of the quantum-electromagnetic formalism as already mentioned; they are in agreement with each other only in the special case $L \sim cT$. In this case, both estimates give the expression Q^2, which corresponds to the order of magnitude, to be expected from the formalism, of the value of the product of the complementary indeterminacies of two field averages in space-time regions that are displaced relative to each other through space-time distances of the same order of magnitude as L and T. Moreover, it is an essential feature of the formalism that the product in question vanishes identically for coinciding regions. The physical meaning of this result becomes obvious as soon as one takes into account the uniform charge distribution of the test body used to measure $\mathbb{F}_x$; since the magnetic field strength which is produced at a point P_2 of the volume V by the displacement of the charge ρdv contained in a volume element situated at the point P_1 is exactly equal and opposite to the magnetic field strength produced at the point P_1 by the same displacement of the charge ρdv at the point P_2, so that the average over the volume V of every magnetic field component produced by the displacement of the test body disappears.

From the foregoing it emerges that in the investigation of the measureability of field quantities it is decisively important to assume that the test bodies to be used behave like uniformly charged rigid bodies whose momenta can be measured, in any given arbitrarily small time interval, with an accuracy, expressed by (16), complementary to the accompanying uncontrollable displacement. Of course, in view of the finite propagation of all forces, we should not think here of the usual mechanical idealization of rigid bodies, but must think of every test body as a system of individual components of sufficiently small dimensions; and think of the measurement of the total momentum of this system as carried out in such a way that, to a sufficient approximation, all the components undergo the same
displacement during the momentum measurement. That this requirement can be fulfilled without difficulties of principle, at least insofar as one can disregard the atomic constitution of the test body is due to the fact that the required momentum measurements can be fully described on a classical basis, irrespective of whether they depend on looking at a collision process between the test body and a suitable material colliding body; or, say, on the study of the Doppler effect involved in the reflection of radiation from the test body. For, if only the mass of the colliding body is sufficiently large or if the packet of radiation that is used to measure the Doppler effect contains a sufficient number of light quanta, then the interaction between the test body and the coiliding body can be described classically to any approximation. In fact, the loss of knowledge of the position of the test body, which accompanies the momentum measurement, is due solely to the impossibility of simultaneously fixing the course of the collision process relative to a weil-defined space-time reference frame. Indeed, the peculiar complementarity of the mode of description ultimately derives from the fact that any such fixation is bound up with an unavoidable, and in principle uncontrollable, transfer of energy and momentum to the scales and clocks needed to establish the co-ordinate system. [10]

We recall that, according to the indeterminacy principle, the latitude in the time Δt that is left open in any description and the accuracy with which the energy exchanged in the collision process between colliding body and test body is known are connected by the well-known relation
(27) $\Delta E \cdot \Delta t \sim \hbar$.

Because of the relation between energy and momentum and velocity components
(28) $\quad \mathrm{d}E = v_x \, \mathrm{d}p_x$
which is valid for both bodies, it follows directly that
(29) $\quad \Delta p_x \, |v_x'' - v_x'| \, \Delta t \sim \hbar$.

Even though, as noted above, the change of velocity $|v_x'' - v_x'|$ of the test body in the momentum measurement can be considered as arbitrarily well known for a sufficiently heavy

test body, the factor
(30) $|v''_x - v'_x|\,\Delta t = \Delta x$
obviously implies a completely free latitude in the position of the body relative to the fixed frame of reference, in complete agreement with the indeterminacy relation (10). From (30) the condition
(31) $\quad \Delta x < c\Delta t,$
follows immediately, which, because of (16), imposes an absolute limit on the accuracy Δp_x that can be achieved in a momentum measurement with a given upper limit for the time latitude At. However, in view of the relativistic invariance of the relations (16) and (27) and in particular of formula (28), this circumstance implies no restriction in the formulation and applicability of the indeterminacy principle. In our problem it is even permissible to disregard all mechanical relativistic effects, for by using sufficiently heavy test bodies we can always arrange that the velocities of all test bodies during the whole measurement process remain small compared to the velocity of light. Consequentiy, we can even consider any displacement Δx in the momentum measurements very small compared to the corresponding value of $c\Delta t$ which itself must be chosen arbitrarily small.

It is exactly the possibility of accurately tracing the relative space-time course of the proccss scring as momentum measurement that enables us to measure the total momentum of an extended body within any given time interval with the required accuracy expressed by (16). Thus, we can determine the total momentum of the system of charged material component bodies serving as test body by a single collision process if we make use of a colliding body of special construction which intervenes everywhere in the test body system and gives every component the same acceleration at the same time. It is true that this device imposes severe demands on the construction of the colliding and test bodies, but these demands do not present any difficulties of principle as long as we can disregard the atomic constitution of the bodies. The measurement of the total momentum of the test body would presumably be performed most simply by optical means, i.e. by determination of the Doppler effect; for this purpose one might proceed as follows: imagine that every component body is equipped with a small mirror at right angles to the x-direction, and that a number of other mirrors are placed in fixed positions in such a way that the light path from the radiation source to each component body is the same. If now by means of a suitable device we produce a packet
of radiation of duration Δt and containing a number of light quanta sufficiently large compared to the number of component bodies, then all these bodies will suffer a coilision simuitaneousiy and undergo an acceleration which for all component bodies can be made equal with arbitrary accuracy.

In order to show that one can in fact measure the total momentum of the test body with an accuracy satisfying relation (16) by means of such an arrangement, we shall consider somewhat more closely the interaction between the test body system and the packet of radiation. In view of the assumed smallness of the velocity of the test body compared to the velocity of light. we have for each component body

$$\begin{cases} m_\tau \left(v''_{\tau,x} - v'_{\tau,x}\right) = \frac{\hbar}{c} \sum_{\bar{n}_\tau} (v' + v'') \\ \frac{1}{2} m_\tau \left(v''^2_{\tau,x} - v'^2_{\tau,x}\right) = \hbar \sum_{n_\tau} (v' - v'') \end{cases} \tag{32}$$

where m_τ denotes the mass of a component body, $v'_{\tau,x}, v''_{\tau,x}$ are its velocity before and after the reflection, and where the summation extends over the n_τ light quanta reflected from the component body whose frequency (reciprocal period times 2π) before and after the reflection are denoted by v' and v'', respectively. It follows from (32) that the momentum of the component body in question before and after the collision is

$$\left.\begin{matrix} p'_{\tau,x} = m_\tau v'_{\tau,x} = \\ p''_{\tau,x} = m_\tau v''_{\tau,x} = \end{matrix}\right\} m_\tau c \sum_{n_\tau}^{\sum_{n_\tau}(v'-v'')} -\frac{1}{2}\frac{\hbar}{c}\sum_{n_\tau}(v'+v'') \tag{33}$$

If we now assume that the mean spectral frequency v_0 of the radiation packet is very large compared to the mean width $(\Delta t)^{-1}$ of its frequency distribution as well as to all frequency changes $v' - v''$, then we can take the change of velocity of the component body in the collision, to a sufficient approximation, as

$$v''_{\tau,x} - v'_{\tau,x} = \frac{\hbar}{m_\tau c}\sum_{n_\tau}(v'+v'') = \frac{2n_\tau \hbar v_0}{m_\tau c} \tag{34}$$

and we can assume that it is the same for all component bodies. Thus, in the collision all component bodies suffer displacements which, although
uncontrollable, are arbitrarily close to being identical and whose order of magnitude Δx satisfies relation (30) where $|v''_x - v'_x|$ is to be identified with the common velocity change of the whole test body system Consequently, since according to our assumptions Δx can be considered negligibly small compared to $c\Delta t$, we get from (33) and (34), for the product of Δx and the uncertainty of the total momentum of the test body, approximately

$$\Delta p_x \Delta x \sim \Delta t \cdot \Delta\left(\sum_\tau \sum_{n_\tau} \hbar v' - \sum_\tau \sum_{n_\tau} \hbar v''\right) \tag{35}$$

The quantities in the bracket in (35) are precisely the total energies of the radiation packets impinging on and reflected from the test body. The energy of the latter packet can be measured with arbitrary accuracy, e.g. by spectral analysis of the reflected radiation. For the incoming radiation packet, however, such an analysis would obviously be incompatible with the experimental conditions. Yet the total energy of this radiation can be measured with an accuracy that is complementary to Δt, as given by (27). To do that it suffices to use a purely mechanical device by means of which the packet in question is separated from a radiation field, whose energy beforc and after the separation can be determined with arbitrary accuracy, e.g. by spectral measurements. Thus, the relation (35) is identical with the usual indeterminacy relation (16). Note further that the demonstration of this identity is essentially dependent on the fact that in accordance with the described arrangement we obtain no information about the momentum of the single component bodies but only about the total momentum of the test body.

The fact that the test body system suffers a common translation during the required momentum measurements is not only important for the calculation of the field effects of the test body which accompany these measurements, but also gives us the possibility to arrange things in such a way that outside the short time intervals occupied by the momentum measurements all the test bodies employed in the field measurement can be considered as being at rest, which greatly simplifies the calculation. For immediately after each momentum measurement, i.e. practically speaking still inside the interval Δt, we can give the test body system a second push in the opposite direction by means of a suitable device, such that the velocity change which every component body suffered in the first collision is cancelled out; this can be done with an arbitrary accuracy, i.e.
an accuracy that is inversely proportional to the mass of the component body, and without losing the desired knowledge of the total momentum of the iest body. However, with this arrangement it is impossible to know the time interval between the two collision processes with a latitude smaller than Δt, and so, as required by the indeterminacy principle, the test body is not returned to its original position by the counter-collision, but rather is brought to rest to the required approximation at an unknown position, displaced by a distance of the order Δx.

To assess the complementary limitations on the measurability of field quantities, which will be more closely investigated in the following sections, we must foilow the behavior of the test body as accurately as possible during the whole measuring process. It turns out that for this purpose it is necessary first of all to know accurately the position of each test body at all times before and after its use in the measurement. This is achieved most expediently by having the test body firmly attached to a rigid frame serving as a spatial reference system, except in the time interval during which the momentum transfer to the test body from the field is to be determined. At the beginning of this interval the attachment must be disconnected, and the momentum component of the test body in the direction of the field component that is to be determined must be measured. We always assume that by an immediately following counterimpulse, as discussed above, the body is brought back to rest with an accuracy inversely proportional to its mass, at a position which is not accurately predictable. At the cad of the time interval and after renewed measurement of the momentum component in question, the firm attachment is re-established; here it turns out to be not unessential that the test body be brought back into exactly the same position as it had originally. If the space-time averaging domains are to be sufficiently sharply defined, these prescriptions alone impose far-reaching demands on the detailed construction of the test body system. For due to the retardation of all forces it is strictly speaking necessary that the severance as well as the re-establishment of the attachment of the test body system to the fixed frame are performed in such a way that all its independent component bodies, whose linear dimensions must be at least as small as the smallest relevant value of $c\Delta t$, are unfastened and fastened simultaneously, i.e. within the time latitude Δt of the momentum measurement, which itself must be chosen sufficiently small compared to the time interval T.

Still more far-reaching demands on idealization with respect to the construction and handling of the test body system are obviously needed to measure field averages over two partialiy overlapping space-time regions. For in this case we must have test bodies at our disposal which can be displaced inside each other without mutual mechanical influence. In order that the electromagnetic field to be measured be disturbed as little as possible by the presence of the test body system, we shall imagine, moreover, that every electric or magnetic component body is placed adjacent to a neutralization body with exactly the opposite charge. In the case of a magnetic test body system it is to be noted that a uniform pole strength distribution cannot exist on a strictiy deilmited body. However, one can imagine, at least in principle, that every component body of such a system is connected with the corresponding neutralization body by magnetizable flexible threads. All these neutralization bodies are to remain connected with the fixed frame during the whole measurement process without mechanically influencing the free mobility of the component bodies belonging to the test body system proper. Of course, the idealizations entailed in such presuppositions, as well as in the still needed compensation mechanisms to be introduced below, are justifiable only as long as we can neglect the atomic constitution of the test body. However, as already mentioned, this neglect does not imply any restrictions in principle on the possibility of testing the quantum electromagnetic formalism, since no universal space-time dimensions appear in this formalism. Accordingly, the purpose of the preceding considerations was above all to show that in the purely mechanical problems which are relevant to the field measurements, it is possible to distinguish strictly between the restrictions on the constitution of the test body stemming from the atomic structure of matter and the restrictions on the handling of these bodies that are due to the quantum of action, formulated in particular in the principle of indeterminacy.

27.3.4 4. Calculation of the Field Effects of the Test Body

After having investigated the physical presuppositions for the constitution of the test body we now turn to a closer consideration of the electromagnetic field effects of the test body which accompany the measurement of field quantities and which are of decisive importance for the measur-
ability question. In accordance with the discussion above we shall treat each test body as a charge distribution which uniformly fills the spatial averaging domain and which undergoes a simple transiation during the momentum measurement. We shall first carry out the calculation of the electromagnetic fields thereby produced on the basis of classical electrodynamics, and only afterwards discuss the restriction on the validity of this treatment due to the quantum of action.

Let us consider two space-time regions, I and II, with volumes V_1 and V_{II} and durations T_1 and T_{II}, and let us ask for the electromagnetic field 'which is produced at a point (x_2, y_2, z_2, t_2) of region II by a measurement of the average of $\boldsymbol{E}_x$ over the region I. Thus, we assume that in volume $\bar{V}_1$ there are originally two electric charge distributions with the constant densities $+\rho_{!}$and $-\rho_{!}$. In the interval from $t'_{!}$ to $t'_1 + \Delta t_1$ the first charge distribution experiences a simple non-uniform translation in the x direction through a distance $D_x^{(1)}$; in the interval from $t'_1 + \Delta t_1$ to t''_1 it remains at rest at the displaced position; finally, in the interval from t''_1 to $t''_{\mathrm{i}} + \Lambda t_{\mathrm{i}}$ it moves non-uniformly parallel to the x-axis back to its original position, which coincides with that of the neutralization distribution. In accordance with the requirement discussed in the preceding sections, we assume further that Δt_1 is very small compared io $T_1 = i''_1 - i'_1$ and that $D_x^{(1)}$ is very small not only compared to the linear dimensions of the spatial averaging region of volume V_{l}, but also small compared with $c\Delta t_{\mathrm{l}}$.

Hence, in the limiting case of vanishingly small Δt_{l}, the sources of the fieid that we are iooking for may be represented as a poiarization in the x-direction of constant density, $P_x^{(1)} = \rho_1 D_x^{(1)}$, existing in the region I during the time interval from t'_1 to t''_1, as well as a current density present only in the immediate vicinity of the times t'_1 and t''_1, which we can write as

(36) $\quad J_x^{(\mathrm{I})} = \rho_1 D_x^{(\mathrm{I})} \left[\delta\left(t - t'_1\right) - \delta\left(t - t''_1\right)\right],$

using δ symbol defined by formula (3). By means of the same symbol we can similarly express the polarization at an arbitrary time t by the formula

$$P_x^{(1)} = \rho_1 D_x^{(1)} \int_{t_i}^{t''_i} \delta\left(t - t_1\right) \mathrm{d}t_1. \tag{37}$$

As is well-known, the components of the fields at the space time point
$(\ x_2, y_2, z_2, t_2\ )$ produced by these sources may be calculated from the formulae

$$\begin{cases} F_x^{(\mathrm{I})} = -\frac{\partial \varphi^{(\mathrm{I})}}{\partial x_2} - \frac{1}{c}\frac{\partial \psi_x^{(\mathrm{I})}}{\partial t_2}, & E_y^{(\mathrm{I})} = -\frac{\partial \varphi^{(\mathrm{I})}}{\partial y_2}, E_z^{(\mathrm{I})} = -\frac{\partial \varphi^{(\mathrm{I})}}{\partial z_2} \quad H_z^{(\mathrm{I})} = -\dfrac{\partial \psi_x^{(\mathrm{i})}}{\partial y_2}, \\ H_x^{(\mathrm{I})} = 0, & H_y^{(\mathrm{I})} = \frac{\partial \psi_x^{(\mathrm{I})}}{\partial z_2}, \end{cases} \tag{38}$$

where we have used latin letters to distinguish these fields from the field components that are to be measured. In (38), $\varphi^{(1)}$ signifies the retarded scalar potential

$$\varphi^{(1)} = \int_{V_1} \frac{\partial}{\partial x_1} \left[\frac{P_x^{(1)}\left(t_2 - r/c\right)}{r}\right] \mathrm{d}v_1 \tag{39}$$

and $\psi_x^{(1)}$ the retarded vector potential component

$$\psi_x^{(1)} = \frac{1}{c} \int_{V_{\mathrm{i}}} \frac{J_x^{(1)}\left(t_2 - r/c\right)}{r}\, \mathrm{d}v_{\mathrm{i}} \tag{40}$$

where r is the distance between the space points (x_1, y_1, z_1) and (x_2, y_2, z_2). Noting that the expression (36) can also be written in the form

$$J_x^{(1)} = -\rho_1 D_x^{(1)} \int_{t_1'}^{t_1'} \frac{\partial}{\partial t_1'} \delta(t - t_1)\, \mathrm{d}t_1 \tag{41}$$

and taking into account (37) and (41) one sees that the field components given by (38), (39) and (40) can be expressed by the typical formulae

$$\begin{cases} E_x^{(\mathrm{I})} = \rho_1 D_x^{(\mathrm{I})} \int_{V_1} \mathrm{d}v_1 \int_{T_1} \mathrm{d}t_1 A_{xx}^{(12)}, E_y^{(\mathrm{I})} = \rho_1 D_x^{(\mathrm{I})} \int_{V_1} \mathrm{d}v_1 \int_{T_1} \mathrm{d}t_1 A_{xy}^{(12)} \\ H_x^{(\mathrm{I})} = 0, \qquad H_y^{(\mathrm{I})} = \rho_1 D_x^{(\mathrm{I})} \int_{V_1} \mathrm{d}v_1 \int_{T_1} \mathrm{d}t_1 B_{xy}^{(12)} \end{cases} \tag{42}$$

where the abbreviations defined in (2) have been used.

In view of the properties of the symbolic δ-function it is easy to see that the field components given by (42) always remain finite and even cannot surpass a value of the order of magnitude $\rho_1 \bar{D}_x^{(\mathbf{t})}$ at any space-time point $(\ x_2, y_2, z_2, t_2\ )$. As already mentioned, the electromagnetic forces which occur during the momentum measurement of the test body in the time interval Δt are just of this order of magnitude (cf. p. 372). The fact that the field intensities do not subsequently increase essentially is solely a consequence of the counter collision taking place right after the momentum measurement which brings the body back to rest, and finds its idealized mathematical expressions in (36) and (37).

The averages of these field components over the region II, which are of particular intercst to us, arc obtained from (42) by a simple space-time integration and, in accordance with (5), are given by the formulae

$$\begin{cases} \bar{E}_x^{(\mathrm{I,II})} = D_x^{(\mathrm{I})} \rho_1 V_1 T_1 \bar{A}_{xx}^{(\mathrm{I,II})}, & \bar{E}_y^{(\mathrm{I,II})} = D_x^{(\mathrm{I})} \rho_1 V_1 T_1 \bar{A}_{xy}^{(\mathrm{I,II})} \\ \bar{H}_x^{(\mathrm{I,II})} = 0, & \bar{H}_y^{(\mathrm{I,II})} = D_x^{(\mathrm{I})} \rho_1 V_1 T_1 \bar{B}_{xy}^{(\mathrm{I,II})}. \end{cases} \tag{43}$$

As a result of the properties of the expressions $\bar{A}$ and $\bar{B}$, already discussed in Section 2, we see that for a given value of $D_x^{(1)}$ the field averages given by (43) are well-defined continuous functions of the regions I and II. Hence, for decreasing latitudes, Δt and Δx, of the duration of the momentum measurements and of the accompanying unpredictable displacements, these field averages are completely independent of the detailed space-time course of the coilision process, and simply proportional to the constant displacement of the test body in the measuring interval T_1. As we shall see, this very fact turns out to be decisive for the possibility of an extensive compensation of the uncontrollable field effects of the test bodies.

Thus far, the calculation of the field effects has been carried out on a purely classical basis. Yet for a more detailed comparison of the measurement possibilities and the requirements of the quantum-electromagnetic formalism one must also take into account the limitation imposed on the classical mode of calculation by the quantum-theoretical features of any field effect, symbolized by the concept of light quanta. In order to get a general view of the situation we assume that the averaging regions in question are of the same order of magnitude and spatially displaced relative to each other through distances of the same order of magnitude
as their linear dimensions, which we denote by L; and that further the corresponding time intervals of order of magnitude T are smaller than L/c. Under these conditions, the spectral decomposition of the field effects contains essentially only waves of wave length of the same order of magnitude as L. Since, furthermore, in the case under consideration the intensity of the field produced in the momentum measurement is of the order $\rho \Delta x$, and consequently the field energy contained in the volume V is of the order $\rho^2 \Delta x^2 V$, then the number of light quanta in question is approximated by the expression

$$n \sim \rho^2 \Delta x^2 V \frac{L}{\hbar c} = \lambda^{-2} \frac{L}{cT}, \tag{44}$$

where λ is the factor, defined in (20), that provides the measure for the accuracy of the measurement. Thus we see that in our case n is always large compared to unity if an accuracy of measurement is required that permits field strengths to be measured which are smaller than the critical field quantity $\underline{Q}$.

Evidently, the classically calculated expressions (42) and (43) for the field effects become relatively more exact, the greater the accuracy aimed di for the field measurements. However, it is essential to note that the absolute accuracy of these expressions does not change for increasing values of n. For in our case the statistical range of fluctuation of the field averages is approximately given by

$$\frac{\rho \Delta x}{\sqrt{n}} \sim \sqrt{\frac{\hbar c}{VL}} \sim \frac{\sqrt{\hbar c}}{L^2}.$$

This expression for the range of fluctuations of the field effects of the test body, which depends only on the linear dimensions of the measurement domain and which always remains finite, agrees in fact with the expression (14) for the order of magnitude of the pure black-body fluctuations which was derived from the formalism in the case $L > cT$. Actually, in the above consideration we are dealing merely with an example of the general relation, mentioned in Section 2, between black-body fluctuations and the deviations, only describable statistically, of field averages from field quantities that are calculated according to classical theory from specification of the sources. Furthermore, as was already there pointed out, in the case $L > cT$, especially important for testing the formalism, the black-body
fluctuations are always smaller than the field strength Q which is a measure of the complementary measurability of field quantities; and, indeed, so much the smaller, the larger the ratio between L and cT. Thus, in the following comparison between field measurements and formalism we shall always start from the classically calculated expressions (43), and only afterwards discuss the significance of the fluctuation phenomena for the consistency of the formalism.

27.3.5 5. Measurement of Single Field Averages

By definition we base the investigation of the measurement possibilities for field averages on equation (15) which expresses the classically described momentum balance for a test body situated in the field. According to the preceding arguments, each field component, such as $\mathfrak{E}_x$, is in this context to be regarded as the superposition of the fields originating from all field sources, including the test body itself, and the core of the measurement problem is precisely the question of the extent to which these fields can be associated with the various sources. However, we must emphasize here immediately that the strict applicability of the classical field concept in defining field averages is not in itself impaired by the previously discussed limited validity of the classical description of the field effects of the test body. Quite apart from the question of the accuracy attainable in the momentum measurements of the test body at the beginning and end of the measuring interval, which was discussed in Section 3, the unambiguous character of this definition would itself require that the masses of the test bodies be chosen sufficiently large that any modifications of the electromagnetic fields, stemming from their accelerations under the influcnce of these fields during the measuring interval, may be neglected. If one were inclined to regard this neglect as in contradiction with the atomic character of the momentum transfer between electromagnetic wave fields and material bodies, then it must be recalled that in the measurement problem under consideration there is no question of tracing well-defined elementary processes in the sense of the light quantum concept. In particular, in the measuring

arrangement described, an uncontrollable amount of momentum is absorbed by the rigid frame to which every test body is attached before and after the measuring interval. In the limiting case of a classically describable interaction between an electro-
magnetic wave train and a sufficiently heavy charged body, the momentum transfer just mentioned wouid obviousiy exactiy compensate the momentum absorbed by the test body in the measuring interval

As a preparation for the general discussion of the measurement problem, we first consider a single field measurement and, as in Section 3, ask for the average value of $\mathscr{E}_x$ in a certain space-time domain which we denote, as in the previous sections, by I. Thus, from the fundamental equation (15), we get for the momentum balance of the test body

$$p_x^{(1)''} - p_x^{(1)'} = \rho_1 V_1 T_1 \left(\mathbb{E}_x^{(1)} + \bar{E}_x^{(1,1)} \right), \tag{45}$$

where $\mathbb{E}_x^{(1)}$ represents the part of the average of $\mathbb{E}_x$ which would be present in the space-time domain I under consideration if no momentum measurement were made on the test body at time t', while $\bar{E}_x^{(1,1)}$ is the part of the field average that arises from this measurement, whose classicaliy estimated expression is given by (43), if regions I and II are set equal.

According to the arguments of Section 3, the sum of the field averages $\mathbb{E}_x^{(1)}$ and $\bar{E}_x^{(1,1)}$ appearing in (45) can be determined with arbitrary accuracy by choosing a sufficiently large value of ρ_1. However, the larger ρ_1 is chosen, the larger will be the uncontrollable value of $\bar{E}_x^{(1,1)}$; and therefore, the attainable accuracy in the determination of $\mathscr{E}_!^{(1)}$ by means of the simple measuring arrangement previously described, which according to (45) is given by

$$\Delta \mathbb{E}_*^{(1)} \sim \frac{\Delta p_x^{(1)}}{\rho_1 \bar{V}_1 \bar{T}_1} + \Delta \bar{E}_*^{(1,1)} \tag{46}$$

has a limit imposed upon it. Indeed, due to relation (16) and to the fact that the quantity $D_x^{(1)}$ appearing in (43) is predictable only with a latitude Δx_i, we get from (46) the expression

$$\Delta \mathbb{E}_x^{(1)} \sim \frac{\hbar}{\rho_1 \Delta x_1 V_1 T_1} + \rho_1 \Delta x_1 V_1 T_1 \left| \bar{A}_{xx}^{(1,1)} \right| \tag{47}$$

for $\Delta \mathbb{E}_x^{(1)}$, whose minimal value obviously is

$$\Delta_m \mathbb{E}_x^{(\mathrm{I})} \sim \sqrt{h \left| \bar{A}_{xx}^{(\mathrm{I}.1)} \right|} \tag{48}$$

and in the case $L_\mathrm{I} > cT_\mathrm{I}$ precisely equals the critical quantity Q_I. It is true that when L_1 is large compared to cT_1, (48) is essentially smaller than the expression (24) which was given by Landau and Peierls as the absolute
limit on the measurability of field quantities; yet if (48) were to be considered as an unavoidable limit on the accuracy of measurement, we should still arrive at the conclusion, in agreement with the view of these authors, that the quantum-electromagnetic formalism admits of no test in the properly quantum domain, and that therefore physical reality can be ascribed to the entire field theory only in the classical limit.

However, this conclusion cannot be maintained, for the fact that according to (43) the coefficient of the unpredictable displacement $D_*^{(\mathrm{I})}$ in $\bar{E}_x^{(\mathrm{I},\mathrm{I})}$ is a well-defined quantity depending solely on geometrical relations, allows us to so arrange things in the measurements that the effect of the field $E_x^{(1)}$ is completely compensated except for the unavoidabie field fluctuations. This is achieved by a measuring arrangement in which the test body is not freely movable, even during the measuring interval T_1, but remains connected with the rigid frame through a spring mechanism whose tension is proportional to $\boldsymbol{D}_{\boldsymbol{x}}^{()}$. If the force in the x-direction exerted by this mechanism on the test body is $-F_x D_x^{(1)}$, then the total momentum transferred from the field $E_x^{(1)}$ to this body will obviously be completely cancelled by the spring if the spring constant is

chosen to be

(49) $F_{\mathrm{I}} = \rho_{\mathrm{I}}^2 V_{\mathrm{I}}^2 T_{\mathrm{I}} \bar{A}_{xx}^{(\mathrm{I},\mathrm{I})}$.

At any rate, this holds when the test body is so heavy that its oscillation period under the influence of the spring is large compared to T_1 and thus its displacement due to the spring tension during the time T_1 is small compared to $D_x^{(1)}$. Furthermore, the action of the spring, which strictly speaking is classically describable only in the asymptotic limiting case, may be calculated on the basis of classical mechanics with an accuracy which is the greater the larger the mass of the test body. Apart from the limitations due to the atomic structure of all bodies, no objcction of principle could exist against such a compensation device. In the first place, by using a mechanical spring all electromagnetic fields are avoided, which would be inseparable from the fields to be measured. Secondly, if the length of the spring is sufficiently small, i.e. small compared to cT_{b}, one may obviously disregard all retardation effects. In doing so, if the test body system is sufficiently heavy, it is clearly immaterial whether the spring acts only on a component body or whether one uses a system of springs that affects each component body uniformly.

Thus we see that the sharpness of a single field measurement is restricted
solely by the limit set for the classical description of the field effects of the test body. However, even in the case $L_1 \leqslant cT_1$ this iimitation, which is the more insignificant the larger L_i is compared to cT_i, implies no restriction at all on the possibility of testing the consequences of the quantumelectromagnetic formalism. In assessing this question, we must distinguish sharply between the testing of theoretical predictions which presuppose data concerning electric or magnetic forces obtained by field measurements, and of those which depend on knowledge of the state of the field in question obtained on some other basis. As for the former predictions, their testing obviously requires a closer investigation of the mutual relations between several ficld measurements; thus, to begin with, here it can only be a matter of testing predictions of the latter kind.

Now, as mentioned in Section 2, it is a major result of the quantum theory of fields that all predictions concerning field averages which do not resi on true field measurements, but on the light quantum composition of the field to be investigated or on the knowledge of classically described field sources, must be of an essentially statistical nature. Further, the more detailed argument presented there shows that inclusion of the fluctuations of the test body's field effects around their classically cstimated value brings about no change whatsoever in these statistical predictions. Without further correction, the measurement results obtained by means of the experimental arrangement described thus appear as the desired field averages for testing the theoretical statements. Such a view of the measuring results, whose general justification we shall investigate more closely in the following, is also suggested by the fact that all measurements of physical quantities, by definition, must be a matter of the application of classical concepts; and that, therefore, in field measurements any consideration of limitations on the strict applicability of classical electrodynamics would be in contradiction with the measurement concept itself.

Even though, consequently, as already stressed in the Introduction, the measurement concept is to be appiied with even greater caution in ficld measurements than in the usual quantum mechanical measurement problems; nevertheless, as regards the inseparability of phenomenon and measuring process the situation described exhibits a far-reaching analogy to these problems. Indeed, even in a position or momentum measurement on the electron in a hydrogen atom in a given stationary state one can assert with a certain right that the measuring result is produced only by
the measurement itself. It is here not a question of a limitation on the sharpness of the measuring result on the basis of classical mechanics, indeed; but only of abandonment of any control over the infiuence of the mcasuring process on the state of the atom. In field measurements, this complementary feature of the description, essential for consistency, corresponds to the fact

that the knowledge of the light quantum composition of the field is lost through the field effects of the test body; and in fact, according to (44) the more so, the greater the desired accuracy of the measurement. Moreover, it will appear from the following discussion that any attempt to re-establish the knowledge of the light quantum composition of the field through a subsequent measurement by means of any suitable device would at the same time prevent any further utilization of the field measurement in question.

However, the fact that pure black-body fluctuations appear as the common limitation in the demonstration of the correspondence between the testability of the consequences of the quantum-electromagnetic formalism by means of a single field measurement and the interpretability of such a measurement on the basis of classical electrodynamics in no way implies that these fluctuations set an absolute limit for any utilization of fieid measurements. Indeed, such a general imitation exists neither for the consequences of the formalism regarding relations between averages of a field component over different regions, nor for the testing of such relations through direct field measurements. This will become clear from the considerations in the following sections; and in particular it will be shown that the requirement of repeatability of measurements of kinematical and dynamical quantities, essential for the discussion of the consistency of the usual quantum mechanics, possesses its natural analog in field measurements.

27.3.6 Б. Measurability of Two-fold Averages of a Field Component

In investigating the measurability of two field quantities it is convenient to start with the measurement of the average of one and the same field component over two different regions, I and II. Thus, considering as above the field component $\mathbb{E}_x$, and disregarding to begin with the limitations of the classical describability of the test bodies' field effects, we have
in this case for the momentum balance of the two test bodies, instead of (45):

$$\begin{cases} p_x^{(\mathrm{i})\prime\prime} - p_x^{(\mathrm{i})} = \rho_{\mathrm{I}} V_{\mathrm{I}} T_{\mathrm{I}} \left(\overline{\mathbb{E}}_x^{(\mathrm{i})} + \bar{E}_x^{(\mathrm{i,i})} + \bar{E}_x^{(\mathrm{i,i})} \right) \\ p_x^{(\mathrm{II})\prime\prime} - p_x^{(\mathrm{II})\prime} = \rho_{\mathrm{II}} V_{\mathrm{II}} T_{\mathrm{II}} \left(\bar{(}_x^{(\mathrm{II})} + \bar{E}_x^{(\mathrm{II,II})} + \bar{E}_x^{(\mathrm{I,II})} \right), \end{cases} \tag{50}$$

where $\bar{E}_x^{(1,11)}$ is defined by expression (43), and $E_x^{(11,1)}$ is obtained from this expression by simple interchange of the indices I and II.

According to the considerations in the previous sections, the appearance of the expressions $\bar{E}_x^{(\mathrm{I,I})}$ and $\bar{E}_x^{(\mathrm{II,II})}$ in equations (50) implies that each of the desired field averages, $\mathbb{E}_x^{(1)}$ and $\mathbb{E}_x^{(II)}$, can only be determined with a iimited accuracy, given by (48), by means of a simple measuring arrangement. Thus, it is evident from the beginning that a compensation procedure is unavoidable, and for preliminary orientation about the more complicated measuring problem considered here we therefore first use a measuring arrangement in which the reactions, $\rho_{\mathrm{I}} V_{\mathrm{I}} T_{\mathrm{I}} \bar{E}_{\mathrm{x}}^{(\mathrm{I,I})}$ and $\rho_{\mathrm{II}} V_{\mathrm{II}} T_{\mathrm{II}}\ \bar{E}_x^{(II,I)}$, are cancelled by means of two springs acting on the test bodies I and II, the spring constants being given by (49) and an analogous expression.

From equations (50), with $\bar{E}_x^{(1,1)}$ and $\bar{E}_x^{(11,11)}$ omitted, it follows, using (16) and (43), that in this arrangement the uncertainties of the two field measurements, taking into account that the displacements of the test bodies, $D_x^{(\mathrm{I})}$ and $D_x^{(\mathrm{II})}$, appearing in $\bar{E}_x^{(\mathrm{I,II})}$ and $\bar{E}_x^{(\mathrm{II,I})}$ are completely independent of each other and known only with the latitudes Δx_1 and Δx_{11}, are given by

$$\begin{cases} \Delta \mathbb{E}_x^{(\mathrm{I})} \sim \frac{\hbar}{\rho_{\mathrm{I}} \Delta x_{\mathrm{I}} V_{\mathrm{I}} T_{\mathrm{I}}} + \rho_{\mathrm{II}} \Delta x_{\mathrm{II}} V_{\mathrm{II}} T_{\mathrm{II}} \left| \bar{A}_{xx}^{(\mathrm{III,I})} \right| \\ \Delta \mathbb{E}_x^{(\mathrm{II})} \sim \frac{\hbar}{\rho_{\mathrm{II}} \Delta x_{\mathrm{II}} V_{\mathrm{II}} T_{\mathrm{II}}} + \rho_{\mathrm{I}} \Delta x_{\mathrm{I}} V_{\mathrm{I}} T_{\mathrm{I}} \left| \bar{A}_{xx}^{(\mathrm{I,II})} \right|. \end{cases} \tag{51}$$

By suitable choice of the values of $\rho_{\mathrm{I}} \Delta x_{\mathrm{I}}$ and $\rho_{\mathrm{II}} \Delta x_{\mathrm{II}}$ either one of the quantities $\Delta \mathfrak{C}_x^{(1)}, \Delta \mathfrak{C}_x^{(1)}$ can obviously be arbitrarily diminished, but oniy at the expense of an increase of the other.

For according to (51) we get for the product of the two quantities the minimum value

$$\Delta\mathbb{C}_x^{(\mathrm{I})}\Delta\mathbb{C}_x^{(\mathrm{II})} \sim \hbar\left[\left|\bar{A}_{xx}^{(\mathrm{I,II})}\right| + \left|\bar{A}_{xx}^{(\mathrm{II,I})}\right|\right]. \tag{52}$$

In spite of the great similarity of relation (52) to the uncertainty relations (8) required by the formalism, there is, nevertheless, a fundamental
difference in that the latter contains not the sum of the magnitudes of the quantities $\bar{A}_{xx}^{(\mathrm{I,1I})}$ and $\bar{A}_{xx}^{(\mathrm{II},1)}$ but their algebraic difference. It is true that (8) and (52) are in generai in agreement as to order of magnitude when the regions I and II are spatially and temporally displaced relative to each other by distances of order of magnitude L and T, in which case they both have the approximate value Q^2. However, as mentioned in Section 2, the difference sign appearing in the indeterminacy relation (8) has the effect that in important cases the product of the complementary uncertainties vanishes identically, even though the quantities $\bar{A}_{xx}^{(1,11)}$ and $\bar{A}_{xx}^{(11,1)}$ each remain different from zero. This happens, for example, when the temporal averaging intervals T_I and T_{II} coincide, and in particular when the two averaging regions I and II completely overlap. In the latter case even the limit on the measurability of two field averages given by (52) would be in glaring contradiction to the result of the previous discussion of measurement of a single field average. In general, the two expressions (52) and (8) agree exactly only when at least onc of the quantities $\bar{A}_{xx}^{(\mathrm{I,II})}$ or $\bar{\Lambda}_{xx}^{(\mathrm{II,I})}$ vanishes which in general requires that one of the expressions $t_1 - t_2 - r/c$ or $t_2 - t_1 - r/c$, appearing as arguments of the δ-function in the integrals (5), remain different from zero for every pair of points (x_1, y_1, z_1, t_1) and (x_2, y_2, z_2, t_2) of regions I and II.

Thus, anart from the last mentioned case in which there exists no correlation, or at any rate only a one-way correlation, between the two field averages, the demonstration of the agreement between measurability and quantum electromagnetic formalism requires more refined measuiing arrangement in which the uncontrollable effects can be compensated to a larger extent. It is true that there appears here, in comparison with the compensation procedure needed already for measuring a single field quantity, the further complication that the displacements of the two test bodies not only must remain unknown but are also completely independent of each other. However, this circumstance implies no fundamental difficulty; only a somewhat more complicated procedure is necessary in order to compensate as much as possible the influence of the relative displacement of the test bodies on the field measurements. For this purpose we select two component bodies ε_I and ε_{II}, one from each test body system I and II, for which the expression $r - c\,(t_1 - t_2)$ vanishes for two times t_{I}^* and t_{II}^* lying in the time intervals T_{I} and T_{II}, respectively. If such a choice were not possible, then as said above the agreement between measurability and formalism would already be attained without further compensation. To establish the necessary correlation between the test bodies one might at first think of a spring which should connect the bodics ε_i and ε_{ii} directly with each other; however, due to the retardation of the forces one would thereby run into difficulties. But one can manage with a short spring, i.e. small compared to cT, if one adds to the second test body system a neutral component body $\varepsilon_{\mathrm{III}}$ which is situated in the immediate neighborhood of component body ε_i, belonging to the first system, and connected with it by a spring.

Like all component bodies of the two test body systems, the body $\varepsilon_{\mathrm{III}}$ is initially to be bound to the rigid frame. Then at time t_1', its momentum is to be mcasured, after severing of this link, with the same accuracy as that of test body system II. It thereby undergoes an unknown displacement $D_x^{(\mathrm{III})}$ in the x-direction which is of the same order of magnitude as Δx_{II}. If now the tension of the spring mounted between $\varepsilon_{\mathrm{III}}$ and ε_1 is chosen equal to $\frac{1}{2}\rho_{\mathrm{I}}\rho_{\mathrm{II}}V_{\mathrm{I}}V_{\mathrm{II}}T_{\mathrm{II}}\left(\bar{A}_{xx}^{(\mathrm{I,II})} + \bar{A}_{xx}^{(\mathrm{II,I})}\right.$, then in the time interval T_1 the momentum

$$P = \frac{1}{2}\rho_{\mathrm{I}}\rho_{\mathrm{II}}V_{\mathrm{I}}V_{\mathrm{II}}T_{\mathrm{I}}T_{\mathrm{II}}\left(\bar{A}_{xx}^{(\mathrm{I,II})} + \bar{A}_{xx}^{(\mathrm{II,I})}\right)\left(D_x^{(\mathrm{I})} - D_x^{(\mathrm{III})}\right) \tag{53}$$

will be transferred from $\varepsilon_{\mathrm{III}}$ to ε_I, while $\varepsilon_{\mathrm{III}}$ undergoes the momentum change $-P$ during the same time interval. At time t'' the momentum of $\varepsilon_{\mathrm{III}}$ is measured again with the same accuracy. However, before this measurement, and in fact at time t_{11}^*, a short light signal is to be sent from $\varepsilon_{\mathrm{II}}$ to $\varepsilon_{\mathrm{III}}$, by which the relative displacement $D_x^{(\mathrm{III})} - D_x^{(\mathrm{II})}$ of these bodies can be measured with arbitrary accuracy by means of a suitable device. At the emission and absorption of the signal the two bodies undergo momentum changes which indeed remain completely unknown, but cancel each other exactly in the sum of the momentum changes measured on the bodies.

Thus, for the momentum baiance of the two test body systems duiring the measurement we have, if we include the body $\varepsilon_{\mathrm{III}}$ in system II,

$$\begin{cases} p_x^{(\mathrm{I})''} - p_x^{(\mathrm{I})'} = \rho_{\mathrm{I}} V_1 T_{\mathrm{I}} \left(\mathfrak{G}_x^{(\mathrm{I})} + \bar{E}_x^{(\mathrm{II,I})} \right) + P \\ p_x^{(\mathrm{II})''} - p_x^{(\mathrm{II})'} + p_x^{(\mathrm{III})''} - p_x^{(\mathrm{III})'} = \rho_{\mathrm{II}} V_{\mathrm{II}} T_{\mathrm{II}} \left(\overline{\mathfrak{F}}_x^{(\mathrm{II})} + \bar{E}_x^{(\mathrm{I,II})} \right) - P \end{cases} \tag{54}$$

Taking into account (43) and (53), these formulae can be put into the form

$$\begin{aligned} & \int p_x^{(1)''} - p_x^{(1)'} = \rho_1 V_1 T_1 \mathbb{E}_x^{(1)} \\ & + \frac{1}{2} \rho_{\mathrm{I}} \rho_{\mathrm{II}} V_{\mathrm{I}} V_{\mathrm{II}} T_{\mathrm{I}} T_{\mathrm{II}} \left\{ -D_x^{(\mathrm{III})} \left(\bar{A}_{xx}^{(\mathrm{II,II})} - \bar{A}_{xx}^{(\mathrm{II,I})} \right) \right. \\ & \left. + \left(D_x^{(\mathrm{II})} - D_x^{(\mathrm{III})} \right) \left(\bar{A}_{xx}^{(\mathrm{I,II})} + \bar{A}_{xx}^{(\mathrm{II,I})} \right) + D_x^{(\mathrm{II})} \left(\bar{A}_{xx}^{(\mathrm{I,II})} + \bar{A}_x^{(\mathrm{II,I})} \right) \right\} \\ & p_x^{(\mathrm{II}\,)''} - p_x^{(\mathrm{III}\,)'} + p_x^{(\mathrm{III}\,)''} - p_x^{(\mathrm{III}\,)'} = p_{\mathrm{II}}\, V_{\mathrm{II}}\, T_{\mathrm{II}}\, \mathbb{E}_x^{(\mathrm{II})} \\ & + \frac{1}{2} \rho_{\mathrm{I}} \rho_{\mathrm{II}} V_{\mathrm{I}} V_{\mathrm{II}} T_{\mathrm{I}} T_{\mathrm{II}} \left\{ D_x^{(\mathrm{I})} \left(\bar{A}_{xx}^{(\mathrm{II,II})} - \bar{A}_{xx}^{(\mathrm{II,I})} \right) \right. \\ & \left. - \left(\bar{D}_x^{(\mathrm{II})} - \bar{D}_x^{(\mathrm{II})} \right) \left(\bar{A}_{xx}^{(\mathrm{I,i,i})} + \tilde{A}_{xx}^{(\mathrm{i,i})} \right) + D_x^{(\mathrm{i})} \left(\bar{A}_{xx}^{(\mathrm{i,\tilde{i}})} + \bar{A}_{xx}^{(\mathrm{i,\tilde{i}})} \right) \right\} \end{aligned} \tag{55}$$

The last terms in the curly brackets in (55) are proportional to the unknown displacements of the test bodies I and II and can therefore, exactly as the simple reactions of each test body on itself, be cancelled by means of suitable spring connections with the rigid frame. This simply amounts to replacing the expression (49) for the tension of the spring acting on body I by

$$F_{1,\mathrm{II}} = \rho_1^2 V_1^2 T_1 \bar{A}_{xx}^{(1,1)} + \frac{1}{2} \rho_1 \rho_{11} V_1 V_{11} T_{11} \left(\bar{A}_{x\lambda}^{(1,11)} + \bar{A}_{x\lambda}^{(11,1)} \right) \tag{56}$$

and similarly changing the tension of the spring between the frame and body II Furthermore, in the measuring arrangement describcd, the terms proportional to the relative displacement $D_r^{(\mathrm{III}\,)} - D_x^{(\mathrm{II}\,)}$ are known with arbitrary accuracy and can therefore easily be taken into account in the field measurements. In fact, by means of a somewhat more complicated device one could even obtain the vanishing of the difference $D_x^{(\mathrm{III}\,)} - D_x^{(\mathrm{II}\,)}$ by using $P_x^{(\mathrm{II}\,)} + P_x^{(\mathrm{III}}$ (in analogy to the arrangement for measuring the total momentum of a test body system described in Section 3) to determine one and the same radiation packet and, by means of suitably placed fixed mirrors, by regulating the light path in such a way that in the first momentum measurement the reflections at body ε_{m} and at all component bodies of system II occur at the times t_1' and $t_{1\mathrm{l}}'$, respectively, and in the second momentum measurement occur at the times t_1'' and t_{11}''.

By means of all these contrivances, whose considerable complexity lies in the nature of the problem, being due solely to the finite propagation of all field effects, we now have actually removed the apparent conflict between the determination of single and two-fold averages of a field component described at the beginning of this section. For from (55) we now obtain for the indeterminacies of $\mathbb{E}_x^{(1)}$ and $\mathbb{E}_x^{(11)}$, instead of (51),

$$\left\{\begin{array}{l} \Lambda\mathbb{E}_x^{(\mathrm{I})} \sim \frac{\hbar}{\rho_{\mathrm{I}}\Delta x_{\mathrm{I}} V_{\mathrm{I}} T_{\mathrm{I}}} + \frac{1}{2}\rho_{\mathrm{in}}\Delta x_{\mathrm{iI}} V_{\mathrm{iI}} T_{\mathrm{iI}} \left|\bar{A}_{xx}^{(\mathrm{I,II})} - \bar{A}_{xx}^{(\mathrm{II,I})}\right| \\ \Lambda\mathbb{E}_x^{(\mathrm{II})} \sim \frac{\hbar}{\rho_{\mathrm{II}}\Delta x_{\mathrm{II}} V_{\mathrm{II}} T_{\mathrm{II}}} + \frac{1}{2}\rho_{\mathrm{i}}\Delta x_{\mathrm{i}} V_{\mathrm{i}} T_{\mathrm{i}} \left|\bar{A}_{xx}^{(\mathrm{II,II})} - \bar{A}_{xx}^{(\mathrm{II,I})}\right|, \end{array}\right. \tag{57}$$

which immediately yields for the minimal value of the product of the uncertainties

$$\Delta\overline{\mathbb{C}}_x^{(\mathrm{i})}\Delta\mathbb{E}_x^{(\mathrm{i})} \sim h\left|\bar{A}_{xx}^{(\mathrm{i,i,i})} - \bar{A}_{xx}^{(\mathrm{i,i,i})}\right| \tag{58}$$

in agreement with the consequence of the quantum theory of fields expressed by (8).

However, in order to demonstrate the complete accord between the measurability of the averages of a field component over two space-time regions and the requirements of the quantum electromagnetic formalism, we must go somewhat further into the question of the extent to which the assumption of the classical describability of the test body's field effects impairs the possibilities of testing theoretical predictions. For, as already indicated, exactly in the case of measurement of several field averages one might think beforehand that the neglect of the fluctuations of all field cffects of the test body, which cannot be followed classically, and are inseparable from the pure black-body fluctuations, in this respect signifies an essential renunciation. At any rate, as long as we are dealing with averaging regions which are displaced spatially and temporally relative to each other by distances of the same order of magnitude as their linear dimensions L and corresponding time intervals T, this neglect is of little significance in the important case where L is large compared to cT. However, if L is of the same order of magnitude or smaller than cT, then the black-body fluctuations, as mentioned in Section 2, are of just the same order of magnitude as the critical field strength $\mathfrak{U}$, which is defined for such displaced regions by means of the indeterminacy relations and is to be regarded as the limit of the classical field description. The neglect in question might appear even more doubtful and seem to imply a complete renunciation of the repeatability of field measurements in the case of two almost coinciding domains, in which the product of the complementary uncertainties of the field averages, given by (8), tends to zero independently of the ratio between L and cT, and where thus the critical field strength U can be arbitrarily small compared to the black-body fluctuations.

Nevertheless, a closer consideration shows that we obtain a consistent interpretation of all consequences of the quantum theory of fields, if, in a necessary generalization of the measurement concept, we interpret the measuring results obtained by the arrangement described as the desired field averages. For the classically undescribable fluctuations included in the field effects of all test bodies cannot be separated in any way from the fundamentally statistical features of every theoretical assertion whose conditions do not refer to actual field measurements. Without in any way limiting the given measurement problem we can therefore always regard the fluctuations in question as an integral part of the field to be measured. The situation in multiple field measurements differs in this respect from that obtaining in measurement of a single field average only insofar as the state of the field, with which we are concerned in every single measurement in the general case, is codetermined by the result of the other field measurements.

However, with regard to this state of affairs it may not be superfluous to point out that in the correlation of several field measurements we have to do with a feature of the general complementarity of description which is alien to the usual measuring problem of non-relativistic quantum mechanics. Indeed, the fundamental simplification which we meet in the latter theory lies precisely in the separation made there between spatial coordination and temporal evolution, which makes it possible to order all measuring processes in a simple temporal sequence. On the other hand, it is possibie to speak of such a sequence of measuring processes during the measurement of two field averages only when the corresponding time intervals do not overlap at all. In general, in accordance with the formalism, the correlation of the two measurements is also a reciprocal one; and only when one of the quantities $r - c\,(t_1 - t_2)$ and $r - c\,(t_2 - t_1)$

remains different from zero for all pairs of points of the regions I and II, do we encounter conditions similar to those of the usual measurement problem of atomic mechanics, since the result of the one field measurement may then be simply included in the preconditions used in the predictions to be tested by the other measurement.

We meet an instructive example of an intimate reciprocal correlation in measurements of the averages of a field component over two almost coinciding space-time domains. In conformity with the requirement of the repeatability of measurement results, the theory demands in this case that
both measurements yield the same result to an arbitrary degree of approximation quite independentily of the siatistical assertions about the values of the field quantities to be measured which are implied by the preconditions. That this requirement is actually fulfilled in our experimental arrangement follows from the fact that in this case we have to do with two test body systems which occupy aimost the same spatial region and are used during almost the same interval of time. Thus, by definition, they are exposed to almost the same field, quite irrespective of the sources producing this field, and of which contribution comes from one or the other test body.

Actually, it follows from the last remark that in the case of coinciding averaging regions we would get exactly identical results of the two measurements even without any compensation. However, on account of the field effects of the test bodies the measurement resuits so obtained would differ in an unpredictable way from the theoretical predictions to be tested, the more so, the greater the desired measuring accuracy. It is true that by means of the compensation mechanism suitable for single field measurements, which we had retained unaltered at the beginning of this section, these deviations are in general diminished; but at the same time any strict correlation of the measuring results is prevented by the effects of the springs which are proportional to the independent displacements of the test bodies. In the arrangement for two field measurements finally adopted, in which all well-defined differences between measurement results and theoretical predictions are compensated, such a correlation is also re-established just in the case of coinciding regions. For, as one easily sees, quite independently of the relation between the magnitudes of the uncontrollable displacements of the test bodies, the momenta transferred to each test body through the combined effect of all the springs, divided by the corresponding charge densities, are exactly identical in this case.

As far as the consistency of the description is concerned, we might still remark that any attempt to control the change in the light quantum composition of the field caused by the field measurement by investigation of the test body's radiation, as already mentioned several times, would exclude the possibility of utilizing the measurement result for a comparison with a second field measurement. For in order even to be able to speak of such a utilization, there must exist pairs of points from the regions I and

II, respectively, for which one of the expressions $r - c(t_1 - t_2)$ or $r - c(t_2 - t_1)$ vanishes. But this implies that the radiation fields produced by the test bodies I and II during the measurement cannot be interecpted and analyzed on their way from one test body to the other without at the same time essentially influencing the fields to be measured by these bodies. Only after the completion of all field measurements, when their direct utilization is no longer of concern, is it possible to perform an arbitrarily accurate analysis of the light quantum composition of the entire field without adversely affecting the given measurement problem.

27.3.7 7. Measurability of Two Averages of Different Field Components

As far as measurements of averages of different field components are concerned, only the case of perpendicular, similar or dissimilar components needs closer investigation; for the complete commutativity and independent measurability of averages of parallel dissimilar components re-

quired by the quantum electromagnetic formalism finds its direct interpretation in the identical vanishing of the component $H_x^{(1)}$ of the field produced by the measurement of $\mathbb{E}_x^{(1)}$, as shown by (42). Besides, on the basis of equations (43), the measurement of averages of perpendicular field components allows a method of treatment analogous to the procedure described in the previous section.

Let us consider the measurement of the average of $\mathfrak{F}_x$ over the region I and the average of $\mathfrak{E}_y$ or $\mathfrak{S}_y$ over the region ii. If to begin with we use a measuring arrangement in which the field effects of each test body on itself during the measurement are compensated in the manner described in Section 5, we get equations of the following type for the momentum balance of the two test bodies to be used:

$$\left\{\begin{array}{l} p_x^{(\mathrm{I})''} - p_x^{(\mathrm{II})'} = \rho_1 V_1 T_\mathrm{I} \left(\bar{(}_x^{(\mathrm{I})} + D_y^{(\mathrm{II})} \sigma_\mathrm{II} V_\mathrm{II} T_\mathrm{II} \bar{C}_{xy}^{(\mathrm{II,I})}\right) \\ p_y^{(\mathrm{II})''} - p_y^{(\mathrm{II})'} = \sigma_\mathrm{II} V_\mathrm{II} T_\mathrm{II} \bar{\mathfrak{R}}_y^{(\mathrm{II})} + D_x^{(\mathrm{I})} \rho_1 V_1 T_\mathrm{I} \bar{C}_{xy}^{(\mathrm{I,II})}\Big) \end{array}\right. \tag{59}$$

Depending on whether we are dealing with a measurement of similar or dissimilar components, the letter $\mathfrak{R}$ here represents the usual designation of the field components $\mathfrak{E}$ or $\mathfrak{H}$, while C is written instead of the symbols A or B appearing in (43); further, the designation σ_II represents the charge density or the pole strength distribution of the test body II accordingly.

In a manner similar to the derivation of (52) one obtains from (59) the relation

$$\Delta\mathbb{E}_x^{(\mathrm{I})} \Delta\bar{\mathfrak{R}}_y^{(\mathrm{II})} \sim \hbar \left[\left|\bar{C}_{xy}^{(\mathrm{I,II})}\right| + \left|\bar{C}_{xy}^{(\mathrm{II,I})}\right|\right], \tag{60}$$

which, like (52), does not generally, but only in certain cases, represent an agreement between measurability and quantum electromagnetic formalism. Of such cases we might mention in particular the measurement of dissimilar perpendicular field components inside the same spatial region, for which, as stressed in Section 2, both expressions $\bar{B}_{.y}^{(\mathrm{I,II})}$ and $\bar{B}_{.y}^{(\mathrm{II,I})}$ vanish. The correctness of interpreting this fact as an arbitrarily accurate independent measurability of the field quantities in question was suggested alrcady in Section 3 by elementary considerations in the case of coinciding space-time regions.

For the general treatment of the measurability problem of perpendicular field components we choose, as in the previous section, two component bodies ε_1 and ε_{II} of the test body systems I and II, respectively, whose separation is $r = c\left(t_1^* - t_{\underline{11}}^*\right)$, where t_1^* and $t_{\underline{11}}^*$ are within the time intervals T_1 and T_{11}, respectively. Furthermore, in the immediate neighborhood of ε_1 we introduce a third body ε_III , whose momentum in the y-direction is measured at the times t_1' and t_1''; the relative displacements $D_y^{(III)} - D_y^{(II)}$ of the bodies ε_III and ε_II are again determined by means of a light signal. as a result of which both bodies undergo equal and opposite momentum changes. Instead of connecting ε_III directly with ε_1 by a spring we must, however, in order to make the force transfer through the spiing mechanism proportional to $D_y^{(\mathrm{III})} - D_x^{(\mathrm{I})}$, use a device which consists of two springs and an angular level with two equally long mutually perpendicular arms which can rotate on a hinge mounted on the rigid frame, and the arms of which are initially parallel to the x - and y-directions, respectively. A spring parallel to the y-axis is fastened between the first arm and the body ε_ml, and a spring parallel to the x-axis acts between the second arm and the body ε_I. Let the tension of the springs be so chosen that the force which acts on the body ε_ill in the y-direction and on the body ε_1 in the x direction during the time interval T_1 is given by

$$\frac{1}{2}\rho_1 \sigma_\mathrm{II} V_1 V_\mathrm{II} T_\mathrm{II} \left(\bar{C}_{xy}^{(\mathrm{I,II})} + \bar{C}_{xy}^{(\mathrm{II,I})}\right)\left(D_x^{(1)} - D_y^{(\mathrm{III})}\right).$$

Thus, the momentum balance of the two test body systems, after suitable rearrangement, may be expressed in the following form, analogous to (55)
(61)

After compensation of the last terms we thus obtain for the uncertainties of the field averages:

$$\begin{cases} \Delta\mathbb{E}_x^{(\mathrm{I})} \sim \frac{\hbar}{\rho_{\mathrm{I}}\Delta x_{\mathrm{I}} V_{\mathrm{I}} T_{\mathrm{I}}} + \frac{1}{2}\sigma_{\mathrm{II}}\Delta y_{\mathrm{II}} V_{\mathrm{II}} T_{\mathrm{II}} \left|\bar{C}_{xy}^{(\mathrm{I,II})} - \bar{C}_{xy}^{(\mathrm{II,I})}\right| \\ \Delta\mathfrak{R}_y^{(\mathrm{II})} \sim \frac{\hbar}{\sigma_{\mathrm{II}}\Delta y_{\mathrm{II}} V_{\mathrm{II}} T_{\mathrm{II}}} + \frac{1}{2}\rho_{\mathrm{I}}\Delta x_{\mathrm{I}} V_{\mathrm{I}} T_{\mathrm{I}} \left|\bar{C}_{xy}^{(\mathrm{I,II})} - \bar{C}_{xy}^{(\mathrm{II,I})}\right| , \end{cases} \tag{62}$$

from which the minimal value of their product is obtained as

$$\Delta\mathbb{E}_x^{(\mathrm{I})}\Delta\mathfrak{R}_y^{(\mathrm{II})} \sim \hbar \left|\bar{C}_{xy}^{(\mathrm{I,II})} - \bar{C}_{xy}^{(\mathrm{II,I})}\right| , \tag{63}$$

again in complete agreement with the quantum electromagnetic formalism.

Furthermore, from the general arguments at the end of the previous section it follows that also in the case considered here the utilization of field measurements for testing the formalism's assertions in no way is impaired by the classical evaluation of the field effects. Besides, in measurements of averages of dissimilar field components the question of repeatability does not arise at all, and the pure black-body fluctuations are included in all theoretical assertions as an unavoidable statistical feature.

27.3.8 8. Concluding Remarks

We thus arrive at the conclusion already stated at the beginning, that with respect to the measurability question the quantum theory of fields
represents a consistent idealization to the extent that we can disregard all limitations due to the atomic structure of the field sources and the measuring instruments. As alrcady emphasized in the Introduction, this result should properly be regarded as an immediate consequence of the fact that both the quantum electromagnetic formalism and the viewpoints on which the possibilities of testing this formalism are to be assessed have as their common foundation the correspondence argument. Nevertheless, it would seem that the somewhat complicated character of the considerations used to demonstrate the agreement between formalism and measurability are hardly avoidable. For in the first place the physical requirements to be imposed on the measuring arrangement are conditioned by the integral form in which the assertions of the quantum-electromagnetic formalism are expressed, whereby the peculiar simplicity of the classical field theory as a purely differential theory is lost. Furthermore, as we have seen, the interpretation of the measuring results and their utilization by means of the formalism require consideration of certain features of the complementary mode of description which do not appear in the measurement problems of non-relativistic quantum mechanics.

At the completion of this work we should not like to leave unmentioned that we have found much stimulation and help in many discussions of the questions considered with past and present colleagues at the Institute, among them Heisenberg and Pauli as well as Landau and Peierls.

Universitetets Institut for teoretisk Fysik
Copenhagen, April 1933

27.3.9 Literature

- Translated by Prof. Aage Petersen; revised by RSC and JS.

[1] W. Heisenberg, The Physical Principies of ine Quanium Theory, tianaisl. by C. Eckart and F. Hoyt (Dover, New York, 1930), pp. 42 ff.

[2] L. Landau and R. Peierls, Zs. f. Phys. 69 (1931), 56.

[3] Cf. N. Bohr, 'Atomic Stability and Conservation Laws', Atti del Congresso di Fisica Nucleare (1932). Added in the proof: A separate publication to appear shortly will

contain a discussion of the consequances for the problems discussed in the cited reference implied by the recent discovery of the occurrence, under special circumstances, of so-called 'positive electrons'; and by the recognition of the connection of this discovery with Dirac's relativistic electron theory.

[4] Cf. L. Rosenfeld, Zs. f. Phys. 76 (1932), 729.

[5] Cf. P. Jordan and W. Pauii, Zs. J. Fhys. 47 (i928), i5i and aiso $\overline{\mathbf{W}}$. Heisenberg and $\overline{\mathbf{W}}$. Pauli, Zs. f. Phys. 56 (1929), 33. Apart from an unessential difference in sign resulting from a difference in the choice of time direction in the Fourier decomposition of the field strengths, the formulae above are equivalent in content with those derived in the namers quoted. In particular, the notation used here, where all terms appear as retarded, is a purely formal change which aims at an interpretation of the measurement problems that is as intuitive as possible.

[6] Cf. L. Rosenfeld and J. Solomon, J. de Physique 2 (1931), 139 and also W. Pauli, Handbuch d. Physik, 2nd edition, Vol. 24/1 (1933), p. 255.

[7] Cf. W. Heisenberg, Leipziger Berichte 83 (1931), 1.

[8] Cf. V. Fock and P. Jordan, Zs. f. Phys. 66 (1930), 206, where reference is made to such restrictions on field measurements, which are unrelated to the quantum theory of fields. Cf. aiso J. Soiomon, J. de Priysique 4 (i933), 3688.

[9] Cf. W. Pauli, Handbuch d. Physik, 2nd edition, Vol. 24/1 (1933), p. 257.

[10] See N. Bohr, Atomic Theory and the Description of Nature (Cambridge University Press, Cambridge, Fingland, 1934). In the meantime, this question has heen treated in more detail by the author in a guest lecture in Vienna, to appear shortly, in which in particular the patadoxes arising in the interpretation of the iudeterminacy pianciple when account is taken of the requirements of relativity are further discussed.

27.4 IV.3 Field and Charge Measurements in Quantum Electrodynamics by Bohr, Rosenfeld

Abstract. A survey is given of the problem of measurability in quantum electrodynamics and it is shown that it is possible in principle, by the use of idealized measuring arrangements, to achieve full conformity with the interpretation of the formalism as regards the determination of field and charge quantities.

27.4.1 Introduction

Recent important contributions [1] to quantum electrodynamics by Tomonaga. Schwinger and others have shown that the problem of the interaction between charged particles and electromagnetic fields can be treated in a manner satisfying at every step the requirements of relativistic covariance. In this formulation, essential use is made of a representation of the electromagnetic field components on the one hand, and of the quantities specifying the electrified particles on the other, corresponding to a vanishing interaction between field and particles. The account of such interaction is subsequently introduced by an approximation procedure based on an expansion in powers of the nondimensional constant $e^2/\hbar c$. As regards the interpretation of the formalism, this method has the advantage of a clear emphasis on the dualistic aspect of electrodynamics. In fact, an unambiguous definition of the electromagnetic field quantities rests solely on the consideration of the momentum imparted to appropriate test bodies carrying charges or currents, while the charge-current distributions referring to the presence of particles are ultimately defined by the fields to which these distributions give rise.

Just from this point of view the problem of the measurability of field quantities has been discussed by the authors in a previous paper. [2] A similar investigation of the measurability

of electric charge density was then also undertaken, but, owing to various circumstances, its publication has been delayed. [3] When recently the work was resumed, it appeared that by making use of the new development as regards the formulation of quantum electrodynamics a more general and exhaustive treatment

Originally published in Physical Review, 78, 794-98 (1950); rcproduced here from Selected Papers of Lon Rosenfeld, Cohen and Stachel, eds. (1979), Reidel, Dordrecht, pp. 401-412.
could be obtained. [4] As these considerations my be helpful in the current discussion of the situation in atomic physics, we shall here give a brief account of the implications of present electron theory for measurements of charge-current densities. For this purpose, it will be convenient to start with a summary of our earlier treatment of the measurability of field quantities. [5]

27.4.2 1. Measurements of Electromagnetic Fields

Classical electrodynamics operates with the idealization of field components $f_{\mu v}(x)$ defined at every point (x) of space-time. Although in the quantum theory of fields these concepts are formally upheld, it is essential to realize that only averages of such field components over finite spacetime regions R, like

$$F_{\mu v}(R) = \frac{1}{R}\int_R f_{\mu v}(x) d^4x \tag{1}$$

have a well-defined meaning (I, §2). In the initial step of approximation, in which all effects involving $e^2/\hbar c$ are disregarded, these averages obey commutation relations of the general form (2) $[F_{\mu\nu}(R), F_{\kappa\lambda}(R')] = i\hbar c\,[A_{\mu\nu,\kappa\lambda}(R,R') - A_{\kappa\lambda,\mu\nu}(R',R)]$, where the expressions of the type $A_{\mu\nu,\kappa\lambda}(R,R')$, defined as integrals over the space-time regions R and R' of certain singular functions, have finite values depending on the shapes and relative situation of the regions R and R'.

The measurement of a field average $F_{\mu\nu}(R)$ demands the control of the total momentum transferred within the space-time region R to a system of movable test bodies with an appropriate distribution of charge or current, of density ρ_v, covering the whole part of space which at any time belongs to the region R. In the case of an electric field component F_{4l}, we shall take a distribution of charge, with constant density ρ_4, and in the case of a magnetic field component F_{mn}, a uniform distribution of current in a perpendicular direction, with density components ρ_m and ρ_n. The field action of such charge-current distribution, so far as it does not originate from the displacements of the test bodies accompanying the momentum control, can in principle be eliminated by the use of fixed auxiliary bodies carrying a charge-current distribution of opposite sign,
and constructed in a way which does not hinder the free motion of the test bodies. In the case of a current distribution, such auxiliary bodies are even indispensable in providing closed circuits for the currents by means of some flexible conducting connection with the test bodies. As a result of this compensation, the field sources of the whole measuring arrangement will thus merely be described by a polarization $\boldsymbol{P}_{\mu v}$ arising from the uncontrollable displacements of the test bodies in the course of the field measurements.

If the test bodies are chosen sufficiently heavy, we can throughout disregard any latitude in their velocities, but the control of their momentum will of course imply an essential latitude in their position, to the extent demanded by the indeterminacy relation. Still, it is possible, without violating any requirement of quantum mechanics, not only to keep every test body fixed in its original position except during the time interval within the region R corresponding to this position, but also to secure that, during such time intervals, the displacements of all test bodies in the direction of the momentum transfer to be measured, although uncontrollable, are exactly the same. This common displacement $\bar{D}_\mu$ is described, in the case of the measurement

of an electric field, by the component D_l narallel to the field component F_{4l}, and when a magnetic field is measured, by the components D_m and D_n perpendicular to $F_{m\pi}$. Without imposing any limit on the accuracy of the held measurement, it is, moreover, possible to keep the displacement D_μ arbitrarily small, if only the chargecurrent density ρ_v of the test bodies is chosen sufficiently large. By a further refinement of the composite measuring arrangement described in our earlier paper (1, §3), it is even possible to reduce the measurement of any field average to the momentum control of a single supplementary body, and thus to obtain a still more compendious expression for the ultimate consequences of the general indeterminacy relation.

An essential point in field measurements is, however, the necessity of climinating so far as possible the uncontrollable contribution to the average field present in R, arising from the displacement of the test bodies in the course of the measurement. In fact, the expectation value of this contribution will vary in inverse proportion to the latitude allowed in the field measurement, since it is proportional to the polarization $P_{\mu\nu} = D_\mu\rho_\nu - D_\nu\rho_\mu$ within the region R. Just this circumstance, however, makes it possible, by a suitable mechanical device, by which a force proportional
to their displacement is exerted on the test bodies, to compensate the momentum transferred to these bodies by the uncontrollable field. insofar as the relation of this field to its sources is expressed by classical field theory. With the compensation procedure described, the resulting measurement of $F_{\mu v}(R)$ actually fulfils all requirements of the quantum theory of fields as regards the definition of field averages (I, §5). In fact, the incompensable part of the field action of the text bodies due to the essentially statistical character of the elementary processes involving photon emission and absorption, corresponds exactly to the characteristic field fluctuations which in quantum electrodynamics are superposed on all expectation values determined by the field sources.

When the measurement of two field averages $F_{\mu v}(R)$ and $F_{\nu\lambda}(R')$ is considered, it appears (I, §4) that the expectation value of the average field component $\Phi_{\mu v,\kappa\hat{\lambda}}(R, R')$ which the displacement of the test bodies operated in the region R produces in the region R' is equal to the product of $\frac{1}{2}RP_{\mu v}$ with the quantity $A_{\mu v,\kappa\hat{\lambda}}(R, R')$ occurring in the commutation relation (2). Likewise, the expectation value of the average component $\Phi_{\kappa\lambda,\mu v}(R', R)$ of the field in R due to the test bodies in R' is equal to $\frac{1}{2}R'\Gamma'_{h\lambda}A_{\lambda\lambda,\mu v}(R', R)$. When optimum compensation of the momenta transferred to the test bodies by these fields is established by suitable devices, making use of a correlation by light signals transmitted between points of the two regions R and R', it can be deduced from the reciprocal indeterminacy of position and momentum control that the only limitations of the measurability of the two field averages considered correspond exactly to the consequences of the commutation rule (2) for such averages (I, §6, 7). In this connection, it must be stressed that the field fluctuations which are inseparable form the incompensable parts of the fields created by the operation of the test bodies, do not imply any restriction in the measurability of a field component in two asymptotically coinciding space-time regions. In fact, we have here to do with a complete analog to the reproducibility of the fixation of observables in quantum mechanics by immediately repeated measurements.

2. Charge-current measurements in
INITIAL APPROXIMATION

In the formalism of quantum electrodynamics, charge-current densities,
like field quantities, are introduced by components $j_v(x)$ at every spacetime point, but, even in the initial approximation in which such symbois are formally commutable, well-defined expressions are only given by integrals of the type

(3) $\quad J_v(R) = \frac{1}{R}\int_R j_v(x)\mathrm{d}^4x,$

representing the average charge-current density within the finite spacetime region R. From the fundamental equations of electrodynamics it follows quite generally that

(4)

$$RJ_v(R) = \int_R \frac{\partial f_{v\mu}}{\partial x_\mu} \mathrm{d}^4x = \int_S f_{v\mu}\ \mathrm{d}\sigma_\mu$$

which expresses the definition of the average charge-current density over the region R in terms of the flux of the electromagnetic field through the boundary S of this region. In this four-dimensional representation, such generalized fluxes comprise, of course, besides the ordinary electric ficld flux defining the average charge density, other expressions pertaining to the average current densities and representing magnetic field circulations and displacement currents.

In the simple special case in which the region R is defined by a fixed spatial extension V and a constant time interval T, the average charge density, in accordance with (4), will be given, in the ordinary vectorial representation, by

$$J_4(V,T) = \frac{1}{VT} \int_T \mathrm{d}t \int_S \mathrm{End}\ \sigma \tag{5}$$

where S is the surface imiting the extension V, and n the unit vector in the outward normal direction on this surface. In such representation, the average current density will be given by

$$\mathbf{J}(V,T) = \frac{1}{VT} \int_T \mathrm{d}t \int_S \mathbf{n} \wedge \mathbf{H}\ \mathrm{d}\sigma - \frac{1}{VT} \int_V \mathbf{E}\ \mathrm{d}v \Big|_{t_1}^{t_2} \tag{6}$$

where the first term on the right-hand side represents the time integral of the tangential component of the magnetic field integrated over the surface 5 , while the iast term expresses the difference of the voiume integrals of the electric field at the beginning and at the end of the time interval T.

The determination of an average charge-current density $J_v(R)$ thus demands the measurement of a field flux through the boundary S of the space-time region R. The approach to the problem of such measurement must rationally start from the consideration of the average flux over a thin four-dimensional shell situated at the boundary S, and which for simplicity we shall assume to have a constant thickness in space-time. As in the situation met with in the measurement of an average field component $F_{\mu v}(R)$, we shall require for this purpose a system of movable test bodies, filling the space which belongs to the shell at any time with an appropriate uniform charge-current distribution, and whose field actions are ordinarily neutralized by a distribution of opposite sign on fixed, penetrable, auxiliary bodies. For the measurement of an average charge density J_4, it suffices to take a set of test bodies with a uniform charge distribution of density ρ_4, while in the measurement of a current component, J_l, we shall have to use, besides such test bodies, another independent set of freely movable test bodies with a uniform current distribution ρ_i parallel to the current component to be measured.

In the measurement of an average charge density, the estimation of the flux over the shell demands the determination of the algebraic sum of the momenta transferred to the test bodies in the direction of the normal to the instantaneous spatial boundary. The evaluation of this sum, however, does not require independent measurements of the momenta transferred to the individual test bodies within the time intervals during which their positions belong to the space-time shell, but can be obtained by a composite measuring process in which the positions of all test bodies are correlated by suitable devices to secure during these intervals a displacement of every test body in the nomal direction by the same amount. By choosing the product of the thickness of the shell and the charge density of the test bodies sufficiently large, it is possible to keep the uncontrollable common displacement D of all the test bodies in the normal direction arbitrarily small, and still to obtain unlimited accuracy for the average flux over the shell. Like in the measurement of a simple field average, it is further possible to achieve an automatic compensation of

the uncontrollable contribution to this average flux, due to the fields created by the displacement of the test bodies, and proportional to $\bar{D}\rho_4$. This compensation will even be complete, in the initial approximation considered, because the field fluctuations, owing to their source-free character, do not give any contribution to the flux. Since these considerations hold for any given thickness of the shell, it is in principie possible, in the asymptotic limit of a sharp boundary, to measure accurately the average charge density within a well-defined space-time region.

In measurements of an average current component J_l, we have to take into account the magnetic circulation as well as the electric field in the space-iime shell. Thus, in the special case in which R is defined by a snatial extension V and a time interval T, we have to do, according to (6), not only with a contribution from the time average over T of the magnetic circulation around the direction l within a thin spatial sheil on the boundary of V, but also with a contribution representing the difference between the volume integrals over V of the electric field component in the direction l, averaged over two short time invervals at the beginning and at the end of the interval T. The evaluation of these contributions requires measuring proccdures of a similar kind as those described above in the case of measurements of simple field averages. While the measurement of the latter contribution demands the control of the momentum in the direction l transferred to a set of test bodies with uniform change density ρ, the evaluation of the former contribution demands the control of the momentum normal to the spatial boundary transferred to another set of test bodies with uniform current density ρ_l.

Just as in the field or change measurements discussed above, all these operations can be correlated in such a way that the determination of the algebraic sum of the momenta transferred to each test body within the time interval and in the direction required can be reduced to the momentum control of some supplementary body. In such a correlation, all the test bodics of charge density ρ will be subjected during the appropriate time intervals to the same displacement D_l and all the test bodies of current density ρ_l to the same normal displacement D. The interpretation of the current measurement requires further the establishment of a correlation between these two displacement, satisfying the condition $\rho D_l = \rho_l D$. Under such circumstances, it is possible, by choosing ρ and ρ_l sufficiently large, to achieve that the displacements D_l and D be arbitrarily
small without imposing any limitation upon the accuracy of the measurement. Moreover, it is possible, by suitable mechanical devices of the kind already meniioned, to obtain a compiete automatic elimination of the uncontrollable contributions from the operation of the test bodies to the average current to be measured.

It need hardly be added that the procedure can be extended to quite general space-time regions R, by using an arrangement in which each test body is displaced just in the time interval during which its position belongs to the space-time shell surrounding the region R. In this connection, it may be noted that a compendious four-dimensional description of ali ine measuring processes pertaining to charge-current components involves a uniform four-vector current distribution in the shell, parallel to the charge-current component to be measured.

Like in charge measurements, all the considerations concerning current measurements are independent of the thickness of the shell, and in principle it is therefore possible, in the initial approximation considered, to determine with unlimited accuracy any average charge-current component $J_v(R)$ within a sharply bounded region R. As regards charge-current measurements over two space-time regions, it can easily be seen that, in the limiting case of sharp boundaries, all field actions accompanying the flux measurements will vanish at any point of space-time which does not belong to the boundaries. In conformity with the formalism, there will therefore, to the approximation concerned, be no mutual influence of measurements of average charge-current densities in different space-time regions.

The situation so far described is of course merely an illustration of the compatibility of a consistent mathematical scheme with a strict application of the definition of the physical concepts

to which it refers, and is in particular quite independent of the question of the possibility of actually constructing and manipulating test bodies with the required properties. The distegard of all limitations in this respect, which may originate in the atomic constitution of matter, is, however, entirely justified when dealing with quantum electrodynamics in the initial stage of approximation. In fact, at this stage, the formalism is essentially independent of space-time scale, since it contains only the universal constants c and $\hbar$ which alone do not suffice to define any quantity of the dimensions of a length or time interval.

27.4.3 3. Charge-current Measurements in Pair Theory

New aspects of the problem of measurements arise in quantum electrodynamics in the next approximation, in which effects proportional to e^z/hc are taken into consideration, and where we meet with additional features connected with electron pair production induced by the electromagnetic fields. For the commutation rules of the field components, this means in general only a smaller modification expressed by additional terms containing $e^2/\hbar\bar{h}$ c. The charge-current quantities, however, wiii no longer be commutable but will obey commutation relations of the form.

(7) $\quad [J_v(R), J_\mu(R')] = i\hbar c\,[B_{v\mu}(R, R') - B_{\mu v}(R', R)],$

where the expressions $\bar{B}_{v\mu}\left(\bar{K}, \bar{K}'\right)$ are integrals of singuiar functions over the regions R and R'. In contrast to the quantities $A_{\mu\nu,\kappa\hat{i}}(R, R')$ occurring in (2), which depend only on simple spatio-temporal characteristics of the problem, the B's will, however, besides such characteristics, also essentially involve the length h/mc and the period h/mc^2, related to the electron mass m.

To approach the problem of the measurability of a charge-current quantity $J_v(R)$ in this approximation, we must again consider systems of electrified test bodies operated in a space-time sheil on the boundary of the region R, but we shall now have to examine the effect of the chargecurrent density appearing as a consequence of actual or virtual electron pair production by the field action of the displacement of the test bodies during the measuring process. As we shaii see, these effects, which are inseparably connected with the measurements, do not in any way limit the possibilities of testing the theory. [6]

In the first place, the average effect of the polarization of the vacuum by virtual and actual pair production in the measuring process can be eliminated by a compensation arrangement like that previously described. It is true that a direct estimate of these polarization effects in quantum electrodynamics involves divergent expressions which can only be given finite values by some renormalization or regularization procedure. [7] By such a procedure the average polarization effects will give rise to a contribution to the charge current density which is proportional to the common displacement of the test bodies. Thus in the limit of a sharp boundary of the region R we get, denoting the surface polarization on the
boundary by P_v, the expression $RP_vB_{\mu v}(R, R)$, where the last factor represents the value of $B_{\mu v}(R, R')$ in (7) for coinciding space-time extensions.

Moreover, the statistical effects caused by actual production of electron pairs in the measurement process are inseparably connected with the interpretation of the fluctuations of average charge-current densities in quantum electrodynamics. While the mean square deviation of the field component $F_m(R)$ over a sharply bounded space-time region R has a finite value, finite mean-square fluctuations of charge-current quantities can only be obtained, however, by further averaging over an ensemble of regions R whose boundaries are allowed a certain latitude around some given surface. [8]

This feature finds its exact counterpart in the estimate of the statistical effects of the real pairs which are produced in measurements of chargecurrent quantitics by the indicated procedure. In fact, the mean square fluctuation of an average flux will increase indefinitely with decreasing thickness of the shell in which the test bodies are operated, in just the same

way as, according to the formalism, the mean-square fluctuation of the corresponding charge-current density will vary with the latitude of the ensemble of space-time extensions over which the averaging is performed. The appearance of an infinite mean-square fluctuation in a sharply limited space-time region is in no way connected with the divergencies which appear in vacuum polarization effects but is a direct consequence of the fundamental assumptions of the theory, according to which the electrons are regarded as point charges.

In the case of measurements of charge-current averages over two spacetime regions, it can be shown that the polarization effects of the manipulation of the test bodies used for the measurement of $J_v(R)$ will give rise, in the limit of sharp boundaries, to a contribution to the average chargecurrent density component of index μ in the region R', equal to the product of the quantity $\boldsymbol{R}_{\mu v}(\boldsymbol{R}', \boldsymbol{R})$ occurring in formula (7) with $\boldsymbol{R}\boldsymbol{P}_v$, where P_v is the surface polarization created on the boundary of R during the measuring process. Conversely, the measurement of $J_\mu(R')$ will give a contribution $R'P'_\mu B_{\nu\mu}(R, R')$ to the average charge-current density of index v in R. By similar compensation devices as required for two field measurements, it is therefore possible, as readily seen, to obtain an accuracy of measurements of average charge-current densities in two
space-time regions subject only to the reciprocal limitation expressed by the commutation relation (7).

27.4.4 4. Concluding Remarks

The conformity of the formalism of quantum electrodynamics with the interpretation of idealized field and charge measurements has of course no immediate relation to the question of the scope of the theory and of the actual possibility of measuring the physical quantities with which it deals.

In the present state of atomic physics, the problem of an actual limita tion of measurements interpreted by means of the concepts of classical electrodynamics can hardly be fully explored. Still, in view of the great success of quantum electrodynamics in accounting for numerous phenomena, the formal interpretation of which involves spacetime coordination of electrons within regions of dimensions far smaller than $\hbar/mc$ and $\hbar/mc^2$, it may be reasonable to assume that measurements within such regions are in principle possible Indeed, the comparatively heavy and highly charged test bodies of such small dimensions and operated over such short time intervals. which would be required for these measurements, might be conceived to be built up of nuclear particles.

Yet, an ultimate limitation of the consistent application of the formalism is indicated by the necessity of introducing forces of short range in nuclear theory, with no analog in classical electrodynamics, and by the circumstance that the ratio between the electron mass and the rest mass of the quanta of the nuclear field has the same order of magnitude as the fundamental parameter $e^2/\hbar c$ of quantum electrodynamics. [9] The further exploration of such problems may, however, demand a radical revision of the foundation for the application of the basic dual concepts of fields and particles.

NOTES

[1] S. Tomonaga, Prog. Theor. Phys. 1 (1946), 27; Phys. Rec. 74 (1948), 224. J. Schwinger, Phis. Rev. 74 (1948), 1439; 75 (1949), 651 : 75 (1949), 1912: 76 (1949), 790. F. Dyson, Phis. Ret. 75 (1949), 486; 75 (1949), 1736. R. Feynman, Phys. Ret. 76 (1949), 749; 76 (1949), 769.
[2] N Bohr and L. Rosenfeld, Kal. Danske Vid. Seis., Math.-fis. Medd. 12 (1933), No. 8. This paper will be referred to in the following as 1 . [English translation: this volume. p. 35 . [3] An account of the preliminary results of the investigation, which were discussed at several physical conferences in 1938, has recently been included in the monograph by
A. Pais, Decelopments in the Theory of the Electron, Princeton University Press, Princeton,

New Jersey, 1948.
[4] The bearing of this development on the elucidation of the problem of measurability was brought to the attention of the writers in a stimulating correspondence with Professor Pauli. [3] A more detailed account of the subject with fuller references to the literature will appear later in the Communications of the Copenhagen Academy.

- in a paper by Halpenn and Johnson, Rhys. Rect. 59 (1941), 896, arguments are brought forward pointing to a far more restrictive limitation of the field and charge measurements. In these arguments, however, no sufficient separation is made between such actions of the charged test bodies as are directly connected with their use in the measuring procedure and those actions which can be eliminated by appropriate neutralization by auxiliary bodies of opposite charge.
[7] Cf. W. Pauli and F. Villars, Rev. Mod. Phys. 21 (1949), 434.
[8] Cf. W. Heisenberg, Leipziger Ber. 96 (1934), 317. We are indebted to Drs Jost and Luttinger for information about their more precise evaluation of charge-current fluctuations, showing that the unimited increase of the chaige-cuitent fluctuations in a spacetime region with decreasing latitude in the fixation of its boundary involves only the logarithm of the ratio between the linear dimensions of the region and the width of this latitude. Even a latitude very small compared with $\hbar/mc$ will therefore imply no excessive effect of the charge fluctuations. A situation entirely similar in all such respects to that in electron methy with dealing with electrical particles mese statistics. We are indebted to Dr. Corinaldesi for the comeffects in a pach a production [9] Cffects in such a theory.
[9] Cf., e.g.. N. Bohr, Report of the Solvay Council (1948).

28 V Irreversibility and Quantum Theory

Commentary of Behavioral Science (1964)

In memory of Leo Szilard, who passed away on May 30, 1964, we present an English translation of his classical paper ber die Entropieverminderung in einem thermodynamischen System bei Eingriffen intelligenter Wesen, which appeared in the Zeitschrift fr Physik, 1929, 53, 840-856. The publication in this journal of this translation was approved by Dr. Szilard before he dicd, but he never saw the copy. At Mrs. Szilard's request, Dr. Carl Eckart revised the translation.

This is one of the earliest, if not the earliest paper, in which the relations of physical entropy to information (in the sense of modern mathematical theory of communication) were rigorously demonstrated and in which Maxwell's famous demon was successfully exorcised: a milestone in the integration of physical and cognitive concepts.

28.1 V.1 On the Decrease of Entropy in a Thermodynamic System by the Intervention of Intelligent Beings by Szilard

Translated by Anatol Rapoport and Mechthilde Knoller from the original article "Uber die Entropieverminderwng in cinem thermodynamischen System bei Wingriffen intelligenter Wesen " Zuitschrift fr Physik, 1929, 53, 840-856.

∞

The objective of the investigation is to find the conditions which apparently allow the construction of a perpetual-motion machine of the second kind, if one permits an intelligent, being to intervene in a thermodynamic system. When such beings make measurements, they make the system behave in a manner distinctly different from the way a mechanical system behaves

when left to itself. We show that it is a sort of a memory faculty, manifested by a system where measurements occur, that might cause a permanent decrease of entropy and thus a violation of the Second Law of Thermodynamics, were it not for the fact that the measurements themselves are necessarily accompanied by a production of entropy. At first we calculate this production of entropy quite generally from the postulate that full compensation is made in the sense of the Second Law (Equation [1]). Seop using an inanimate device able a measurements-however under continual entropy production-we shall calculate the resulting quantity of entropy. We find that it is exactly as great as is necessary for full compensation. The actual production of entropy in connection with the measurement, therefore, need not be greater than Equation (1) requires.

T[1]here is an objection, already historical, against the universal validity of the Second Law of Thermodynamics, which indeed looks rather ominous. The objection is embodied in the notion of Maxwell's demon, who in a different form appears even nowadays again and again; perhaps not unreasonably, inasmuch as behind the precisely formulated question quantitative connections seem to be hidden which to date have not been clarified. The objection in its origino nal formulation concerns a demon who catches the fast molecules and lets the slow ones pass. To be sure, the objection can be met with the reply that man cannot in principle foresee the value of a thermally fluctuating parameter. However, one cannot deny that we can very well measure the value of such a fluctuating parameter and therefore could certainly gain energy at the expense of heat by arranging our interven-
tion areording to the results of the measurements. Presently, of course, we do not know whether we commit an error by not including the intervening man into the system and hy discegarding his biological phenomena.

Apart from this unuesolved matter, it is known today that in a system left to itself no "perpetuum mobile" (perpetual motion machine) of the second kind (more exactly, no "automatic machine of continual finite work-yield which uses heat at the lowest temperature") can operate in spite of the fluctuation phenomena. A perpetuum mobile would have to be a machine which in the long run could lift a weight at the expense of the heat content of a reservoir. In other words, if we want to use the fluctuation phenomena in order to gain energy at the expense of heat, we are in the same position as playing a game of chance, in which we may win certain amounts now and then, although the expectation value of the wimings is zero or negative. The same applies to a system where the intervention from outside is performed strictly periodically, say by periodically moving machines. We consider this as established (Szilard, 192.5) and intend here only 10 ronsider the difficulties that occur when intelligent beings intervene in a system. We shall try to discover the quantitative relations having to do with this intervention.

Smoluchowski (1914, p. 89) writes: "As far as wo know today, there is no automatic, permanently effective perpetual motion machine, in spite of the molecular fluctuations, but surfl a device might, perhaps, function regularly if it were appropriately operated by intelligent beings...."

A perpetual motion machine therefore is possible if-according to the general method of physics-we view the experimenting man as a sort of deus e.r machina, one who is continuously and exactly informed of the existing state of nature and who is able to start or interrupt the macroscopic course of nature at any moment without expenditure of work. Therefore he would definitely not have to possess the ability to catch single molecules like Maxwell's demon, although he would definitely be different from real living beings in possessing the above abilities. In eliciting any physical effect by action of the sensory
as well as the motor nervous systems a degradation of energy is always involved, quite apart from the fact that the very existence of a nervous system is dependent on continual dissipation of energy.

Whether considering these circum-stances-real living beings could continually or at least

regularly produce energy at the expense of heat of the lowest temperature appears very doubtful, even though our ignorance of the biological phenomena dees not allow a definite answer. However, the latter questions lead beyond the scope of physics in the strict sense.

It appears that the ignorance of the biological phenomena need not prevent us from understanding that which seems to us to be the essential thing. We may be sure that intelligent living beings-insofar as we are dealing with their intervention in a thermodynamic system-can be replaced by nonliving devices whose "biological phenomena" one could follow and determine whether in fact a compensation of the entropy decrease takes place as a result of the intervention by such a device in a system.

In the first place, we wish to learn what circumstance conditions the decrease of entropy which takes place when intelligent living beings intervene in a thermodynamic system. We shall see that this depends on a certain type of coupling between different parameters of the system. We shall consider an unusually simple type of these ominous couplings. [1] For brevity we shall talk about a "measurement," if we succeed in coupling the value of a parameter y. (for instance the position co-ordinate of a pointer of a measuring instrument) at one moment with the simultaneous value of a fluctuating parameter x of the system, in such a way that, from the value y, we can draw conclusions about the value that x had at the moment of the "measurement." Then let x and y be uncoupled after the measurement, so that x can change, while y retains its value for some time. Such measurements are not harmless interventions. A system in which such measurements occur shows a sort of memory

faculty, in the sense that one can recognize by the state parameter y what value another state parameter x had at an earlier moment, and we shall see that simply because of such a memory the Second Law would be violated, if the measurement could take place without compensation. We shall realize that the Second Law is not threatened as much by this entropy decrease as one would think, as soon as we see that the entropy decrease resulting from the intervention would be compensated completely in any event if the execution of such a measurement were, for instance, always accompanied by production of $k \log 2$ units of entropy. In that case it will be possible to find a more general entropy law, which applies universally to all measurements. Finally we shall consider a very simple (of course, not living) device, that is able to make measurements continually and whose "biological phenomena" we can casily follow. By direct calculation, one finds in fact a continual entropy production of the magnitude required by the abovementioned more general entropy law derived from the validity of the Second Law.

The first example, which we are going to consider more closely as a typical one, is the following. A standing hollow cylinder, closed at both onds, can bo separated into two possibly unequal sections of volumes V_1 and V_2 respectively by inserting a partition from the side at an arbitrarily fixed height. This partition forms a piston that can be moved up and down in the cylinder. An infinitely large heat reservoir of a given temperature T insures that any gas present in the cylinder undergoes isothermal expansion as the piston moves. This gas shall consist of a single molecule which, as long as the piston is not inserted into the cylinder, tumbles about in the whole cylinder by virtue of its thermal motion.

Imagine, specifically, a man who at a given time inserts the piston into the cylinder and somehow notes whether the molecule is caught in the upper or lower part of the cylinder, that is, in volume F_1 or F_2. If he should find that the former is the case, then he would move the piston slowly downward until it reaches the bottom of the cylinder. During this slow movement of the piston the molecule stays, of course, above the piston.

However, it is no longer constrained to the upper part of the cylinder but bouners many times against the piston which is already moving in the lower part of the evlinder. In this way the molecule does a certain amount of work on the piston. This is the work that corresponds to

[81] The author evidently uses the word "ominous" in the sense that the possibility of realizing the proposed arrangement threatens the validity of the Second Law.-Translator

the isothermal expansion of an ideal gas-consisting of one single mole-cule-from volume $\bar{V}_1$ to the volume $V_1 + V_2$. After some time, when the piston has reached the bottom of the container, the molecule has again the full volume $V_1 + I_2$ to move about in, and the piston is then removed. The procedure can be repeated as many times as desired. The man moves the piston up or down depending on whether the molecule is trapped in the upper or lower half of the piston. In more detail, this motion may be caused by a weight, that is to be raised, through a mechanism that transmits the force from the piston to the weight, in such a way that the latter is always displaced upwards. In this way the potential energy of the weight certainly increases constantly. (The transmission of force to the weight is best arranged so that the force exerted by the weight on the piston at any position of the latter equals the average pressure of the gas.) It is clear that in this manner energy is constantly gained at the expense of heat, insofar as the liological phenomena of the intervening man are ignored in the calculation.

In order to understand the essence of the man's effect on the system, one best imagines that the movement of the piston is performed mechanically and that the man's activity consists only in determining the altitude of the molecule and in pushing a lever (which steers the piston) to the right or left, depending on whether the molecule's height requires a down- or upward movement. This means that the intervention of the human being consists only in the coupling of two position eo-ordinates, namely a co-ordinate r, which determines the altitude of the molecule, with another co-ordinate y, which determines the position of the lever and therefore also whether an upward or downward motion is imparted to the piston. It is best to imagine the mass of the piston as large and its speed sufficiently great, so that the thermal agitation of the piston at the temperature in question can he neglected.

In the typical example presented here, we wish to distinguish two periods, namely:

1. The period of measurement when the piston has just been inserted in the middle of the cyluder and the molecule is trapped either in the upper or lower part; so that if we choose the origin of co-ordinates appropriately, the x-co-ordinate of the molecule is restricted to either the interval $x > 0$ or $.c < 0$;

2. The period of utilization of the measurement, "the period of decrease of entropy," during which the piston is moving up or down. During this period the x-co-ordinate of the modecule is certainly not restricted to the original interval $x > 0$ or $x < 0$. Rather, if the molecule was in the upper half of the cylinder during the period of measurement, i.e., when $x > 0$, the molecule must bounce on the downward-moving piston in the lower part of the cylinder, if it is to transmit energy to the piston; that is, the co-ordinate x has to enter the interval $x < 0$. The lever, on the contrary, retains during the whole period its position toward the right, corresponding to downward motion. If the position of the lever toward the right is designated by : $t = 1$ (and correspondingly the position toward the left by $y = -1$) we see that during the period of measurement, the position $x > 0$ corresponds to $y = 1$; but afterwards $y = 1$ stays on, even though x passes into the other interval $x < 0$. We see that in the utilization of the measurement the coupling of the two parameters x and y disappears.

We shall say, quite generally, that a parameter "measures" a parameter x (which varies according to a probability law), if the value of " 1 is directed by the value of parameter x at a given moment. A measurement procedure underlies the entropy decrease effected by the intervention of intelligent beings.

One may reasonably assume that a measurement proredure is fundamentally associated with a certain definite average entropy production, and that this restores concordance with the Second Law. The amount of entropy generated by the measurement may, of course, always be greater than this funda-

mental amount, but not smaller. To put it precisely: we have to distinguish here between two entropy values. One of them, $\bar{S}_1$, is produced when during the measurement y assumes the value 1 , and the other, $\bar{S}_2$, when y assumes the value -1 . We cannot expect to get general information about $\overline{S_1}$ or $\overline{S_2}$ separately, but we shall see that if the amount of entropy produced by the "measurement" is to compensate the entropy decrease affected by utilization, the relation must always hold good.

$$e^{-\bar{s}_1/k} + e^{-\bar{s}_2/k} \leqq 1 \tag{1}$$

One sees from this formula that one can make one of the values, for instance $\overline{S_1}$, as small as one wishes, but then the other value $\overline{S_2}$ becomes correspondingly greater. Furthermore, one can notice that the magnitude of the interval under consideration is of no consequence. One can also easily understand that it cannot be otherwise.

Conversely, as long as the entropies $\overline{S_1}$ and $\bar{S}_2$, produced by the measurements, satisfy the inequality (1), we can be sure that the expected decrease of entropy caused by the later utilization of the measurement will be fully compensated.

Before we proceed with the proof of inequality (1), let us see in the light of the above mechanical example, how all this fits together. For the entropies $\overline{S_1}$ and $\overline{S_2}$ produced by the measurements, we make the following Ansatz:

$$\bar{S}_1 = \bar{S}_2 = k \log 2 \tag{2}$$

This ansatz satisfies inequality (1) and the mean value of the quantity of entropy produced by a measurement is (of course in this special case independent of the frequencies w_1, w_2 of the two events):

$$\bar{S} = k \log 2 \tag{3}$$

In this example one achieves a decrease of entropy by the isothermal expansion:-

$$\begin{aligned} -\bar{s}_1 &= -k \log \frac{V_1}{V_1 + V_2}; \\ -\bar{s}_2 &= -k \log \frac{V_2}{V_1 + \Gamma_2} \end{aligned} \tag{4}$$

[2] The entropy generated is denoted by $\bar{s}_1, \bar{s}_2$.

depending on whether the molecule was found in volume V_1 or V_2 when the piston was inserted. (The decrease of entropy equals the ratio of the quantity of heat taken from the heat reservoir during the isothermal expansion, to the temperature of the heat reservoir in question). Since in the above case the frequencies w_1, w_2 are in the ratio of the volumes V_1, V_2, the mean value of the entropy generated is (a negative number):

$$\begin{aligned} &\bar{s} = w_1 \cdot (+\bar{s}_1) + w_2 \cdot (+\bar{s}_2) = \\ &\frac{T_1}{Y_1 + V_2} k \log \frac{V_1}{V_1 + V_2} + \\ &\frac{V_2}{V_1 + V_2} l \log \frac{V_1}{V_1 + V_2} \end{aligned} \tag{5}$$

As one can see, we have, indeed

$$\begin{aligned} &\tfrac{V_1}{V_1+V_2} l_1 \log \tfrac{V_1}{V_1+V_2} + \tfrac{V_2}{V_1+\Gamma_2} \\ &\cdot l_1 \log \tfrac{V_2}{\Gamma_1+V_2} + k \log 2 \geqq 0 \end{aligned} \tag{6}$$

and therefore:

$$\bar{S} + \bar{s} \geqq 0. \tag{7}$$

In the special case considered, we would actually have a full compensation for the deerrase of entropy achieved by the utilization of the measurement.

We shall not examine more special cases, but instead try to clarify the matter by a general argument, and to derive formula (1). We shall therefore imagine the whole sys-tem-in which the co-ordinate x, exposed to some kind of thermal fluctuations, can be measured by the parameter y in the way just explained -as a multitude of particles, all enclosed in one box. Every one of these particles can move freely, so that they may be considered as the molecules of an ideal gas, which, because of thermal agitation, wander about in the common box independently of each other and exert a certain pressure on the walls of the box-the pressure being determined by the temperature. We shall now consider two of these molecules as chemically different and, in principle, separable by semipermeable walls, if the co-ordinate x for one molecule is in a preassigned interval while the corresponding co-ordinate of the other molecule falls outside that interval. We
also shall look upon them as chemically different, if they differ only in that the y coordinate is $+1$ for one and -1 for the other.

We should like to give the box in which the "molecules" are stored the form of a hollow cylinder containing four pistons. Pistons A and A' are fixed while the other two are movable, so that the distance BB' always equals the distance AA', as is indicated in Figure 1 by the two brackets. A', the bottom, and B, the cover of the container, are impermeable for all "molecules," while A and B' are semipermeable; namely, A is permeable only for those "molecules" for which the parameter x is in the preassigned interval, i.e., (x_1, x_2), B' is only permeable for the rest.

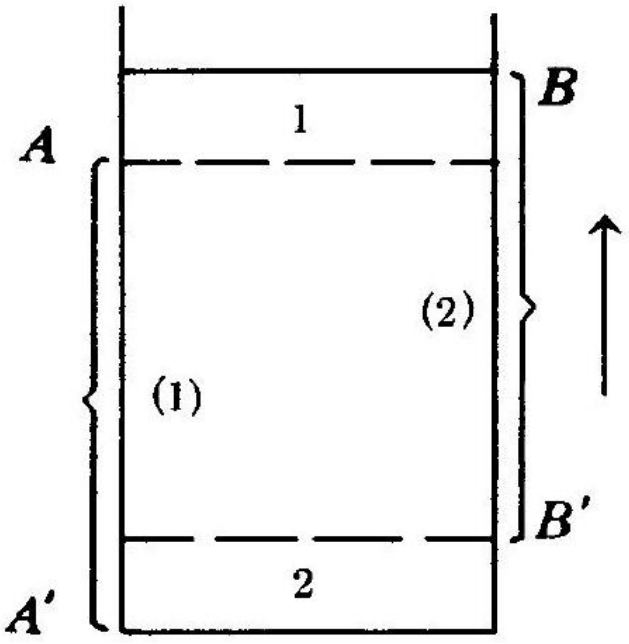


Fig. 1

In the beginning the piston B is at A and therefore B' at A', and all "molecules" are in the space between. A certain fraction of the molecules have their co-ordinate x in the preassigned interval. We shall designate by w_1 the probability that this is the case for a randomly selected molecule and by w_2 the probability that x is outside the interval. Then $w_1 + w_2 = 1$.

Let the distribution of the parameter y be over the values +1 and -1 in any proportion but in any event independent of the x-values. We imagine an intervention by an intelligent being, who imparts to y the value 1 for all "molecules" whose x at that moment is in the selected interval. Otherwise the value -1 is assigned. If then, because of thermal fluctuation, for any "molecule," the parameter x should come out of the preassigned interval or, as we also may put it, if the "molecule" suffers a monomolecular chemical reaction with regard to x (by which tion of the piston at the temperature in question can he neglected.

In the typical example presented here, we wish to distinguish two periods, namely:

1. The period of measurement when the piston has just been inserted in the middle of the cylinder and the molecule is trapped either in the upper or lower part; so that if we choose the origin of co-ordinates appropriately, the x-co-ordinate of the molecule is restricted to either the interval $x > 0$ or $.c < 0$;

2. The period of utilization of the measurement, "the period of decrease of entropy," during which the piston is moving up or down. During this period the x-co-ordinate of the molecule is certainly not restricted to the original interval $x > 0$ or $x < 0$. Rather, if the molecule was in the upper half of the cylinder during the period of measurement, i.e., when $x > 0$, the molecule must bounce on the downward-moving piston in the lower part of the cylinder, if it is to transmit energy to the piston; that is, the co-ordinate x has to enter the interval $x < 0$. The lever, on the contrary, retains during the whole period its position toward the right, corresponding to downward motion. If the position of the lever toward the right is designated by $:|= 1$ (and correspondingly the position toward the left by $y - -1$) we see that during the period of measurement, the position $x > 0$ corresponds to $y = 1$; but afterward: $y = 1$ stays on, cven though x passes into the other interval $x < 0$. We see that in the utilization of the measurement the coupling of the two parameters x and y disappears.

We shall say, quite generally, that a parameter " "neasures" a parameter x (which varies according to a probability law), if the value of (???) is directed by the value of parameter x at a given moment. A measurement procedure underlies the entropy decrease effected by the intervention of intelligent beings.

One may rasonably assume that a measurement procedure is fundamentally associated with a certain definite average entropy production, and that this restores concordance with the Second Law. The amount of entropy generated by the measurement may, of course, always be greater than this funda-
mental amount, but not smaller. To put it precisely: we have to distinguish here between two entropy values. One of them, $\bar{S}_1$, is produced when during the measurement y assumes the value 1 , and the other, $\bar{S}_2$, when y assumes the value -1 . We cannot expect to get general information about $\bar{S}_1$ or $\bar{S}_2$ separately, but we shall see that if the amount of entropy produced by the "measurement" is to compensate the entropy decrease affected by utilization, the relation must always hold good.

$$e^{-\bar{s}_1/k} + e^{-\bar{s}_2/k} \leqq 1 \tag{1}$$

One sees from this formula that one can make one of the values, for instance $\bar{S}_1$, as small as one wishes, but then the other value $\vec{S}_2$ becomes correspondingly greater. Furthermore, one can notice that the magnitude of the interval under consideration is of no consequence. One can also easily understand that it camot be otherwise.

Conversely, as long as the entropies $\overline{S_1}$ and $\bar{S}_2$, produced by the measurements, satisfy the inequality (1), we can be sure that the expected decrease of entropy caused by the later utilization of the measurement will be fully compensated.

Before we proceed with the proof of inequality (1), let us see in the light of the above mechanical example, how all this fits together. For the entropies $\bar{S}_1$ and $\bar{S}_2$ produced by the measurements, we make the following Ansatz:

$$\bar{S}_1 = \bar{S}_2 = k \log 2 \tag{2}$$

This ansatz satisfies inequality (1) and the mean value of the quantity of entropy produced by a measurement is (of course in this special case independent of the frequencies w_1, w_2 of the two events):

$$\bar{S} = k \log 2 \tag{3}$$

In this example one achieves a decrease of entropy by the isothermal expansion:-

$$\begin{aligned} -\bar{s}_1 &= -k \log \frac{V_1}{V_1 + V_2}; \\ -\bar{s}_2 &= -k_i \log \frac{\Gamma_2}{V_1 + \Gamma_2}, \end{aligned} \tag{4}$$

[2] The entropy generated is denoted by $\bar{s}_1, \bar{s}_2$.
depending on whether the molecule was found in volume V_1 or V_2 when the piston was inserted. (The decrease of entropy equals the ratio of the quantity of heat taken from the heat reservoir during the isothermal expansion, to the temperature of the heat reservoir in question). Since in the above case the frequencies w_1, w_2 are in the ratio of the volumes I_1, V_2, the mean value of the entropy generated is (a negative number):

$$\begin{aligned} &\bar{s} = w_1 \cdot (+\bar{s}_1) + w_2 \cdot (+\bar{s}_2) = \\ &\frac{V_1}{V_1 + V_2} k \log \frac{V_1}{V_1 + V_2} + \\ &\frac{V_2}{V_1 + V_2} k \log \frac{V_1}{V_1 + V_2} \end{aligned} \tag{5}$$

As one can see, we have, indeed

$$\begin{aligned} &\tfrac{\Gamma_1}{\Gamma_1 + V_2} l \cdot \log \tfrac{V_1}{\Gamma_1 + V_2} + \tfrac{V_2}{V_1 + \Gamma_2} \\ &\cdot l \cdot \log \tfrac{V_2}{\Gamma_1 + V_2} + k \log 2 \geqq 0 \end{aligned} \tag{6}$$

and therefore:

$$\bar{S} + \bar{s} \geqq 0 \tag{7}$$

In the special case considered, we would actually have a full compensation for the decrease of entropy achieved by the utilization of the measurement.

We shall not examine more special cases, but instead try io clarify the matter by a general argument, and to derive formula (1). We shall therefore imagine the whole sys-tem-in which the co-ordinate x, exposed to some kind of thermal fluctuations, can be measured by the parameter y in the way just explained -as a multitude of particles, all enclosed in one box. Every one of these particles can move freely, so that they may be considered as the molecules of an ideal gas, which, because of thermal agitation, wander about in the common box independently of each other and exert a certain pressure on the walls of the box-the pressure being determined by the temperature. We shall now consider two of these molecules as chemically different and, in principle, separable by semipermeable walls, if the co-ordinate x for one molecule is in a

preassigned interval while the corresponding co-ordinate of the other molecule falls outside that interval. We
also shall look upon them as chemically different, if they differ only in that the y coordinate is $+1$ for one and -1 for the other.

We should like to give the box in which the "molecules" are stored the form of a hollow cylinder containing four pistons. Pistons A and A' are fixed while the other two are movable, so that the distance BB' always equals the distance AA', as is indicaled in Figure 1 by the two brackets. A', the bottom, and B, the cover of the container, are impermeable for all "molecules," while A and B' are semipermeable; namely, A is permeable only for those "molecules" for which the parameter x is in the preassigned interval, i.e., (x_1, x_2), B' is only permeable for the rest.

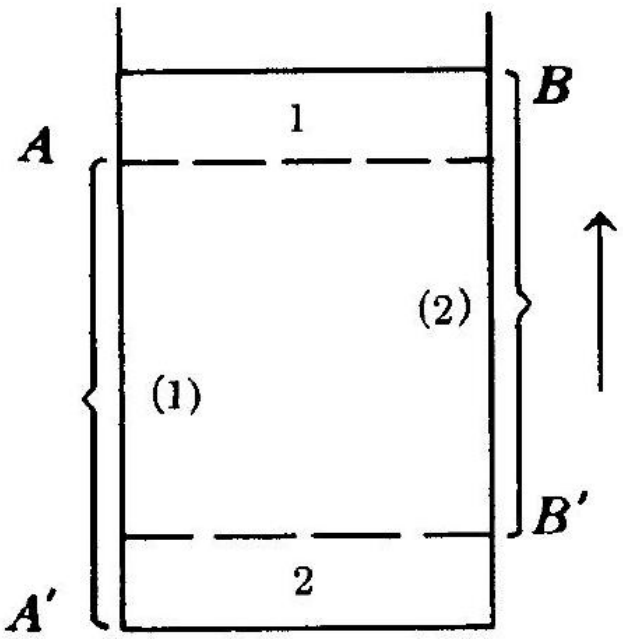


Fig. 1

In the beginning the piston B is at A and therefore B' at A', and all "molecules" are in the space between. A certain fraction of the molecules have their co-ordinate x in the preassigned interval. We shall designate by w_1 the probability that this is the case for a randomly selected molecule and by w_2 the probability that x is outside the interval. Then $w_1 + w_2 = 1$.

Let the distribution of the parameter y be over the values $+1$ and -1 in any proportion but in any event independent of the x-values. We imagine an intervention by an intelligent being, who imparts to y the value 1 for all "molecules" whose x at that moment is in the selected interval. Otherwise the value -1 is assigned. If then, because of thermal fluctuation, for any "molecule," the parameter x should come out of the preassigned interval or, as we also may put it, if the "molecule" suffers a monomolecular chemical reaction with regard to x (by which it is transformed from a species that can pass the semipermeable piston A into a species for which the piston is impermeable), then the parameter y retains its value 1 for the time being, so that the "molecule," because of the value of the parameter y, "remmenter" during the whole following process that x originally was in the preassigned interval. We shall see immediately what part this memory may play. After the intervention just discussed, we move the piston, so that we separate the two kinds of molecules without doing work. This results in two containers, of which the first contains only the one modification and the second only the other. Each modification now occupies the same volume as the mixture did previously. In one of these containers, if considered by itself, there is now no equilibrium with regard to the

two "modifications in x." ()f course the ratio of the two modifications has remained $w_1 : w_2$. If we allow this equilibrium to be achieved in both containers independently and at constant volume and temperature, then the entropy of the system certainly has increased. For the total heat release is 0 , since the ratio of the two "modifications in x"$w_1 : w_2$ does not change. If we accomplish the equilibrium distribution in both containers in a reversible fashion then the entropy of the rest of the world will decrease by the same amount. Therefore the entropy increases by a negative value, and, the value of the entropy increase per molecule is exactly:

$$\bar{s} = k\left(w_1 \log w_1 + w_2 \log w_2\right). \tag{9}$$

(The entropy ronsiants that we must assign to the two "modifications in r " do not oreur here explicitly, as the process leaves the total number of molecules belonging to the one or the other species unchanged.)

Now of course we cannot bring the two gases back to the original volume without expenditure of work by simply moving the piston back, as there are now in the con-tainer-which is bounded by the pistons BB'-also molecules whose x-co-ordinate lies outside of the preassigned interval and for which the piston A is not permeable any longer. Thus one can see that the calculated decrease of entropy (Equation [9]) does not mean a contradiction of the Second Jaw. As long as we do not use the fact that the molecules in the container BB', by writue of their coordinate y, "remember" that the x-ordinate for the molecules of this container originally was in the preassigned interval, full compensation exists for the calculated deverase of entropy, by virtue of the fact that the partial pressures in the two containers are smaller than in the original mixture.

But now we can use the fact that all molecules in the conlainer BB' have the y-co-ordinate 1, and in the other accondingly -1 , to bring all molecules back again to the original volume. To accomplish this we only need to replace the semipermeable wall . I by a wall .*, which is semipermeable not with regard to x but with regard to y, mamely so that it is permeable for the molecules with the y-coordinate 1 and impermeable for the others. Correspondingly we replace B' by a piston B'^*, which is impermeable for the molecules with $y = -1$ and permeable for the others. Then both containers can be put into each other again without expenditure of energy. The distribution of the y-co-ordinate with regard to 1 and -1 now has become statistically independent of the u-values and besides we are able to re-establish the original distribution over 1 and -1 . Thus we would have gone through a complete cycle. The only change fhat we have to register is the resulting decrease of entropy given by (9):

$$\bar{s} = k\left(w_1 \log w_1 + u_2 \log u_2\right). \tag{10}$$

If we do not wish to admit that the Second Law has been violated, we must conclude that the intervention which catublishes the coupling between y and x, the measurement of x by y, must be accompanied by a production of entropy. If a definite way of achieving this coupling is adopted and if the quantity of entropy that is inevitably produced is designated by S_1 and S_2, where S_1 slands for the mean increase in entropy that occurs when y acquires the value 1 , and accordingly S_2 for the increase that occurs when y acquires the value -1 , we arrive at the equation:

$$w_1 \aleph_1 + w_2 \aleph_2 = \bar{S} \tag{11}$$

In order for the Second Law to remain in force, this quantity of cutropy must be greater than the decrease of entropy $\vec{s}$, which according to (9) is produced by the utilization of the measurement. Therefore the following unequality must be valid:

$$\begin{gathered}\bar{S}+\bar{s} \geqq 0 \\ w_1 S_1+w_2 S_2 \\ +l_2\left(w_1 \log w_1+w_2 \log w_2\right) \geqq 0\end{gathered} \tag{12}$$

This equation must be valid for any values of w_1 and w_2,[3] and of course the constraint $w_2+w_2=1$ cannot be violated. We ask, in particular, for which w_1 and w_2 and given $\therefore$-values the expression becomes a minimum. For the 1 wo minimizing values w_1 and w_2 the inequality (12) must still be valid. Under the above constraint, the minimum occurs when the following equation holds:

$$\frac{s_1}{l_i}+\log w_1=\frac{s_2}{l_i}+\log w_2 \tag{13}$$

But then:

$$e^{-i_1/k}+e^{-i_2 k} \leqq 1 \tag{14}$$

This is easily seen if one introduces the notation

$$\frac{S_1}{l_i}+\log w_1=\frac{S_2}{l_i}+\log w_2=\lambda \tag{15}$$

then:

$$w_1=c^\lambda \cdot c^{-\lambda_1 k}; \quad w_2-e^\lambda \cdot e^{-k_2 k} \tag{16}$$

If one substitutes these values into the inequality (1') one gets:

$$\lambda_c^\lambda\left(e^{-s_1/k}+e^{-s_2 k}\right) \geqq 0 \tag{17}$$

Therefore the following also holds:

$$\lambda \geqq 0 \tag{18}$$

If one puts the values w_1 and w_2 from (16) into the equation $w_1+w_2=1$, one gets

$$e^{-s_1/k}+e^{-s_2 k}=e^{-\lambda} \tag{19}$$

And because $\lambda \geqq 0$, the following holds:

$$e^{-S_1/k}+e^{-S_2/k} \leqq 1 \tag{20}$$

This equation must be universally valid, if thermodynamics is not to be violated.

As long as we allow intelligent beings to perform the intervention, a direct test is not possible. But we can try to describe simple nonliving devices that effect such coupling, and see if indeed entropy is generated and in what quantity. Having already recognized that the only important factor is a certain characteristic lype of coupling, a "measurement," we need not construct any complicated models which imitate the intervention of living beings in detail. We can be satisfied with the construction of this particular type of coupling which is accompanicd by memory.

In our next example, the position co-ordinate of an oscillating pointer is "measured" by the energy content of a body K. The pointer is supposed to connect, in a purely mechanical

[83] The increase in entropy can depend only on the types of measurement and their results but not on how many systems of one or the other type were present.

way, the body K-by whose energy content the position of the pointer is to be measured - by heat conduction with one of two intermediate pieces, A or B. The body is connected with A as long as the co-ordinate-which determines the position of the pointer-falls into a certain preassigned, but otherwise arbitrarily large or small interval a, and otherwise if the co-ordinate is in the interval b, with B. Up to a certain moment, namely the moment of the "measurement," both intermediate pieces will be themally comected with a heat reservoir at temperature T_0. At this moment the insertion A will be cooled reversibly to the temperature T_A, e.g., by a periodically functioning mechanical device. That is, after successive contacts with heat reservoirs of intermediate temperatures, A will be brought into contact with a heat reservoir of the temperature T_A. At the same time the insertion B will be heated in the same way to temperature T_B. Then the intermediate pieces will again be isolated from the corresponding heat reservoirs.

We assume that the position of the pointer changes so slowly that all the operations that we have sketched take place while the position of the pointer remains unchanged. If the position co-ordinate of the pointer foll in the preassigned interval, then the body was connected with the insertion A during the above-mentioned operation, and consequently is now cooled to temperature T_A.

In the opposite case, the body is now heated to temperature T_B. Its energy content becomes-according to the position of
the pointer at the time of "measurement"small at temperature T_A or great at temperature T_B and will retain its value, even if the pointer eventually leaves the preassigned interval or enters into it. After some time, while the pointer is still oscillating, one can no longer draw any definite conclusion from the energy content of the body K with regard to the momentary position of the pointer but one can draw a definite conclusion with regard to the position of the pointer at the time of the measurement. Then the measurement is completed.

After the measurement has been accomplished, the above-mentioned periodically functioning mechanical device should connect the thermally isolated insertions A and B with the heat reservoir T_0. This has the purpose of bringing the body K-which is now also connected with one of the two intermediate pieces-back into its original state. The direct commection of the intermediate pieces and hence of the body K-which has been either cooled to T_A or heated to T_B-to the reservoir T_0 consequently causes an increase of entropy. This cannot possibly be avoided, because it would make no sense to heat the insertion A reversibly to the temperature T_0 by successive contacts with the reservoirs of intermediate temperatures and to cool B in the same manner. After the measurement we do not know with which of the two insertions the body K is in contact at that moment; nor do we know whether it had been in connection with T_A or T_B in the end. Therefore neither do we know whether we should use intermediate temperatures between T_A and T_0 or between T_0 and T_B.

The mean value of the quantity of entropy S_1 and S_2, per measurement, can be calculated, if the heat capacity as a function of the temperature $\bar{u}(T)$ is known for the body K, since the entropy can be calculated from the heat capacity. We have, of course, neglected the heat capacities of the intermediate pieces. If the position co-ordinate of the pointer was in the preassigned interval at the time of the "measurement," and accordingly the body in connection with insertion A, then the entropy conveyed to the heat reservoirs during successive cooling was

$$\int_{T_A}^{r_9} \frac{1}{T} \frac{d\bar{u}}{dT} \tag{21}$$

However, following this, the entropy withdrawn from the reservoir T_0 by direct contact with it was

$$\bar{u}\,(T_0) - \bar{u}\,(T_A)\,. \tag{22}$$

All in all the rentropy was increased by the amount

$$S_A = \frac{\bar{u}\,(T_A) - \bar{u}\,(T_0)}{T_0} + \int_{T_A}^{T_0} \frac{1}{T}\frac{d\vec{u}}{dT}dT. \tag{2;3}$$

Analogously, the entropy will increase by the following amount, if the body was in contact with the intermediate piece B al. the time of the "measurement":

$$S_B = \frac{\bar{u}\,(T_B) - \bar{u}\,(T_0)}{T_0} + \int_{T_B}^{T_0} \frac{1}{T}\frac{d\bar{u}}{dT}dT. \tag{24}$$

We shall now evaluate these expressions for the very simple case, where the body which we use has only two energy states, a lower and a higher state. If such a body is in thermal contact with a heat reservoir at any temperature I, the probability that it is in the lower or upper state is given by respectively:

$$\begin{aligned} p(T) &= \frac{1}{1 + ge^{-ukT}} \\ q(T) &= \frac{ge^{-ukT}}{1 + ge^{-u/kT}} \end{aligned} \tag{25}$$

Here u stands for the difference of energy of the two states and g for the statistical weight. We can set the energy of the lower state equal to zero without loss of generality. Therefore: [4]

$$\left.\begin{array}{c} S_A = q\,(T_A)\,l_i \log \frac{q(T_A)p(T_0)}{q(T_0)p(T_A)} \\ +l_i \log \frac{p(T_A)}{p(T_0)} \end{array}\right\}. \qquad \left.\begin{array}{c} S_B = p\,(T_B)\,l_i \log \frac{q(T_0)p(T_B)}{q(T_B)p(T_1)} \\ +k \log \frac{q(T_B)}{q(T_{11})} \end{array}\right\}. \tag{26}$$

Here q and p are the functions of T given
by equation (25), which are here to be taken for the arguments T_0, T_A, or T_B.

If (as is necessitated by the above concept of a "measurement") we wish to draw a dependable conclusion from the energy content of the body K as to the position co-ordinate of the pointer, we have to see to it that the body surely gets into the lower energy state when it gets into contact with T_B. In other words:

$$\begin{aligned} p\,(T_A) = 1, q\,(T_A) = 0 \\ p\,(T_B) = 0, q\,(T_B) = 1 \end{aligned} \tag{27}$$

This of course cannot be achieved, but may be arbitrarily approximated by allowing T_A to approach absolute zero and the statistical weight g to approach infinity. (In this limiting process, T_0 is also changed, in such a way that $p\,(T_0)$ and $q\,(T_0)$ remain constant.) The equation (26) then becomes:
$S_A = -k \log p\,(T_0)\,;$

$$S_B = -k \log q\,(T_0) \tag{28}$$

[84] See the Appendix.

and if we form the expression $e^{-S_A/k} + e^{-s_B/k}$, we find:

$$e^{-s_A/k} + e^{-s_B/k} = 1 \tag{29}$$

Our foregoing considerations have thus just realized the smallest permissible limiting care. The use of semipermeable walls according to Figure 1 allows a complete utilization of the measurement: inequality (1) certainly cannot be sharpened.

As we have seen in this example, a simple inanimate device can achieve the same essential result as would be achieved by the intervention of intelligent beings. We have examined the "biological phenomena" of a nonliving device and have seen that it generates exactly that quantity of entropy which is required by thermodynamics.

APPENDIX

In the case considered, when the frequency of the two states depends on the temperature according to the equations:

$$p(T) = \frac{1}{1 + ge^{-u/kT}}; q(T) = \frac{ge^{-u/kT}}{1 + ge^{-u/kT}} \tag{30}$$

and the mean energy of the body is given by:

$$\bar{u}(T) = uq(T) = \frac{uge^{-u/kT}}{1 + ge^{-u/kT}}, \tag{31}$$

the following identity is valid:

$$\frac{1}{T}\frac{d\bar{u}}{dT} = \frac{d}{dT}\left\{\frac{\bar{u}(T)}{T} + k\log\left(1 + e^{-u/kT}\right)\right. \tag{32}$$

Therefore we can also write the equation:

$$B_A = \frac{\bar{u}\,(T_A) - \bar{u}\,(T_0)}{T_0} + \int_{T_A}^{T_0} \frac{1}{T}\frac{d\bar{u}}{dT}dT \tag{33}$$

as

$$\begin{aligned} S_A = {} & \frac{\bar{u}\,(T_A) - \bar{u}\,(T_0)}{T_0} \\ & + \left\{\frac{\bar{u}(T)}{T} + k\log\left(1 + ge^{-ukT}\right)\right\}_{T_A}^{T_0} \end{aligned} \tag{34}$$

and by substituting the limits we obtain:
$S_A = \bar{u}\,(T'_A)\left(\frac{1}{T_0} - \frac{1}{T_A}\right) + k\log\frac{1+ge^{-u/kT_0}}{1+ge^{-u/kT_A}}$.

If we write the latter equation according to (25):

$$1 + ge^{-u/kT} = \frac{1}{p(T)} \tag{36}$$

for T_A and T_0, then we obtain:

$$S_A = \bar{u}\,(T_A)\left(\frac{1}{T_0} - \frac{1}{T_A}\right) + k\log\frac{p\,(T_A)}{p\,(T_0)} \tag{37}$$

and if we then write according to (31):

$$\bar{u}\,(T_A) = uq\,(T_A) \tag{38}$$

we obtain:

$$S_A = q\,(T_A)\left(\frac{u}{T_0} - \frac{u}{T_A}\right) + k\log\frac{p\,(T_A)}{p\,(T_0)}. \tag{39}$$

If we finally write according to (25):

$$\frac{u}{T} = -k\log\frac{q(T)}{gp(T)} \tag{40}$$

for T_A and T_0, then we obtain:

$$S_A = q\,(T_A)\,k\log\frac{p\,(T_0)}{q\,(T_0)}\frac{q\,(T_A)}{p\,(T_A)} + k\log\frac{p\,(T_A)}{p\,(T_0)} \tag{41}$$

We obtain the corresponding equation for S_H, if we replace the index A with B. Then we obtain:
$\mathrm{S}_B = q\,('_B)\,\hbar\log\frac{p(T_0)}{q(T_0)}\frac{q((T_B)}{p((T_B)} + \hbar\log\frac{p(T_B)}{p(T_0)}$. (42)
Formula (41) is identical with (26), given, for S_A, in the text.
We can bring the formula for S_B into a somewhat different form, if we write:
$q\,(T_B) = 1 - p\,(T_B)$,
expand and collect terms, then we get $S_{\bar{\Delta}} - p\,(T_{\bar{\Delta}})\,k\log\frac{q(T_0)}{p(T_0)}\frac{p(T_B)}{q(T_B)} + k\log\frac{q(T_B)}{q(T_0)}$. This is the formula given in the text for S_B.

References

Smoluchowski, F. Tortrge ber die kinetische Theoric der Materie u. Rlektrizitat. Leipaig: 1914.

Szilard, L. Zeitschrilt fur Physik, 1925, 32, 753.

28.2 V.2 Measurement and Reversibility by Von Neumann

28.2.1 1. Measurement and Reversibility

What happens to a mixture with the statistical operator U, if a quantity M with the operator R is measured in it? This uperatur must be thought of as moasuring $\mathfrak{M}$ in each element of the ensemble and collecting the elements that have been thus treated into a new ensemble. We can answer this question – to the extent to which it admits of an unambiguous answer.

Hirst, let R have a pure discrete, simple spectrum, let $^*{}_1, ^*{}_2, \cdot$ be the complete orthonormal set of eigenfunctions and $\lambda_1, \lambda_2, \ldots$ the corresponding eigenvalues (by assumption, all different from each other). After the measurement, the state of affairs is the following: In the fraction (U $_n, \Phi_n$) of the jriginal ensemble, M has the value λ_n $(n = 1, 2, \ldots)$. This fraction then forms an ensemble in which $\mathfrak{R}$ has the value λ_n with certainty (M. in IV.3.); it is therefore in the state $^i n$ with the (correctly normalized) statistical operator $P_{[\phi_n]}$. Upon collecting these sub-ensembles, therefore, we obtain a mixture with the statistical operator

$$\bar{U}' = \sum_{n=1}^{\infty} \left(\bar{U}_n, \Phi_n\right) P_{[\Phi_n]}.$$

Originally published as chapters V and VI of Mathematische Grundlagen der Quantenmechanik by John von Neumann, pp. 184-237, Springer, Berlin (1932); translation into English by Robert T. Beyer, Mathematical Foundations of Quantum Mechanics, pp. 347-445, Princeton University Press, Princeton (1955).

Second, let R have just a pure discrete spectruin, and let the meaning of $\varphi_1, \varphi_2, \ldots$ and $\lambda_1, \lambda_2, \ldots$ he as before, except that the eigenvalues λ_n are not all simple – i.e., among the λ_n there are coincidences.* Then the measuring process of $\mathfrak{R}$ is not uniquely defined (the same was the case, for example, with $_{\mathbb{C}}$ in IV.3.). Indeed: Let $\mu_1, \mu_2, \ldots$ be distinct real numbers, and S the operator corresponding to the $^{1}{}_{1}, {}_{1}, \ldots$ and $\mu_1, \mu_2, \ldots$. Let Ξ be the corresponding quantity. If $F(x)$ is a function with

$$F\left(\mu_n\right) = \lambda_n \quad (n - 1, 2, \ldots)$$

then $F(S) = R$, therefore $F(\mathbb{S}) = \mathfrak{R}$. Hence the $\mathbb{S}$ measurement can also be regarded as an $\mathfrak{R}$ measurement. This now changes U into the U ' given above, and U ' is independent of the (ontirely arbitrary) $\mu_1, \mu_2, \ldots$, but not of the $\phi_1, \phi_2, \cdots$. Yet the $\phi_1, \phi_2, \cdots$ are not uniquely determined, because of the multiplicity of the eigenvalues of R. In IV.2., we stated (following II.8.), what can be said regarding the $\phi_1, \phi_2, \cdots$: Let $\lambda', \lambda'', \ldots$ be the different eigenvalues among the $\lambda_1, \lambda_2, \ldots$, let $\mathfrak{M}_{\lambda}, , \mathfrak{M}_{\lambda}, \ldots$ be the sets of the f with Rf $= \lambda$ 'f , $Rf = \lambda$"$f, \ldots$ respectively. Finally, let $x_1', x_2', \ldots$; $x_1'', x_2'', \ldots$; ..., respectively be arbitrary orthonormal sets which span $\mathfrak{M}_{\lambda'}, \mathfrak{M}_{\lambda''}, \ldots$. Then $x_1^1, x_2^1, \ldots, x_1'', x_2'', \ldots, \ldots$ is the most general $\phi_1, \phi_2, \cdots$ set. Hence U' may be depending upon the choice of $\mathfrak{s}$, i.e., depending upon the actual measuring arrangement, any expression

$$U' = \sum_n \left(U_{x_n'}, x_n'\right) P_{[x_n']} + \sum_n \left(U_{x_n''}, x_n''\right) P_{[x_n'']} + \cdots .$$

This expression, however, is unambiguous only in special cases.

We determine this special case. Each individual term must be unambiguous. That is, for each eigenvalue λ,

- Eds. note: A. S. Wightmann informs us that von Neumann's expression here is incorrect for the density matrix after a measurement in which the observable in question has degenerate eigenvalues (Lders, 1951; Furry, 1966).

if $\mathfrak{R}_{\lambda}$ is the set of the f with $Rf = \lambda f$, the sum

$$\sum_n \left(Ux_n, x_n\right) F_{[x_n]}$$

must have the same value for every choice of the orthonormal set $x_1, x_2, \ldots$ spanning the manifold $\mathfrak{M}_{\lambda}$. If we call this sum V, then verbatim repetition of the observations in IV.3. (in which the U_O, U, M, there are to be replaced by $U, V, \mathfrak{M}_{\lambda}$) shows that we must have $V = c_{\lambda} P_{\mathfrak{M}}$ (c_{λ} constant, > 0), and that this is equivalent to the validity of (Uf, f) $= c_{\lambda}(f, f)$ for all f of m_{λ} Since these f are the same as the $p_{m_{\lambda}}{}^{g}$ for all g, we require: ($\mathrm{UP}_{\mathfrak{M}_{\lambda}}\mathrm{g}, \mathrm{P}_{\mathfrak{M}_{\lambda}}\mathrm{g}$) = c $_{\lambda}\left(\mathrm{P}_{\mathfrak{W}_{\lambda}}\mathrm{g}, \mathrm{P}_{\mathfrak{W}_{\lambda}}\mathrm{g}\right)$, i.e.. $\left(P_{M_{\lambda}} U P_{M_{\lambda}} g, g\right) = c_{\lambda}\left(P_{M_{\lambda}} g, g\right)$, i.e.,

$$\mathrm{P}_{\mathfrak{M}_{\lambda}} \mathrm{U} \mathrm{P}_{\mathfrak{M}_{\lambda}} = c_{\lambda} \mathrm{P}_{\mathfrak{M}_{\lambda}}$$

for all eigenvalues λ of R. But if this condition, clearly restricting U sharply, is not satisfied, then different arrangements of measurement for $\mathfrak{R}$ can actually transform U into different U.

(Nevertheless, we shall succeed in V.4. in making some statements about the result of a general $\mathfrak{R}$ measurement, on a thermodynamical basis.

Third, let R have no pure discrete spectrum. Then by III.3. (or IV.3., criterion 1.), it is not measurable with absolute precision, and $\mathfrak{R}$ measurements of limited precision (as we discussed in the case referred to) are equivalent to measurements of quantities with pure discrete spectra.

Another type of intervention in material systems, in contrast to the discontinuous, non-causal and instantaneously acting experiments or measurements, is given by the time dependent Schrödinger differential equation. This describes how the system changes continuously and causally in the course of time, if its total energy is known. For
states , these equations are

$$(\mathbf{T}_1.) \quad \frac{\partial}{\partial t}\phi_t = -\frac{2\pi i}{h} H\phi_t$$

where H is the energy operator.
For the statistical sperator of the state ϕ_t, $U_t = P_{[\phi_t]}$, this means:

$$\left(\frac{\partial}{\partial t}U_t\right) f = \frac{\partial}{\partial t}\left(U_t f\right) = \frac{\partial}{\partial t}\left((f,\phi_t)\cdot\phi_t\right) = \left(f, \frac{\partial}{\partial t}\phi_t\right)\cdot\phi_t + (f,\phi_t)\cdot\frac{\partial}{\partial t}\phi_t$$

$$= -\left(f, \tfrac{2\pi i}{h} H\hat{*}_t\right)\cdot\hat{*}_t - (f,\hat{*}_t)\,\tfrac{2\pi i}{h} H_t$$
$$= \tfrac{2\pi i}{n}\left((Hf,\phi_i)\cdot\phi_i - (f,\phi_i)\cdot H\Phi_i\right) = \tfrac{2\pi i}{\Pi}\left(U_i H - HU_i\right) f.$$
that is:

$$(\bar{r}_2,) \quad \frac{\partial}{\partial t}U_t = \frac{2\pi i}{h}\left(U_t H - HU_t\right).$$

Now if U_t is not a stato, but a mixture of several states, say $P_{\left[\phi_t^{(1)}\right]}, P_{\left[\phi_t^{(2)}\right]}, \cdots$ with the respective weights $w_1, w_2, \ldots$, then it must be changed in such a way as results from the changes of the individual
$P_{\left[\phi_+^{(1)}\right]}, P_{\left[\phi_+^{(2)}\right]}, \cdots$. By the addition of the corresponding equations $\mathbf{T}_2$., we recugnize that $\mathbf{T}_2$. holds for this U_t also. Now since all U are such mixtures, or limiting cases of such (for example, each U with finite $\operatorname{Tr} U$ is such a mixture), we can claim the general validity of $T_.$.

In $\mathbf{T}_1$., moreover, H may also depend on t, just as in the Schrödinger differential equation $\mathbf{T}_1$. If that is not the case, then we can even given explicit solutions: For $\mathbf{T}_1$., as we already know,

$$(\boldsymbol{T}_1'\cdot) \quad \phi_t = e^{-\frac{2\pi i}{h} t\cdot H_{\phi_0}},$$

and for T_2.,

$$(\mathbf{T}_2'\cdot) \quad U_t = e^{-\frac{2\pi i}{h} t\cdot 1} U_0 e^{\frac{2\pi i}{h} tH}.$$

(It is easily verified that inese are solutions, and also that they follow from each other. It is clear also that there is only one solution with a fixed initial ϕ_o or U_0 respectively: the differential equations $\mathbf{T}_1$., $\mathbf{T}_2$. are of first order in t.)

We therefore have two fundamentally different types of interventions which can occur in a system s or in an ensemble $[\mathbf{s}_1, \ldots, \mathbf{s}_\mathrm{N}]$. First, the arbitrary changes by measurements which are given by the formula

$$(1.)\ U \to U' = \sum_{n=1}^{\infty} (U\phi_n, \phi_n)\, P_{[\phi_n]}$$

($\phi_1, \phi_2, \cdots$ a complete urthonormal set, of. supra). Socond, the automatic changes which occur with passage of time. These are given by the formula
(2.) $U \to U_t = e^{-\frac{2\pi i}{h} \cdot tH}{}_{Ue}{}^{\frac{2\pi i}{h} tH}$
(H is the energy operator, t the time; H is independent of t). If H depends on t, then we may divide the time interval under consideration into small time intervals in each one of which H does not change – or changes only very slightly, and apply 2. to these individual intervals. Superposition then gives the final result.

We must now analyze in more detail these two types of intervention, their nature, and their relation one to another.

First of all, it is noteworthy that the time
dependence of H is included in 2 . (in the manner described there), so that one should expect that 2. would suffice to describe the intervention caused by a measurement: Indeed, a physical intervention can be nothing else than the temporary insertion of a certain energy coupling into tho observed system, i.e., the introduction of an appropriate time dependency of H (prescribed by the observer). Why then do we need the special process 1 . for the measurement? The reason is this: In the measurement we cannot observe the system s by itsclf, but must rather investigate the system $\mathbf{S}+\mathbf{M}$, in order to obtain (numerically) its interaction with the measuring apparatus $\mathbf{M}$. The theory of the measurement is a statement concerning $\mathbf{S}+\mathbf{M}$, and should describe how the state of $\boldsymbol{s}$ is related to certain properties of the state of $\mathbf{M}$ (namely, the posilions of a certain pointer, since the observer reads these). Moreover, it is rather arbitrary whether or not one includes the observer in $\mathbf{M}$, and replaces the relation between the s state and the pointer positions in M by the relations of this state and the chemical changes in the observer's eye or even in his brain (i.e., to that which he has "scon" or "perceived"). We shall investigate this more precisely in VI.1. In any case, therefore, the application of 2. is of importance only for $\mathbf{S}+\mathbf{M}$. Of course, we must show that this gives the same result for $\mathbf{s}$ as the direct application of $\mathbf{1}$. on $\mathbf{S}$. If this is successful, then we have achieved a unified way of looking at the physical world on a quantum mechanical basis. We postpone the discussion of this question until VI.3.

Second, it is to be noted, with regard to 1. , that we have repeatedly shown that a measurement in the sense of 1. must be instantaneous, i.e., must be carried through in so short a time that the change of U given by 2. is not yet noticeable. (If we wanted to correct this by calculating the changed U_t by 2., we would still gain nothing, because to apply any U_t, we must first know t, the moment of measurement, exactly, i.e., the time duration
of the measurement must be short.) This is now questionable in principle, because it is well-known that there is a quantity which, in classical mechanics, is canonically conjugate with the time: the energy. [180] Therefore it is to be expoctod that for the canonically conjugate pair timeenergy, there must exist indeterminacy relations similar to those of the pair cartesian coordinate-momentum. [181] Note that the special relativity theory shows that a far reaching analogy must exist: the three space coordinates and time form a "four vector" as do the three momentum courdinates and the energy. Such an indeterminacy relation would mean that it is not possible to carry out a very precise measurement of the energy in a very short time. In fact, one would expect for the error of measurement (in the energy) and the lime duration τ a relation of the form

$$\in \tau \sim h.$$

A physical discussion, similar to that carried out in III.4. for p, q, actually leads to this result. [181] Without going into details, we shall consider the case of a light quantum. Its energy uncertainty ϵ is, because of the Dohr frequency condition, h times the frequency uncertainty: $h\Delta v$. But, as we discussed in Note 137, Δv is at best the reciprocal of the time duration, $1/\tau$, i.e., $\epsilon \gtrsim \mathrm{h}/\tau$– and in order that the monochromatic nature of the light quantum be established

in the entire time interval τ, the measurement must extend over this entire time interval. The case of the light quantum is characteristic,

since the atomic energy levels, as a rule, are determined from the frequency of the corresponding spectral lines. Since the energy behaves in such fashion, a relation between the precision of measurement for other quantities π and the duraiion of the measurement is also possible. Then how can our assumption of instantaneous measurements be justified?

First of all we must admit that this objection points at an essential weakness which is, in fact, the chief weakness of quantum mechanics: its nun-relativistic character, which distinguishes the time t from the three space coordinates x, y, z, and presupposes an objective simultaneity concept. In fact, while all other quantities (especially those x, y, z closely connected with t by the Lorentz transformation) are represented by operators, there corresponds to the time an ordinary number-parameter t, just as in classical mechanics. Or: a system consisting of 2 particles has a wave function which depends on its $2 \times 3 = 6$ space coordinates, and only upon one time t, although, because of the Lorentz transformation, two times would be desirable. It may be connected with this non-relativistic character of quantum mechanics that we can ignore the natural law of minimum duration of the measurements. This might be a clarification, but not a happy one!

A more detailed investigation of the problem, however, shows that the situation is really not so bad as this. For what we really need is not that the change of t be small, but only that it have little effect in the calculation of the probabilities $(\mathrm{U_n}, \phi_\mathrm{n})$, and therefore in the formation of

$$U' = \sum_{n=1}^{\infty} \left(U\phi_n, \quad \phi_n \right) P_{[\phi_n]}$$

whether we start out from U itself or from a

$$U_t = e^{-\frac{2\pi i}{h} tH} \frac{2\pi i}{h} tH.$$

$$\text{Recause of} \quad \begin{matrix} (U_t\Phi_n, \Phi_n) = \\ e^{-\frac{2\pi}{h}}\Phi_n \end{matrix} \quad \begin{matrix} \left(e^{-\frac{2\pi i}{h} iH \frac{2\pi i}{h}} Li \right. \\ \left. \right) \end{matrix}$$

$$= \left(\bar{U}^{\frac{2\pi i}{h} tH} \quad \phi_n, e^{\frac{2\pi i}{h} tH}\Phi_n \right),$$

this can be accomplished by so changing H by an appropriate perturbation energy that

$$e^{\frac{2\pi i}{in} tH}\Phi_n$$

differs from ψ_n only by a constant factor of absolute value 1 . That is, the state ϕ_n should be essentially constant under the influence of **2**., i.e., a stationary state; or equivalently $H\Phi_n$ must be equal to a real constant times ϕ_n, i.e., ϕ_n an eigenfunction of H. At first glance, such a change of the onorgy operator H, which makes the eigenfunctions of R stationary, and therefore eigenfunctions of H (i.e., R, H commutative) may seem implausible. But this is not really the case, and one can even see that the typical arrangements of measurement aim at exactly this sort of effect on H.

In fact, each measurement results in the emission of a light quantum or a mass particle, with a certain energy, in a certain direction. It is then by these characteristics, i.e., by its momentum, that the particle expresses the result of the measurement or, a mass point (for

[8180] Any textbook of classical (Hamiltonian) mechanics gives an account of these connections.

[181] The uncertainty relations for the pair time-energy have been discussed froquently. Cf. the comprehensive treatmont of Heisenberg, Die Physikalischen Prinzipien der Quantentheorie, II.2.d., Leipzig, 1930.

example, a pointer on a scale) comes to rest, and its cartesian coordinates give the result of the measurement. In the case of light quanta, using the terminology of III.6., the desired measurement is thus equivalent to the statement as to which $M_n = 1$ (the rest being $= 0$), i.e., to the enumeration of all $M_1, M_2, \ldots$ values. For a moving (departing) mass point, the statement of its three momentum components $\mathrm{P^X}, \mathrm{P^Y}, \mathrm{P^Z}$ is the corresponding
equivalent; for a mass point at rest (the index point), the statement of its three cartesian coordinates x, y, z, or, using their operators, of the Q^X, Q^Y, Q^Z. But the measurement is completed only if the light quantum or mass point is aciually vorne "away," i.e., only when the light quantum is not in danger of absorption; or when the mass point may no longer be deflected by potential energies; or, if the mass point is actually at rest, in which case a large mass is necessary. [182] (This latter is certainly necessary because of the uncertainty relaiions, since the volocity must be near 0 , and therefore its dispersion must be small, although its product with the mass – the momentum – has a large dispersion, because of the small dispersion of the coordinates. Ordinarily, the pointers are macroscopic objects, i.e., enormous.) Now the energy operator ii, so far as it concerns the light quantum, is (III.6, page 270)

$$\begin{aligned}&\sum_{n=1}^{\infty} h\rho_n \cdot M_n \\ &+\sum_{p=1}^{\infty}\sum_{n=1}^{\infty} w_{kj}^n \left(\sqrt{\bar{M}_n + 1}\cdot \begin{pmatrix} k \\ i \\ M_n \to M_n + 1 \end{pmatrix}\right. \\ &\left. +\sqrt{M_n}\cdot \quad \begin{matrix} k \\ M_n \to M_n - 1 \end{matrix} \right)\end{aligned}$$

while for both mass point examples, H is given by

$$\frac{(\mathrm{P^x})^2 + (\mathrm{P^y})^2 + (\mathrm{P^z})^2}{2\ \mathrm{m}} + \mathrm{V}\,(\mathrm{Q^x}, \mathrm{Q^y}, \mathrm{Q^z})$$

(m the mass, V the potential energy). Our criteria say: the w_{kj}^n should vanish, or V should be constant, or m should be very large. But this actually produces the effect that the P^X, P^Y, P^Z and the Q^X, Q^Y, Q^Z rospoctively commute with the H given above.

In conclusion, it should be mentioned that the making stationary of the really interesting states (here the $\Phi_1, \Phi_2, \ldots$) plays a role elsewhere, too, in theoretical physics. The assumptions on the possibility of the interruption of chemical reactions (i.e., their "poisoning"), which are often unavoidable in physical-chemical "ideal experiments," are of this nature. [183]

The two interventions 1. and 2. are fundamentally different from one another. That both are formally unique, 1.e., causal, is unimportant; indeed, since we are working in terms of the statistical properties of mixtures, it is not surprising that each change, even if it is statistical, effects a causal change of the probabilities and the expectation values. Indeed, it is precisely for this reason, linal one introduces statistical onsombles and probabilities: On the other hand, it is important that 2. does not increase the statistical uncertainty existing in U, but that 1. does: 2. transforms states into states

$$\begin{pmatrix} P_{[\phi]} & \text{into} & P \\ & & \left[e^{-\frac{2\pi i}{h}tH} \right. \\ & & \left. \phi\right] \end{pmatrix}$$

[8182] All other details of the measuring arrangement aim only at the connection of the quantity $\mathfrak{R}$, which is actually of interest, or of its operator R, with the M_n or the P^X, P^Y, P^Z or the Q^X, Q^Y, Q^Z, respectively, that have

while 1. can transform states into mixtures. In this sense, therefore, the development of a state according to 1. is statistical, while according to 2. it is causal.

Furthermore, for fixed H and t, 2. is simply a unitary transformation of all $U : U_t = AUA^{-1}$, $A = e^{-\frac{2\pi i}{h}tH}$ is unitary. That is, $Uf = g$ implies that $U_t(Af) = Ag$, so that U_t results from U by the unitary transformation A of Hilbert space, that is, by an isomorphism which leaves all our basic geometric concepts invariant (cr. the principies sei duwn in I.4.). Therefore it is rovorsible: it suffices to replace A by A^{-1}– and this is possible, since A, A^{-1} can be regarded as entirely arbitrary unitary operators because of the far reaching freedom in the choice of H, t. Just as in classical mechanics therefore, 2. does not reproduce une uf the wost important and striking properties of the real world, namely its irreversibility, the fundamental difference between the time directions, "future" and "past."

1. behaves in a fundamentally different fashion: the transition

$$U \to U' = \sum_{n=1}^{\infty} (U\Phi_n; \Phi_n)\, P_{[\Phi_n]}$$

is certainly not prima facie reversible. We shall soon see that it is in general irreversible, in the sense that it is not possible in general to come back from a given U ' to its U by repeated applications of any processes ., 2.

Therefore, we have reached a point at which it is desirable to utilize the thermodynamical method of analysis, because it alone makes it possible for us to understand correctly the difference between 1. and 2., into which reversibility questions obviously enter.

28.2.2 2. Thermodynamical Considerations

We shall investigate the thermodynamics of quantum mechanical ensembles according to two different points of view. First, let us assume the validity of both fundamental laws of thermodynamics, i.e., the impussibility of perpetual motion of the first and second kind (energy law and entropy law), [184] and calculate the entropy for each ensemble from this. In this case, nurmal methods of the phenomenological thermodynamics are applied, and quantum mechanics plays a role only insofar as our thermodynamical observations relate to such objects whose behavior is regulated by the laws of quantum mechanics (our ensombles, as well as their statistical operators U)– but the correctness of both laws will be assumed and not proved. Afterwards we shall prove the validity of these fundamental laws in quantum mechanics. Since the energy law holds in any case, only the entropy law has to be considered. That is, we shall show linat the intervontions 1., 2. never decrease the ontropy, as calculated by the first method. This order may seem somewhat unnatural, but it is based on the fact that it is by the phenomenological discussion that we obtain that overall view of the problem which is required for considerations of the second kind.

Wo therefore begin with the phenomenological consideration, which will also permit us to solve a wellknown paradox of classical thermodynamics. First we must emphasize that the unusual character of our "ideal experiments," i.e., their practical infeasibility, does not impair their demonstrative power: In the sense of phenomenological thermodynamics, each conceivable

[8] been mentioned. Of course, this is the most important practical aspect of the measuring technique.

[183] Cf. e.g., Nernst, Theoretische Chemie, Stuttgart (numerous editions since 1893), Book IV, Discussion of the thermodynamic proof of the "mass action law."

process constitutes valid evidence, provided that it does not conflict with the two fundamental laws of thermodynamics.

Our purpose is to determine the entropy of an ensemble $[\mathbf{s}_1, \ldots, \mathbf{s}_N]$ with the statistical operator U, where U is assumed io be correctily normalized, i.e., TrU = 1. In the terminology of classical statistical mechanics, we are dealing with a Gibbs ensemble: i.e., the application of statistics and thermodynamics will be made not on the (interacting) components of a single, very complicated mechanical system with many (only imperfectly known) degrees of freedom [185]– but on an onsomble of vory many (identical) mechanical systems, each of which may have an arbitrarily large number of degrees of freedom, and each of which is entirely separated from the others, and does not interact with any of them. [186] As a consequence of the complote separation of the systems $s_1, \ldots, s_N$, and of the fact that we shall apply to them the ordinary methods of enumeration of the calculus of probability, it is evident that ordinary statistics be used, and that the BoseEinstein and Fermi-Dirac statistics, which differ from those and which are applicable io certain ensembles uf indistinguishable and interacting particles (namely, for light quanta or electrons and protons, cf. III.6., in particular, Note 147), do not enter into the problem.

The method introduced by Einstein for the thermodynamical treatment of such ensembles $[\mathbf{s}_1, \ldots, \mathbf{s}_N]$ is the following: [187] Each system $s_1, \ldots, s_N$ is confined in a box $\mathbf{K_i}, \ldots, \mathbf{K}_N$, whose walls are impenetrable to all transmission effects – which is possible for this system because of the lack of interaction. Furthermore, each box must have a very large mass, so that the possible state (and hence energy and mass) changes of the $\mathbf{s}_1, \ldots, \mathbf{s}_N$ affects its mass only slightly. Also, their velocities in the ideal experiments which are to be carried out are thereby kept so small that the calculations may be performed nonrelativistically. We then enclose these boxes into a very large bux $\overline{\mathbf{K}}$ (i.e., the volume $\boldsymbol{\gamma}$ of $\overline{\mathbf{K}}$ should be much larger than the sum of the volumes of the $\mathrm{w}_1, \ldots, \mathrm{w}_N$). For simplicity, no force field will be present in $\overline{\mathbf{K}}$ (in particular, it should be free from all gravitational fields, and so large that the masses of the $\boldsymbol{K}_1, \ldots, \boldsymbol{K}_N$ have no relevant effects either. We can therefore regard the $M_1, \ldots, M_N$ (which contain $s_1, \ldots, s_N$ respectively) as the molecules of a gas which is enclosed in the large container $\overline{\mathbf{K}}$. If we now bring $\overline{\mathbf{K}}$ into contact with a very large heat reservoir of temperature $\mathbf{T}$, then the walls of $\overline{\mathbf{K}}$ also take on this temperature, and its (true) molecules assume the corresponding Brownian motion. Therefore they will contribute momentum to the adjacent $\mathbf{K}_1, \ldots, \mathbf{K}_N$, so that these engage in motion, and transfer momentum to the other $\mathbf{K}_1, \ldots, \mathbf{K}_N$. Soon all $\mathbf{K}_1, \ldots, \mathbf{K}_N$ will be in motion and will be exchanging momentum (on the wall of $\overline{\mathbf{K}}$) with the (true) molecules of the wall, and will each uther (in the interior of $\overline{\mathbf{K}}$) by collision processes. The stationary equilibrium state of motion is then obtained if the $\mathbf{K}_1, \ldots, \mathbf{K}_n$ have taken on that velocity distribution which is in equilibrium with the Brownian motion of the wall

molecules (of temperature T) – i.e., the Maxwellian velocity distribution of a gas of temperature $\mathbf{T}$, the "molecules" of which are the $\mathbf{k}_1, \ldots, \mathbf{k}_N$. [188] we can then say: the $\{\mathbf{s}_1, \ldots, \mathbf{s}_N\}$-gas has taken on the temperature $\mathbf{T}$. por brevity, we shall call the ensemble $[\mathbf{s}_1, \ldots, \mathbf{s}_M]$ with the statistical operator U the U-ensemble, and the $[\mathbf{s}_1, \ldots, \mathbf{s}_N]$-gas the U-gas.

---

[184] The phenomenological system of thermodynamics built upon this foundation can be found in numerous texts. For example, Planck, I'reatise on Thermodynamics, London, 1927. For the following, the statistical aspect of these laws is of chief importance. This is analyzed in the following treatises: Einstein, Verh. d. dtsch. physik, Ges. 12 (1914); Szilard, Z. Physik 32 (1925).

[185] This is the Maxwell-Boltzmann method of statistical mechanics (cf. the review in the article of P. and T. Ehrenfest in Enzykl. d. Math. Wiss., Vol. II.4. D., Leipzig, 1907). In the gas theory for example, the "very complicated" system is the gas which consists of many (interacting) molecules, and the molecules are investigated statistically.

[186] This is the Gibbs method (cf. the reference in Note 185). Here the individual system is the entire gas, and many replicas of the same system (i.e., of the same gas) are considered simultaneously, and their properties are evaluated statistically.

[187] See the reference in Note 184 . This was further developed by L. Szilard.

The reason that we concern ourselves will such a gas is that we must determine the entropy difference of the U-ensemble and the V-ensemble (U, V definite operators with $\mathrm{Tr}\, U = 1, \mathrm{Tr}\, V = 1$, and with the corresponding ensembles $[\mathbf{s}_1, \ldots, \mathbf{s}_\mathrm{N}]$ and $\{\mathbf{s}_1, \ldots, \mathbf{s}_\mathrm{N}\}$). The determination requires by definition a reversible transformation of the former ensemble into the latier, [189] and this is best accomplished by the aid of the $U-$ and V-gases. That is, we maintain that the entropy difference of the $U-$ and $V-$ ensembles is exactly the same as that of the $U-$ and $V-$ gases – if both are observed at the same temperature $\mathbf{T}$, but are otherwise arbitrary. If T is very near 0 , then this is uvvijusly the caso with arbitrary precision; because the difference between the U-ensemble and the V gas vanishes at the temperature 0 , since the $\boldsymbol{K}_1, \ldots, \boldsymbol{K}_\mathrm{N}$ of the latter have then no motion of their own, and the

presence of the $\mathbf{K}_1, \ldots, \mathbf{K}_\mathrm{N}, \overline{\mathbf{K}}$, when they are at rest is thermodynamically unimportant (and likewise for V). Therefore we shall have accomplished our aim if we can show that for a given change of $\mathbf{T}$, the entropy of the U-gas changes just as much as the entropy of the V-gas. The entropy change of a gas which is heated from $\mathbf{T}_1$ to $\mathbf{T}_2$ depends only upon its caloric equation of state, or more precisely, upon its specific neat. [190] Naturaily, the gas must not be assumed to be an ideal gas here if, as in our case, $\mathbf{T}_1$ must be chosen near 0.[191] on the other nand, it is certain that both gases (U and V) have the same equation of state and the same specific heats because, by kinetic theory, the boxes $\mathbf{K}_1, \ldots, \mathbf{K}_\mathrm{N}$ dominate and cover completely the systems $\boldsymbol{s}_1, \ldots, \boldsymbol{s}_\mathrm{N}$ and $\boldsymbol{s}_1, \ldots, \boldsymbol{s}'_\mathrm{N}$ which are enclosed in them. In this heating process therefore, the difference of U and V is not noticeable, and the two entropy differences coincide, as was maintained. In the following therefore, we shall compare only the $U-$ and V-gases with each other, and we shall choose the temperaturc $\boldsymbol{T}$ so high that these can be regarded as ideal gases. [192] In this way, we control its kinetic behavior

[190] If $\mathbf{c}(\mathbf{T})$ is the specific heat at the temperature $\mathbf{T}$ of the gas quantum under discussion, then in the temperature interval $\mathbf{T}, \mathbf{T} + \mathrm{d}\mathbf{T}$ it takes on the quantity of heat $c(\mathbf{T})\mathrm{d}\mathbf{T}$. By Note 185, the entropy difference is then

$$\int_{T_1}^{T_2} \frac{c(T)dT}{T}$$

[191] For an ideal gas, $c(\tau)$ is constant; for very small $\boldsymbol{\tau}$, this certainly fails. Cf. for example, the reference in Note 6.

[192] In addition to this, it is required that the volume V of $\overline{\mathbf{K}}$ be large in comparison to the total volume of the

completely, and we can apply ourselves to the real problem: to transform U-gas reversibly into V-gas. In this case, in contrast to the processes used so far, we shall also have to consider the $s_1, \ldots, s_N$ found in the interior of the $\mathbf{K}_1, \ldots, \mathbf{K}_{\tilde{N}}$ i.e., we shall have to "open" the boxes $\mathrm{K}_1, \ldots, \mathrm{K}_\mathrm{N}$.

Next, we show that all states $U = P_{[\phi]}$ have the same entropy, i.e., that the reversible transformation of the $P_{[\phi]}$ ensemble into the $P_{[\psi]}$ ensemble is accomplished without the absorption or liberation of heat energy (mechanical energy must naturally be consumed or produced if the expectation value of the energy in $P_{[\phi]}$ is different from that in $P_{[\psi]}$), cf. Note 189. In fact, we shall not even have to refer to the gases just considered. This transformation succeeds even at the temperature 0 , i.e., with the ensembles themselves. It should be mentioned, furthermore, that as soon as this is proved, we shall be able to and shall so normalize the entropies of the U ensembles that all states have the entropy 0 .

Moreover, the transformation of $\mathrm{P}_{[\phi]}$ into $\mathrm{P}_{[\psi]}$ described above does not need to he reversible:

[8188] The kinetic theory of gases, as is well-known, describes in this way that process in which the walls communicate their temperature to the gas enclosed by them. Cf. the references in Notes 184 and 185.

[189] In this transformation, if the heat quantities $\mathbf{Q}_1, \ldots, \mathbf{Q}_\mathrm{i}$ are required at the respective temperatures $\mathbf{T}_1, \ldots, \mathbf{T}_\mathbf{i}$, then the entropy difference is equal to

Cf. the reference in Note 184.

Recause it is not so, then the entropy difference must be $\geq$ the expression given in Note 189 (cf. reference in Note 185), therefore ≥ 0. Permutation of $P_{[\phi]}, P_{[\psi]}$ shows that this value must also be ≤ 0. Therefore the value is $= 0$.

$\mathbf{K}_1, \ldots, \mathbf{K}_N$: furthermore that the "energy per degree of freedom" $\kappa \boldsymbol{T}$ (κ = Boltzmann's constant) be large in comparison to

$$h^2/\mu \boldsymbol{V}^{2/3}$$

(h = Planck's constant, μ = mass of the individual molecule; this quantity is of the dimensions of energy). Cf. for example, Fermi, Z. Physik, 36 (1926).

The simplest process would be to refer to the time dependent Schrodinger differential equation, i.e., our process 2. , in which an energy uperaior if and a numerical value of t must be found such that the unitary operator

$$e^{-\frac{2\pi i}{h} tH}$$

transforms ϕ into ψ. Then, in t seconds, $\bar{P}_{[\phi]}$ would change spontaneously into $\mathrm{P}_{[\psi]}$. The process is also reversible, and no mention has been made of the heat (cf. V.1.). However, we prefer to avoid assumptions regarding the possible forms of the energy operators H and to apply the process 1. alone, i.e., measuring interventions. The simplest such measuremont would be to moasure the quantity $\mathfrak{R}$ in the ensemble $P_{[\Phi]}$, whose operator R has a pure discrete spectrum with simple eigenvalues $\lambda_1, \lambda_2, \ldots$, and in which ψ occurs among the eigenfunctions $\psi_1, \psi_2, \ldots$, say $\psi_1 = \psi$. This measurement transfurms ψ into a mixture of the states $\psi_1, \psi_2, \ldots$, and there $\psi_1 = \psi_1$ will be present. along with the other states Ψ_n. However, this procedure is unsuitable, because $\psi = \psi$ occurs only with the probability $|(\phi, \psi)|^2$, while the portion $1 - |(\phi, \psi)|^2$ goes over into other states. In fact, the latter portion is the entire result for orthogonal $\$, \psi$. A different experiment however will accomplish our purpose. By repetition of a great number of different measurements, we shall change $P_{[\Phi]}$ into such an ensemble, which differs from $P_{[\psi]}$ by an arbitrarily small amount. That all these operators are (ur at least, can be) irreversible is unimportant, as we discussed above.

We assume ϕ, ψ srthogonal, since we could otherwise choose a $x(\|x\| = 1)$ orthogonal to both, and could go from ϕ to x, and then from x to ψ. Now let $k = 1, 2, \ldots$ be a number which is at our disposal, and set $\psi^{(\nu)} = \cos \frac{\pi\nu}{2k} \cdot \phi + \sin \frac{\pi\nu}{2k} \cdot \psi \quad (\nu = 0, 1, \ldots, k)$ Clearly, $\psi^{(0)} = \Phi, \psi^{(K)} = \psi$, and $\left|\left|\psi^{(\nu)}\right|\right| = 1$. We
extend each $^{(v)}(v = 1, 2, \ldots, k)$ to a complete orthonormal set $\psi_1^{(v)}, \psi_2^{(v)}, \ldots$ with $\psi_1^{(v)} = \psi^{(v)}$. Let $R^{(v)}$ be an operator with a pure discrete spectrum and different eigenvalues, say $\lambda_1^{(v)}, \lambda_2^{(v)}, \ldots$, whose eigenfunctions are the $\psi_1^{(v)}, \psi_2^{(v)}, \ldots$, and $\mathfrak{R}^{(v)}$ the corresponding quantity. We observe further that
$\left(\psi^{(\nu-1)}, \psi^{(\nu)}\right) = \cos \frac{\pi(\nu-1)}{2k} \cos \frac{\pi\nu}{2k} + \sin \frac{\pi(\nu-1)}{2k} \sin \frac{\pi\nu}{2k} = \cos\left(\frac{\pi\nu}{2k} - \frac{\pi(\nu-1)}{2k}\right) = \cos \frac{\pi}{2k}$

In the ensemble with $\mathrm{U}^{(0)} = \mathrm{P}_{[0}(0)\big] = \mathrm{P}_{[\psi]}$ we now measure the quantity $\mathfrak{R}^{(1)}$, in which case $U^{(1)}$ results. We then measure the quantity $\mathfrak{R}^{(2)}$ on $U^{(1)}$, when $U^{(2)}$ results, etc. We finally measure the quantity $\mathfrak{R}^{(k)}$ on $U^{(k-1)}$ whence $U^{(k)}$ results. That $U^{(k)}$, for sufficiently large k, lies arbitrarily close to $\bar{P}_{[\psi}(k)_{]} = \bar{P}_{[\psi]}$ can easily be established. If we measure $\mathfrak{R}^{(v)}$ on $\psi^{(\nu-1)}$, then the fraction $\left|\left(\psi^{(\nu-1)}, \psi^{(\nu)}\right)\right|^2 = \left(\cos \frac{\pi}{2k}\right)^2$ goes over into $\psi^{(v)}$, and in the successive measuremenis of $\mathfrak{R}^{(1)}, \mathfrak{R}^{(2)}, \ldots, \mathfrak{R}^{(k)}$ thereforc, at least the fraction $\left(\cos \frac{\pi}{2K}\right)^2$ will go over from $\psi^{(O)} = \phi$ over $\psi^{(1)}, \psi^{(2)}, \ldots, \psi^{(k-1)}$ into $\psi = \psi^{(k)}$. And since $\left(\cos \frac{\pi}{2k}\right)^{2k} \to 1$ as $k \to \infty, \psi$ results as nearly exclusively as one may wish, if k is sufficiently large. The exact proof runs as follows. Since the process 1. does not change the trace, and since $\mathrm{Tr}\, \mathrm{U}^{(0)} = \mathrm{Tr}\, \mathrm{P}_{[\Phi]} = 1$, therefore $\mathrm{Tr}\, U^{(1)} = \mathrm{Tr}\, U^{(2)} = \ldots = \mathrm{Tr}\, U^{(K)} = 1$. On the other hand,

$$\begin{aligned}\left(U^{(v)}f,f\right)&=\sum_n\left(U^{(v-1)}\psi_n^{(v)},\psi_n^{(v)}\right)\left(P_{\left[\psi_n^{(v)}\right]}f,f\right)\\&=\sum_n\left(U^{(v-1)}\psi_n^{(v)},\psi_n^{(v)}\right)\left|\left(\psi_n^{(v)},f\right)\right|^2.\end{aligned}$$

Therefore, for $v=1,\ldots,k-1$ and $f=\psi_1^{(v+1)}=\psi^{(v+1)}$, and for $v=k$ and $f=\psi_1^{(k)}=\psi^{(k)}=\psi$, we have:

$$\begin{aligned}\left(U^{(v)}\psi^{(v+1)},\psi(v+1)\right)&\geq\left(U^{(v-1)}\psi^{(v)},\psi^{(v)}\right)\left|\left(\psi^{(v)},\psi^{(v+1)}\right)\right|^2\\&=\left(\cos\frac{\pi}{2k}\right)^2\cdot\left(U^{(v-1)}\psi^{(v)},\psi^{(v)}\right)\\\left(U^{(k)}\psi^{(k)},\psi^{(k)}\right)&=\left(U^{(k-1)}\psi^{(k)},\psi^{(k)}\right)\end{aligned}$$

togethor with

$$\begin{aligned}\left(\bar{U}^{(0)}\psi^{(1)},\psi^{(1)}\right)=\left(P_{\left[\psi^{(0)}\right]}\psi^{(1)},\psi^{(1)}\right)&=\left|\left(\psi^{(0)},\psi^{(1)}\right)\right|^2\\&=\left(\cos\frac{\pi}{2k}\right)^2\end{aligned}$$

this gives

$$\left(U^{(k)\psi}_{\psi,}\right)\geq\left(\cos\frac{\pi}{2k}\right)^{2k}.$$

Since $\operatorname{Tr}U^{(K)}=1$ and $\left(\cos\frac{\pi}{2K}\right)^{2K}\to 1$ as $k\to\infty$, we can apply the result obtained in II.11.: $U^{(k)}$ converges to $P_{[\psi]}$. Hence vur aill is accomplishod.

How far may we use one of the main instruments of "ideal experiments" of phenomenological thermodynamics, namely the so-called semipermeable walls, when dealing with quantum mechanical systems?

In phenomenological thermodynamics, this theorem holds: It 1 and Il are two different states of the same system s, thon it is permissible to assume the existence of a wall which is completely permeable for I and not permeable for II [193]– this is, so to speak, the thermodynamical definition of difference, and therefore of

[193]Cf. for example, the reference in Note 184.

equality also, for two systems. How far is such an assumption permissible in quantum mechanics?

We first show that if $\phi_1,\phi_2,\ldots,\psi_1,\psi_2,\ldots$ is an orthonormal set, then there is a semipermeabie wall which lets the system s in each of the states $^*{}_1,{}^*{}_2,\cdots$ pass through unhindered, and which reflects unchanged the system in each of the states $\psi_1,\psi_2,\ldots$. Systems which are in other states may, on the other hand, be changed by collision with the wall.

The system $\varphi_1,\psi_2,\cdots,\psi_1,\psi_2,\cdots$ can be assumed to be complete, since otherwise it could he made so by additional $x_1,x_2,\ldots$ which one could then add to the $\phi_1,\phi_2,\ldots$. We now choose an operator R with a pure discrete spectrum, and only simple eigenvalues $\lambda_1,\lambda_2,\ldots,\mu_1,\mu_2,\ldots$ whose eigenfunctions are $\phi_1,\phi_2,\ldots,\psi_1,\psi_2,\ldots$ respectively. In fact, lot the $\lambda_{\mathrm{n}}<0$ and the $\mu_{\mathrm{n}}>0$. Let the quantity $\mathfrak{R}$ belong to R. We construct many windows in the wall, each of which is defined as follows: each "molecule" $\mathbf{K}_1,\ldots,\mathbf{K}_{\mathrm{N}}$ of our gas (we are again considering U-gases at the temperature $T>0$) is detained there, opened, the quantity $\mathfrak{R}$ measured on tho system s_1 or s_2 or ... $s_{\bar{N}}$ contained in it. Then the box is closed again, and according to whether the measured value of $\mathfrak{R}$ is <0 or >0, the box, together with its contents, penetrates the window or is reflected, with unchanged momentum. That this contrivance satisfies the

desired end is clear – it remains only to discuss what changes remain in it after such collisions, and how closely it is related to the so-called "Maxwell's demon" of thermodynamics. [194]

In the first place, it must be said that since the measurement (under certain circumstances) changes the

state of **S**, and perhaps its energy expectation value also, this difference in the mechanical energy must be added or absorbed by the measurement action, in the sense of the firsi law of thermodynamics (for example, by installing a spring which can be extended or compressed, or something similar). Since it is a case of a purely automatically functioning measuring mechanism, and since only mechanical (not heat!) energies are transformed, certainly no entropy changes occur, and at present, only this is of importance to us. (If s is in one of the states $\phi_1, \phi_2, \cdots, \psi_1, \psi_2, \cdots$, then the $\mathfrak{R}$ measurement does not, in general, change s, and no compensating changes remain in the measuring apparatus.)

The second point is more doubtful. our arrangement is rather similar to "Maxwoll's demon," i.e., to a semi-permeable wall which transmits molecules coming from the right and reflects those coming from the left. If we insert such a wall in the midst of a container filled with a gas, then all the gas is soon on the left hand side -i.e., the volume is halved without entropy consumption. This means an uncompensated entropy increase of the gas, and therefore, by the second law of thermodynamics, such a wall cannot exist. Nevertheless, our semi-permeable wall is essentially different from this thermodynamically unacceptable one; because reference is made with it only to the internal properties of the "molecules" $\mathbf{K}_1, \ldots, \mathbf{K}_\mathrm{N}$ (i.e., the state of $\mathbf{s}_1$ or ... or $\mathbf{s}_\mathrm{N}$ enclosed therein), and not to the exterior (i.e., whether it comes from the right or left, or something similar). This, however, is the decisive circumstance. A thorough going analysis of this question is made possible by the researches of L. Szilard, which clarified the nature of the semi-permeable wall, "Maxwell's demon," and the general role of the "intervention of an intelligent being in thermodynamical systems." We cannot go any further into these things here, especially since the reader can find a treatment of this in the references to Note 194.

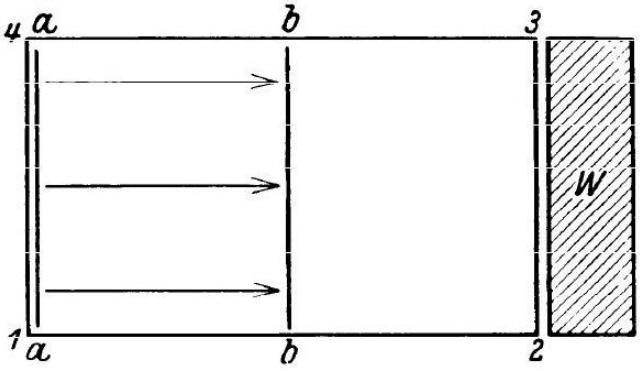
In particular, the above treatment shows that two states ϕ, ψ of the system **s** can be certainly divided by a semi-permeable wall if they are orthogonal. We now want to prove the converse: it ϕ, ψ are not orthogmal, then the assumption of such a somi-permeable wall contradicts the second law of thermodynamics. That is, the necessary and sufficient condition for the separability by semipermeable walls is $(\phi, \psi) = 0$, and not, as in classical theory, $\phi \neq \psi$ (we write ϕ, ψ instead of the I, II used above). This clarifies an old paradox of the classical form of thermodynamics, namely, the uncomfortable discontinuity in the operations with semi-permeable walls: states whose differences are arbitrarily small are always 100% separable, the absolutely equal states are in general not separable: We now have a continuous transition: It will be seen that lood separability exists only for $(\phi, \psi) = 0$ and for increasing (ϕ, ψ) it becomes steadily worse. Finally, at maximum (ϕ, ψ), i.e., $|(\phi, \psi)| = 1$ (here $|| \phi|| = ||\psi|| = 1$, and therefore it follows from $|(\phi, \psi)| = 1$ that $\phi = c\psi, c$ constani, $|c| = i$), the states ϕ, ψ arc identical, and the separation is completely impossible.

In order to carry out these considerations, we must anticipate the end result of this section, the value of the entropy of the U-ensemble. Naturally we shall not use this result in its derivation.

Let us then assume that there is a semi-permeable wall separating ϕ and ψ. We shall then prove $(\phi, \psi) = 0$. We consider a $\frac{1}{2}\left(P_{[\phi]} + P_{[\psi]}\right)$ gas (i.e., of $N/2$ systems in the state ϕ and N/2 systems in the state ψ, the trace of this operator is 1), and choose $\boldsymbol{V}$ (i.e., $\overline{\mathbf{K}}$), and **T** so that the gas is ideal. Let $\overline{\mathbf{K}}$ have the longitudinal cross section shown in Fig. 3: 12341 . We insert a semi-permeable wall at one end aa , and then move it halfway, up to the center bb . The temperature of the gas is kept fixed by contact with a large heat reservoir **w** of temperature **T**

[8194]Cf. the reference in Note 185. The reader will find a detailed discussion of the difficulties connected with the concept of "Maxwell's demon" in L. Szilard, Z. Physik, 53 (1929).

at the other end 23 .



In this process, nothing happens to the ϕ molecules, but the ψ molecules are pushed into the right half of $\bar{N}$ (between bb and 23). That is, the $\frac{1}{2}\left(\mathrm{P}_{[\phi]}+\mathrm{P}_{[\psi]}\right)$ gas is a 1:1 mixture of a $P_{[\infty]}$ gas and a $P_{[w]}$ gas. Nothing happens to the former, but the latter is isothermally compressed to one half its original volume. From the equation of state of the ideal gas, it follows that in this process the mechanical work $\frac{N}{2}\kappa\,\boldsymbol{T}\ln 2$ is performed ($N/2$ is the number of the molecules of the $P_{[\psi]}$ gas, κ is Boltzmann's constant), [195] and since the energy of the gas is not changed (because of the isothermy), [196] this quantity of energy is taken over by the heat reservoir The entropy change of the reservoir is then

[195] If an ideal gas consists of M molecules, then its prossure is $p-\mathrm{M}_{\kappa}\boldsymbol{T}$. In the compression from the volume $\boldsymbol{\gamma}_1$ to the volume $\boldsymbol{\gamma}_2$ therefore, the mechanical work

$$\int_{\gamma_1}^{\gamma_2}\mathrm{p}\mathrm{d}\boldsymbol{V}=\mathrm{M}\kappa\boldsymbol{T}\int_{\gamma_1}^{\gamma_2}\frac{\mathrm{d}\boldsymbol{V}}{\boldsymbol{V}}=\mathrm{M}\kappa\boldsymbol{T}\ln\frac{\boldsymbol{\gamma}_2}{\boldsymbol{\gamma}_1}$$

is done. In our case, $\mathrm{M}=\mathrm{N}/2,\boldsymbol{\gamma}_1=\boldsymbol{\gamma}/2,\boldsymbol{\gamma}_2=\boldsymbol{\gamma}$. [196] The energy of an ideal gas, as is well known, depends only on its temperature.

$\mathbf{Q}/\mathbf{T}=\mathrm{N}\kappa\cdot\frac{1}{2}\ln 2$ (see Note 186).

After this process, the half of the original gas is present to the left of bb , i.e., $N/4$ molecules. To the right of by on the other hand, there is the half of the original $P_{[\varphi]}$ gas, i.e., $N/4$ molecules, and the entire $P_{[\psi]}$ gas, i.e., $N/2$ molecules – therefore a total of $3N/4$ molecules of a $\frac{1}{3}P_{[\phi]}+\frac{2}{3}P_{[\psi]}$ gas. We compress or expand these gases to the volumes $\gamma/4$ and $3\mathscr{N}/4$ respectively, and mechanical work is again taken from or given to the heat reservoir $\mathbf{w}$: this amounts to $\frac{N}{4}\kappa\mathbf{T}\ln 2$ and $\frac{3N}{\frac{1}{4}}\kappa\mathbf{T}\ln\frac{3}{2}$ respectively (see Note 195), and the entropy increase of the reservoir is then $\mathrm{N}_{\kappa}\cdot\frac{1}{4}\ln 2$ and $-\mathrm{N}_{\kappa}\cdot\frac{3}{4}\ln\frac{3}{2}$ respectively. Altogether:

$$\mathrm{N}_{\kappa}\cdot\left(\frac{1}{2}\ln 2+\frac{1}{4}\ln 2-\frac{3}{4}\ln\frac{3}{2}\right)=\mathrm{N}_{\kappa}\cdot\frac{3}{4}\ln\frac{4}{3}.$$

Finally, we have a $P_{[\Phi]}$ and a $P_{[\psi]}$ gas of N/4 and 3N/4 molecules respectively, with the respective volumes $\tilde{\gamma}/4$ and $3\tilde{\gamma}/4$. Originally there was a $\frac{1}{2}\mathrm{P}_{[\phi]}+\frac{1}{2}\mathrm{P}_{[\psi]}$ gas of N molecules in the volume ψ j.e., if we wjll, two $\frac{1}{2}P_{[\Phi]}+\frac{1}{2}P_{[\psi]}$ gases with $N/4$ and $3N/4$ molecules respectively, in the volumes r and $3N/4$ respectively. The change effected by the entire process is then this: $N/4$ molecules in volume $\mathscr{V}/4$ changed from a $\frac{1}{2}P_{[\Phi]}+\frac{1}{2}P_{[\psi]}$ gas into a $P_{[\Phi]}$ gas, $3N/4$ molecules in the volume $3V/4$ changed from $A\frac{1}{2}P_{[\phi]}+\frac{1}{2}P_{[\psi]}$ gas into a $\frac{1}{3}P_{[\phi]}+\frac{2}{3}P_{[\psi]}$ gas, and the entropy of $\mathbf{w}$ increased by $\mathrm{N}_{\kappa}\cdot\frac{3}{4}\ln\frac{4}{3}$. Since the process was reversible, the entire entropy increase must be zero, i.e., the two gas-entropy changes must entirely compensate the change of entropy of $\mathbf{w}$. We must therefore find the entropy changes of the gases.

As we shall see, a U-gas of N molecules has the entropy $-\mathrm{M}_{\kappa}\cdot\mathrm{Tr}(\mathrm{U}\ln\mathrm{U})$ if that of the $\mathrm{P}_{[x]}$-gas of equal volume and temperature is taken as zero (see above). If therefore U has a pure discrete spectrum with

the eigenvalues $w_1,w_2,\ldots$, then this is

$$-M_k \cdot \sum_{n=1}^{\infty} w_n \ln w_n$$

(therefore x ln x is to be set equal to 0 for x = 0). As may easily be calculated, $P_{[\phi]}$, $\frac{1}{2}P_{[\phi]} + \frac{1}{2}P_{[\psi]}$,
$\frac{1}{3}P_{[\Phi]} + \frac{2}{3}P_{[\psi]}$ have the respective eigenvalues 1,0 and $\frac{1+\alpha}{2}, \frac{1-\alpha}{2}, 0$ and

$$\frac{3+\sqrt{1+8\alpha^2}}{6}, \frac{3-\sqrt{1-8\alpha^2}}{6}, 0$$

($\alpha = |\ \phi, \psi)\ |$, therefore $\geq 0, \leq 1$), in which the multiplicity of the zero is always infinito, but in which the others are simple. [197] Therefore the entropy of the

[197] We delemine the eigenvalues of $aP_{[\phi]} + bP_{[\psi]} =$ The requirement is

$$\left(aP_{[\phi]} + bP_{[\psi]}\right) f = \lambda f.$$

Since the left side is a linear combination of the ϕ, ψ, the right side is also, therefore also f, is too if $\lambda \neq 0$. $\lambda = 0$ is certainly an infinitely multiple eigenvalue, since each f orthogonal to ϕ, ψ belongs to it. It therefore suffices to consider $\lambda \neq 0$ and f = xϕ + yψ (let ϕ, ψ be Iinearly independent, otherwise, $\psi = c_\psi$, $|c| - 1$, and the two states are identical).

The above equation then becomes

$$a(x + y(\psi, \phi)) \cdot \phi + b(x(\phi, \psi) + y) \cdot \psi = \lambda x \cdot \phi + \lambda y \cdot \psi,$$

i.e.,

$$\mathrm{a} \cdot \mathrm{x} + \overline{\mathrm{a}(\phi, \psi)} \cdot \mathrm{y} = \lambda \cdot \mathrm{x},\ \ \mathrm{b}(\phi, \psi) \cdot \mathrm{x} + \mathrm{b} \cdot \mathrm{y} = \lambda \cdot \mathrm{y}.$$

gas has increased by
$-\frac{N}{4}\kappa \cdot 0 - \frac{3N}{4}\kappa \cdot \left(\frac{3+\sqrt{1+8\alpha^2}}{2} \ln \frac{3:\sqrt{1,8\alpha^2}}{6} + \frac{3-\sqrt{1+8\alpha^2}}{2} \ln \frac{3-\sqrt{1+8\alpha^2}}{6} \right)$
$+N_K \cdot \left(\frac{1+\alpha}{2} \ln \frac{1+\alpha}{2} + \frac{1-\alpha}{2} \ln \frac{1-\alpha}{2} \right)$.
This should equal 0 when the entropy increase $N_k \cdot \frac{3}{4} \ln \frac{4}{3}$ of **W** is added to it. If we divide by $N_\kappa/4$ then we have
$-\frac{3+\sqrt{1+8u^2}}{2} \ln \frac{3+\sqrt{1+8u^2}}{6} - \frac{3-\sqrt{1+8u^2}}{2} \ln \frac{3-\sqrt{1:8a^2}}{6}$
$+2(1+\alpha) \ln \frac{1+\alpha}{2} + 2(1-\alpha) \ln \frac{1-\alpha}{2} + 3 \ln \frac{4}{3} = 0$

Also $0 \leq \alpha \leq 1$.

Now it can easily be seen that the left side increases monotonically as α varies from 0 to 1, [198]

The determinant of these equations must vanish:

$$\left| \begin{array}{ll} a - \lambda, & \overline{a(\phi, \psi)} \\ b(\phi, \psi), b - \lambda & \end{array} \right| = 0, (a - \lambda)(b - \lambda) - ab|(\phi, \psi)|^2 = 0,$$

$$\lambda^2 - (a + b)\lambda + ab\left(1 - \alpha^2\right) = 0,$$

$\lambda = \frac{a+b \pm \sqrt{(a+b)^2 - 4ab(1-\alpha^2)}}{2} = \frac{a+b \pm \sqrt{(a-b)^2 + 4\alpha^2 ab}}{2}$

If we put a = 1, b = 0 or a = 1/2, b = 1/2 or a = 1/3, $b = 2/3$ respectively, then the formulas of the text are obtained.

[198] Since $(x \ln x)' = \ln x + 1$, therefore
and in fact from 0 to $3 \ln \frac{4}{3}$; therefore α must be zero (for $\alpha \neq 0$ the inverse process to that described

$$\left(\frac{1+y}{2} \ln \frac{1+y}{2} + \frac{1-y}{2} \ln \frac{1-y}{2} \right)' = \frac{1}{2} \left(\ln \frac{1+y}{2} + 1 \right) - \frac{1}{2} \left(\ln \frac{1-y}{2} + 1 \right)$$
$$= \frac{1}{2} \ln \frac{1+y}{1-y}$$

and the derivative of our expression is

$$-3\cdot\frac{1}{2}\ln\frac{3+\sqrt{1+8\alpha^2}}{3-\sqrt{1+8\alpha^2}}\cdot\frac{1}{3}\frac{8\alpha}{\sqrt{1+8\alpha^2}}+4\cdot\frac{1}{2}\ln\frac{1+\alpha}{1-\alpha}$$
$$=2\left(\ln\frac{1+\alpha}{1-\alpha}-\frac{2\alpha}{\sqrt{1+8\alpha^2}}\ln\frac{3+\sqrt{1+8\alpha^2}}{3-\sqrt{1+8\alpha^2}}\right)$$

That this is >0 means that

$$\ln\frac{1+\alpha}{1-\alpha}>\frac{2\alpha}{\sqrt{1+8\alpha^2}}\ln\frac{3+\sqrt{1+8\alpha^2}}{3-\sqrt{1+8\alpha^2}},$$

i.e.,

$$\frac{1}{2\alpha}\ln\frac{1+\alpha}{1-\alpha}>\frac{2}{3}\cdot\frac{1}{2\beta}\ln\frac{1+\beta}{1-\beta},\quad \beta=\frac{\sqrt{1+8\alpha^2}}{3}.$$

We shall prove this with 8/9 in place of 2/3. Since $1-\beta^2=\frac{8}{9}(1-\alpha^2)$ and $\alpha<\beta$ (which follows from the former, since $\alpha<1$), this means that

$$\frac{1-\alpha^2}{2\alpha}\ln\frac{1+\alpha}{1-\alpha}>\frac{1-\beta^2}{2\beta}\ln\frac{1+\beta}{1-\beta}$$

and this is proved it $\frac{1-x^2}{2x}\ln\frac{1+x}{1-x}$ is shown to be monotonically decreasing in $0<x<1$. This last property, however, follows, for example, from the power series expansion:
would be entropy decreasing, contrary to the second law). Therefore $(\phi,\psi)=0$ has been proved.

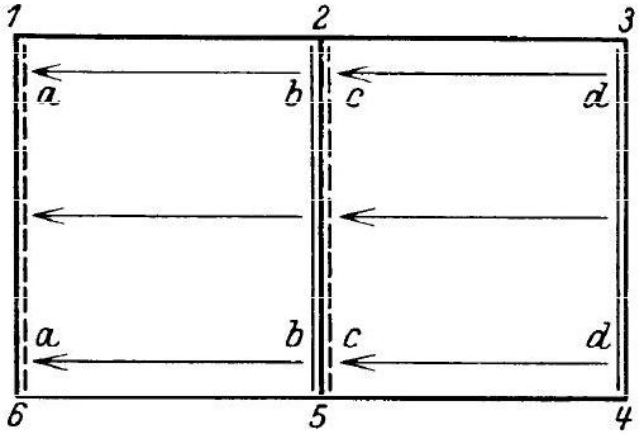
After these preparations, we can go on to determine the entropy of a U gas of N molecules in the volume $\mathscr{V}$ and at temperature $\mathbf{T}$– i.e., more precisely, its entropy excess with respect to a $P_{[\Phi]}$ gas under the same conditions. By our earlier remarks and in the sense of the normalization given above, this is the entropy of a U-ensemble of N individual systems. Let $\operatorname{Tr}U=1$, as was done above.

The U, as we know, has a pure discrete spectrum $w_1,w_2,\ldots$ with $w_1\geq 0, w_2\geq 0,\ldots, w_1+w_2+\ldots=1$. Let the corresponding eigentunctions be $\phi_1,\phi_2,\ldots$. I'hen

$$U=\sum_{n=1}^{\infty}{w_n}^P[\Phi_n]$$

(cf. IV.3.). Consequently, our U-gas is composed of a mixture of $\mathrm{P}_{[\psi_1]},\mathrm{P}_{[\psi_2]},\cdots$ gases of w_1 N, w_2 N,... molecules respectively, all in the volume $\mathscr{V}$. Let. $\mathbf{T},\mathscr{V}$ again be such that all these gases are ideal, and let $\overline{\mathbf{K}}$ be of rectangular cross section. Now we will apply the following reversible interventions in order to separate the $\phi_1,\phi_2,\ldots$ molecules from each other (cf. Fig. 4.). We add an equally large rectangular box $\overline{\mathbf{K}}'$ (1 2 5 6) on to $\overline{\mathbf{K}}$ (2 3452), and replace the common wall 25 by two walls lying next to each other. Let the one (2 5) be fixed and semi-permeable – transparent for ϕ_1, but opaque for $\varphi_2,\phi_3,\cdots$; let the other wall (bb) be movable, but an ordinary, absolutely impenetrable wall. In addition, we insert another semi-permeable wall at dd ,

$$\frac{1-x^2}{2x}\ln\frac{1+x}{1-x}=\left(1-x^2\right)\left(1+\frac{x^2}{3}+\frac{x^4}{5}+\cdots\right)$$
$$=1-\left(1-\frac{1}{3}\right)x^2-\left(\frac{1}{3}-\frac{1}{5}\right)x^4-\cdots\Big)$$



close to 34 , which is transparent for $\phi_2, \phi_3, \cdots$ and opaque for ϕ_1. We then push *bb* and *dd*, the distance between them being kept constant, to aa and cc respoctively (i.e., close to 16 and 25 respectively). By this means, the $\Phi_2, \Phi_3, \cdots$ are not affected, but the Φ_1 are forced to remain between the moving walls bb, dd. Since the distance between these walls is a constant, no work is done (against the gas pressure), and no heat development takes place. Finally, we replace the walls 25, cc by a rigid, absolutely impenetrable wall 25 , and remove aa – in this way the boxes $\overline{\mathbf{K}}, \overline{\mathbf{K}}'$ are restored. There is, however, this change. All Φ_1 molecules are in $\mathbf{K}'$, i.e., we have transferred all these from $\overline{\mathbf{K}}$ into the same sized box $\overline{\mathbf{K}}'$, reversibly and without any work being done, without any evolution of heat or tenperature change. [199]

Similarly, we "tap off" the $\phi_2, \phi_3, \ldots$ molecules into the equal boxes $\overline{\mathbf{K}}'', \overline{\mathbf{K}}''', \ldots$, and have finally, $P_{[\phi_1]}, P_{[\phi_2]}, \cdots$ gases, consisting of $w_1 N, w_2 N, \ldots$ mole-

cules, respectively, each in the volume $\mathscr{V}$. We now compress these isothermally to the volumes $w_1\gamma, w_2\gamma, \ldots$ respectively. We must therefore add the quantities of heat w_1 Nκ T$\ln w_1, w_2$NκT$\ln w_2, \ldots$, respectively, as compensation, from a large heat reservoir (of temperature **T**, so that the process may be reversible; the quantities of heat are all less than zero), since the amounts of work done in compressing the individual gases are the negatives of these values (cf. Note 191). Therefore, the entropy increase for this procese mounts to

$$\sum_{n=1}^{\infty} w_n N_k \cdot \ln w_n.$$

Finally, we transform the $P_{[\phi_1]}, P_{[\phi_2]}, \cdots$ gases all ints a $P_{[\phi]}$ gas (reversibly, cf. above, Φ an arbitrarily chosen state). We have then only $P_{[\phi]}$ gases of $W_1 N, W_2 N, \ldots$ molecules respectively, in the volumes $w_1\%, w_2\%, \ldots$. Since all of these are identical and of equal density (N/N), we can mix them, and this is also reversible. We then obtain a $P_{[\oplus]}$ gas of N molecules in the volume $\mathscr{V}$ (since

$$\sum_{n=1}^{\infty} w_n = 1\Bigg)$$

Consequently, we have carried out the desired reversible process. The entropy has increased by

$$N_\kappa \sum_{n=1}^{\infty} w_n \ln w_n$$

and since it is zero in the final state, it was

[8] [199] Cf., for example, the reference in Note 184 for this artifice which is characteristic of the phenomenological thermodynamical method.

$$-N_\kappa \sum_{n=1}^{\infty} w_n \ln w_n$$

in the initial state.

Since U has the eigenfunctions $\phi_1, \phi_2, \cdots$ with the eigenvalues $W_1, W_2, \ldots, U$ in U has the same eigenfunctions, but the eigenvalues $w_1 \ln w_1, w_2 \ln w_2, \ldots$. Consequently,

$$\mathrm{Tr}(U \ln U) = \sum_{n=1}^{\infty} w_n \ln w_n$$

It may be observed that $w_n \geq 0, \leq 1$, therefore $\mathrm{w_n} \ln \mathrm{w_n} \leq 0$, and in fact equals zero only for $\mathrm{w_n} = 0, 1$. Note that for $w_n = 0, w_n$ In w_n is to be taken equal to zero – this follows from the circumstance that in our above considerations, the vanishing w_n are not considered at all. The same conclusion may also be obtained from continuity considerations.

We have then determinod tho entropy of a $U-$ ensemble, consisting of N individual systems, to be $-N\kappa \,\mathrm{Tr}(U \ln U)$. The previous discussion on $W_n \ln W_n$ shows that it is always ≥ 0, and in order that it be 0 , all W_n must be zero or 1 . Since $\mathrm{Tr}\, U = 1$, exactly une $\mathrm{w_n} = \mathrm{i}$, while the others - 0 , thorofore $\mathrm{U} = \mathrm{P}_{[\phi]}$ That is, the states have an entropy = 0, and the other mixtures have entropies > 0.

28.2.3 3. Reversibility and Equilibrium Problems

We can now prove the irreversibility of the measurement process as asserted in V.1. For example, if U is a state, $U = P_{[\phi]}$, then in the measurement of a quantity M whose operator R has the eigenfunctions $\phi_1, \phi_2, \cdots$, it goes over into the ensemble

$$U' = \sum_{n=1}^{\infty} \left(P_{[\phi]}\phi_n, \phi_n\right) \cdot P_{[\phi_n]} = \sum_{n=1}^{\infty} |(\phi, \phi_n)|^2 \, P_{[\phi_n]}$$

and if U' is not a state, then an entropy increase has

occurred (the entropy of U was 0 , that of U' is > 0), so that the process is irreversible. If U', too, is to be a state, it must be a $\mathrm{P}_{[\phi_n]}$, and since the ϕ_n are its eigenfunctions, this means that all $i\,(\phi, \phi_n)\, i^p = 0$ except one (that one - 1) 1.0., \$ is orthogonal to all $\Phi_n, n \neq \bar{n} - -$ but then $\phi = c\phi_{\bar{n}}$, where $|c| = 1$, and therefore $P_{[\$]} = P_{[\phi,n]}, U = U'$. Therefore, each measurement on a state is irreversible, unless the eigenvalue of the measured quantity (i.e., this quantity in the given state) has a sharp value, in which case the measurement does not change the state at all. As we see, the noncausal behavior is thus unambiguously related to a certain concomitant thermodynamical phenomena.

We shall now discuss in complete generality when the process 1.,

$$U \to U' = \sum_{n=1}^{\infty} (U\Phi_n, \Phi_n) \cdot P_{[\phi_n]}$$

incroasos the entropy-

U has the entropy $-\mathbb{N}\kappa \,\mathrm{Tr}(U \ln U)$. If $w_1, w_2, \ldots$ are its eigenvalues and $\psi_1, \psi_2, \ldots$ its eigenfunctions then this is equal to

$$-N_\kappa \sum_{n=1}^{\infty} w_n \ln w_n = -N_\kappa \sum_{n=1}^{\infty} \left(U_{\Psi_n}, \psi_n\right) \ln \left(U_{\Psi_n}, \psi_n\right).$$

U has the eigenvalues $\left(U\phi_1, \phi_1\right), \left(U\phi_2, \phi_2\right), \ldots$, and therefore its entropy is

$$-N\kappa \sum_{n=1}^{\infty} (U\Phi_n, \Phi_n) \ln (U\Phi_n, \Phi_n) .$$

Consequently the entropy of U is $\geq$ that of U' depending on whether

- $\sum_{n=1}^{\infty} (U\psi_n, \psi_n) \ln (U\psi_n, \psi_n) \lessgtr \sum_{n=1}^{\infty} (U\phi_n, \phi_n) \ln (U\phi_n, \phi_n)$.

We next show that in $^*, \geq$ holds in any case, i.e., that the process $U \to U'$ is not entropy-diminishing – this is indeed clear thermodynamically, but it is of importance for our subsequent purposes to have a purely mathematical proof of this fact. We proceed in such a way that U, and with it $\psi_1, \psi_2, \ldots$, are fixed, while the $\phi_1, \phi_2, \cdots$ run through all complete orthonormal sets.

Next, for reasons of continuity, we may limit ourselves to such sets $\phi_1, \phi_2, \cdots$ in which only a finite number of $_i$n are different from the corresponding ψ_n Then, for example, let $\phi_{11} = \psi_{11}$ for n > M. Then the $\phi_n, n \leq M$ are linear combinations of the $\psi_n, n \leq M$, and conversely – therefore,

$$\Phi_m = \sum_{n=1}^{M} x_{mn} \psi_n \quad (m = 1, \ldots, M)$$

and the M dimensional matrix (x_{mn}) is obviously unitary. Wo obtain ($\mathrm{U_w}, \psi_\mathrm{m}$) = w_m and, as can casily be calculated,

$$(U\Phi_m, \Phi_m) = \sum_{n=1}^{N} w_n |x_{mn}|^2 \quad (m = 1, \ldots, M)$$

so that

$$\sum_{m=1}^{M} w_m \ln w_m \geq \sum_{m=1}^{M} \left(\sum_{n=1}^{M} w_n |x_{mn}|^2 \right) \ln \left(\sum_{n=1}^{M} w_n |x_{mn}|^2 \right)$$

is to be proved. Since the right side is a continuous function of the M^2 bounded variables π_mn, it has a maximum, and it also assumes its maximum value ($\{\mathrm{x_{mn}}$) unitary); since the left side is its value for

$$x_{mn} \left\{ \begin{array}{lll} = 1 & \text{for} & m = n \\ = 0 & \text{for} & m \neq n \end{array} \right|$$

we must show: the maximum just mentioned occurs at this $\mathrm{x_{mn}}$-complex.

Therefore, let. $x^2_{mn} (m, n = 1, \ldots, M)$ be a set of values for which the maximum occurs. If we multiply the matrix (x°_{mn}) by the unitary matrix

$$\left\{ \begin{array}{ccccc} \alpha, & \beta, & 0, & \vdots & 0 \\ -\bar{\beta}, & \bar{\alpha}, & 0, & \vdots & 0 \\ 0, & 0, & 1, & \vdots & 0 \\ \cdots\cdots & \cdots\cdots & \cdots & \cdots & \\ 0 & 0 & 0 & \vdots & 1 \end{array} \right\}, |\alpha|^2 + |\beta|^2 = 1$$

then we obtain a unitary matrix $\{x'_{mn}\}$, and therefore an acceptable x_{mn}-complex. Now, let $\alpha = \sqrt{1 - \epsilon^2}, \beta = \theta\epsilon$ (ϵ real, $|\theta| = 1$) . ϵ will be small, and in the following we shall carry in

our calculations the $1, \epsilon, \epsilon^2$ terms only, and noglect the $\epsilon^3, \epsilon^4, \ldots$ terms. Then $\alpha \approx 1 - \frac{1}{2}\epsilon^2$, and in the new matrix $\{x'_{mn}\}$,

$$\begin{aligned} x'_{1n} &\approx \left(1 - \frac{1}{2}\epsilon^2\right) x^{\circ}_{1n} + \theta\epsilon x^{\circ}_{2n} \\ x'_{2n} &\approx -\bar{\theta}\epsilon x^{\circ}_{1n} + \left(1 - \frac{1}{2}\epsilon^2\right) x^{\circ}_{2n} \\ x'_{mn} &= x^{\circ}_{mn} (m \geq 3) \end{aligned}$$

therefore

$$\begin{aligned} \sum_{n=1}^{M} w_n \left|x'_{1n}\right|^2 \approx \sum_{n=1}^{M} w_n \left|x^{\circ}_{1n}\right|^2 + \sum_{n=1}^{M} 2w_n \Re\left(\bar{\theta} x^{\circ}_{1n} \bar{x}'_{2n}\right) \cdot \epsilon \\ + \sum_{n=1}^{M} w_n \left(-\left|x^{\circ}_{1n}\right|^2 + \left|x^{\circ}_{2n}\right|^2\right) \cdot \epsilon^2 \end{aligned}$$

$$\begin{aligned} \sum_{n=1}^{M} w_n \left|x'_{2n}\right|^2 = &\sum_{n=1}^{M} w_n \left|x^{\circ}_{2n}\right|^2 \\ &- \sum_{n=1}^{M} 2w_n \Re\left(\bar{\theta} x^{0}_{1n} \bar{x}^{0}_{2n}\right) \cdot \epsilon \\ &- \sum_{n=1}^{M} w_n \left(-\left|x^{0}_{1n}\right|^2 + \left|x^{0}_{2n}\right|^2\right) \cdot \epsilon^2 \end{aligned}$$

$$\sum_{n-1}^{M} w_n \left|x^{i}_{mn}\right|^2 = \sum_{n=1}^{M} w_n \left|x^{0}_{mn}\right|^2$$

If we substitute these expressions in f'(x) = x In x , in which

$$f'(x) = \ln x + 1, f''(x) = \frac{1}{x}$$

and add the resulting expressions togother, then

$$\begin{aligned} &\sum_{m=1}^{M} \left(\sum_{n=1}^{M} w_n \left|x'_{mn}\right|^2\right) \ln \left(\sum_{n=1}^{M} w_n \left|x'_{mn}\right|^2\right) \\ &= \sum_{m=1}^{M} \left(\sum_{n=1}^{M} w_n \left|x^{o}_{mn}\right|^2\right) \ln \left(\sum_{n=1}^{M} w_n \left|x^{o}_{mn}\right|^2\right) \\ &+ \left(\ln \left(\sum_{n=1}^{M} w_n \left|x^{\circ}_{1n}\right|^2\right) - \ln \left(\sum_{n=1}^{M} w_n \left|x^{\circ}_{2n}\right|^2\right)\right) \cdot \sum_{n=1}^{M} 2w_n \Re\left(\bar{\theta} x^{\circ}_{1n} \bar{x}^{\circ}_{2n}\right) \cdot \epsilon \\ &+ \left[-\left(\ln \left(\sum_{n=1}^{M} w_n \left|x^{\circ}_{1n}\right|^2\right) - \ln \left(\sum_{n=1}^{M} w_n \left|x^{\circ}_{2n}\right|^2\right)\right) \left(\sum_{n=1}^{M} w_n \left|x^{\circ}_{1n}\right|^2\right)\right. \\ &- \left(\sum_{n=1}^{M} w_n \left|x^{o}_{2n}\right|^2\right) \\ &\left. + \frac{1}{2} \left(\frac{1}{\sum_{n=1}^{M} w_n \left|x^{o}_{1n}\right|^2} + \frac{1}{\sum_{n=1}^{M} w_n \left|x^{o}_{2n}\right|^2}\right) \left(\sum_{n=1}^{M} 2w_n \Re\left(\bar{\theta} x^{o}_{1n} \bar{x}^{o}_{2n}\right)\right)^2\right] \cdot \epsilon^2. \end{aligned}$$

In order that the first term on the right be the maximum value, the ϵ coefficient must be $= 0$, and the ϵ^2 coefficient ≤ 0. The former has two factors,

$$\ln\left(\sum_{n=1}^{M} w_n \left|x_{1n}^0\right|^2\right) - \ln\left(\sum_{n=1}^{M} w_n \left|x_{2n}^0\right|^2\right)$$

and

$$\sum_{n=1}^{M} 2w_n \mathfrak{R}\left(\bar{\theta} x_{1n}^{\circ} \bar{x}_{2n}^{\circ}\right)$$

If the first is zero, then the first term in the ϵ^2 coefficient $= 0$ (this is always ≤ 0), so that the second term, which is clearly ≥ 0 always, must vanish in order that the entire coefficient be ≤ 0. This means that

$$\sum_{n=1}^{M} 2w_n \mathfrak{R}\left(\bar{\theta} x_{1n}^{\circ} \bar{x}_{2n}^{\circ}\right) = 0$$

Therefore, the second factor of the ϵ coefficient is $= 0$ in any case, which can also be written

$$2\mathfrak{R}\left(\bar{\theta} \sum_{n=1}^{M} w_n x_{1n}^{\circ} \bar{x}_{2n}^{\circ}\right)$$

Since this goes over into the absolute value of the

$$\sum_{n=1}^{M}$$

for appropriate θ, this must disappear:

$$\sum_{n=1}^{M} w_n x_{1n}^{\circ} \bar{x}_{2n}^{\circ} = 0$$

Since we can replace 1,2 by any two different
$k, j = 1, \ldots, M$, we have

$$\sum_{n=1}^{M} w_n x_{kn}^0 \bar{x}_{jn}^0 \text{ for } x \neq j$$

That is, the unitary coordinate transformation with the matrix (x_{mn}°) brings the diagonal matrix with the elements $w_1, \ldots, w_n$ again into diagonal form. Since the diagonal elements are the multipliers (or eigenvalues) of the matrix, they are not changed by the coordinate transformation, and are at most permuted. Before the transformation they were the $w_m (m = 1, \ldots, M)$, afterwards, they are the

$$\sum_{n=1}^{M} w_n \left|x_{mn}^c\right|^2$$

(m $= 1, \ldots,$ $\overline{\text{N}}$). The sums

$$\sum_{n=1}^{M} w_n \ln w_n, \sum_{m=1}^{M} \left(\sum_{n=1}^{M} w_n \left|x_{mn}^0\right|^2\right) \ln\left(\sum_{n=1}^{M} w_n \left|x_{mn}^0\right|^2\right)$$

then have the same values. Hence there is at any rate a maximum at

$$X_{mn}\left\{\begin{array}{lll} =1 & \text{for} & m=n \\ =0 & \text{for} & m\neq n \end{array}\right|$$

too, as was asserted.
Let us determine when the equality holds in *.
If it does hold, then

$$\sum_{n=1}^{\infty}(Ux_n,x_n)\ln(Ux_n,x_n)$$

takes on its maximum value not only for $x_n=\psi_n$
($n=1,2,\dots$) (these are the eigenfunctions of U, cf.
above), but also for $x_n=o_n \quad (n=1,7,\dots) \quad (x_1,x_2,\dots$ running through all complete orthonomal sets). This holds in particular if only the first M among the ϕ_n are transformed (i.e., $x_n=\phi_n$ for $n>M$) and hence, of course, transformed unitarily among each other. Let $\mu_{mn}=(U\phi_m,\phi_n)\,(m,n=1,\dots,M)$, let $v_1,\dots,v_N$ be the eigenvalues of the finite (and at the same time Hermitian and definite) matrix $\{\mu_{mn}\}$, and $\{\alpha_{mn}\}$ ($m,n=1,\dots,M$) the matrix that transforms (μ_{mn}) to the diagonal form. This transtorms the $\phi_1,\cdots,\phi_{\mathrm{M}}$ into $\omega_1,\dots,\omega_{\mathrm{M}}$,

$$\Phi_m=\sum_{n=1}^{M}\alpha_{mn}\omega_n$$

$(m=1,\dots,M)$, and then

$$U_n=v_n\omega_n,\ \text{therefore}\qquad (\omega_m,\omega_n)=\left\{\begin{array}{ll} v_n, & \text{for } m=n \\ 0, & \text{for } m\neq n \end{array}\right. .$$

For

$$\xi_m=\sum_{n=1}^{M}x_{mn}\omega_n$$

($m=1,\dots,M$, let $\{x_{mn}\}$ also be unitary),

$$(U\xi_k,\xi_j)=\sum_{n-1}^{M}v_nx_{kn}\bar{x}_{jn}.$$

Because of the assumption on the $\phi_1,\cdots,\phi_{\mathrm{M}}$,

$$\sum_{n=1}^{M}\left(\sum_{n=1}^{M}v_n\left|x_{mn}\right|^2\right)\ln\left(\sum_{n=1}^{M}v_n\left|x_{mn}\right|^2\right)$$

takes on its maximum for $x_{mn}=\alpha_{mn}$. According to our previous proof, it follows from this that

$$\sum_{n=1}^{M}v_n\alpha_{kn}\bar{\alpha}_{jn}=0$$

fror $k\neq j$, i.e., $\quad (U\phi_k,\phi_j)=0$ for $k\neq j$, $k,j=1,\dots,M$.
This must hold for all M, therefore $U\phi_k$ is orthogonal to all $\Phi_j, k\neq j$– hence it is equal to $w_k'\phi_k$ (w_k' a constant). Consequently, the $\phi_1,\phi_2,\dots$ are the eigenfunctions of U. The

corresponding eigenvalues are $w_1, w_2', \cdots$ (and therefore a pormutation of the $w_1, w_2, \ldots$). Rut under these circumstances,

$$U' = \sum_{n=1}^{\infty} (U\Phi_n, \Phi_n) \cdot P_{[\hat{t}_n]} = \sum_{n=1}^{\infty} w_n' \cdot P_{[\hat{t}_n]} = U.$$

We have therefore found.
The process 1.,

$$U \to U' = \sum_{n=1}^{\infty} (U\Phi_n, \Phi_n) \cdot P_{[\Phi_n]}$$

($\phi_1, \phi_2, \cdots$ are the eigenfunctions of the operator R of Lhe measured quantity M), novor diminishes the entropy. It actually increases it, unless all $\phi_1, \phi_2, \ldots$ are eigenfunctions of U, in which case $U = U'$.

In the case mentioned moreover, U commutes with R, and this is actually characteristic for it (because it is equivalent to the existence of the common eigenfunctions $\phi_1, \phi_2, \cdots$, cf. TT.10.).

Hence the process 1. is irreversible in all cases in which it effects a change at all.

The reversibility question should now be treated for the processes 1., 2., independently of phenomonological thermodynamics, as was announced as the second point of the program in V.2.. The mathematical method with which this can be accomplished we already know: if the second law of thermodynamics holds, the entropy must be equal to

- No Tr (U 1 n T) , and this may not decrease in any process 1., 2. We must then treat $-\mathrm{N}\kappa\mathrm{Tr}(\mathrm{U}\ln\mathrm{U})$ merely as a calculated quantity, independently of its meaning as entropy, and find out what it does in i., 2. [200]

In 2., we obtain

$$U_t = e^{-\frac{2\pi i}{h}tH} U e^{\frac{2\pi i}{h}tH}$$

from U, i.e., if we designate the unitary operator

$$e^{-\frac{2\pi i}{n}tH}$$

hy $A, U \to T_L = AUA^{-1}$. Since $f \to Af$, because of the unitary nature of A, is an isomorphic mapping of Hilbert space on itself, which transforms each operator P into APA^{-1}, therefore always $F(APA^{-1}) = AH'(P)A^{-1}$. Consequently $U_t \ln U_t = A \cdot U \ln U \cdot A^{-1}$. Henco $\mathrm{Tr}(U_t \ln U_t) = \mathrm{Tr}(U \ln U)$, i.e.; our quantity $-N_\kappa \mathrm{Tr}(U \ln U)$ is constant in 2. We have already ascertained what happens in 1 , and in fact, without reference to the second law of thermodynamics. If U changes (i.e., $U \neq U'$), then - $N\kappa\overline{Ir}(U \text{ in } U)$ increases, while for unchanged U (i.c., $U = U'$; or $\psi_1, \psi_2, \cdots$ eigenfunctions of U; or U, R commutative), it naturally remains unchanged. In an intervention composed of several process 1. and 2. (in arbitrary number and order) - $N\kappa \mathrm{Tr}(U \ln U)$ remains unchanged if each process 1. is ineffective (i.e., causes no change), but in all othor cases it increases.

Therefore, if only interventions 1., 2. are
taken into consideration, then each process 1., which effects a change at all, is irreversible.

It is worth noting, there are also other, simpler

[8]200 Naturally, we could neglect the factor N_κ and consider - $\mathrm{Tr}(\mathrm{U}\ln\mathrm{U})$. Or, preserving the proportionality with the number of elements N, $-N\,\mathrm{Tr}(U \ln U)$.

expressions than $-\mathrm{Tr}(\mathrm{U}\ln\mathrm{U})$ which do not decrease in 1., and are constant in 2.: for example, the largest eigenvalue of $\bar{U}$. Indeed: For 2., it is invariant, as arc all eigenvalues of U– while in 1. , the eigenvalues $W_1, W_2, \ldots$ of U go over into the eigenvalues of U' :

$$\sum_{n=1}^{\infty} w_n \left|x_{1n}\right|^2, \sum_{n=1}^{\infty} w_n \left|x_{2n}\right|^2, \ldots$$

(cf. the earlier considerations of this section), and since, by the unitary nature of the matrix $\{x_{mn}\}$,

$$\sum_{n=1}^{\infty} \left|x_{1n}\right|^2 = 1, \sum_{n=1}^{\infty} \left|x_{2n}\right|^2 = 1, \ldots$$

all these numbers are $\leq$ than the largest w_n. (A maximum w_n cxiste, since all $w_n \geq 0$, and since

$$\sum_{n=1}^{\infty} w_n = 1$$

$\mathrm{w_n} \to 0$.) Now since it is possible so to change U that

$$-\mathrm{Tr}(U\ln U) = -\sum_{n=1}^{\infty} w_n \ln w_n$$

remains invariant, but that the largest w_n decreases, we see that these are changes which are possible according to phenomenological thermodynamics – therefore they are actually possible of execution with our gas processes -but which can never be brought about by successive applications of 1., 2. alone. This proves that our introduction of gas processes was indeed necessary.

Instead of - Tr (U ln U) we can also consider $\mathrm{Tr}(F(U))$ for appropriate functions $F(x)$. That this increases in 1. for $U \neq U'$ (for $U = U'$, as well as in 2., it is of course invariant), can also be proved, as was done for $F(x) = -x\ln x$, if the special properties of
this function, which we used above are also present in $F'(x)$. These are: $F''(x) < 0$, and the monotonic decrease of $F \cdot (x)$; but the latter follows from the former. Therefore, for our non-themodynamical irreversibility considerations, we can use each $\mathrm{Tr}\, F(U)$, if $F(x)$ is a function that is convex from above, i.e., if $F''(x) < 0$ (in $0 \leq x \leq 1$ since all eigenvalues of U lie in that interval).

Finally, it should be shown that the mixing of two ensembles U, V (say in the ratio $\alpha : \beta$: $\alpha > 0, \beta > 0$, $\alpha + \beta = 1$) is also not entropy-diminishing, i.e.,

$$\begin{aligned} &-\mathrm{Tr}((\alpha U + \beta V)\ln(\alpha U + BV)) \\ \geq &-\alpha\,\mathrm{Tr}(U\ln U) - \beta\,\mathrm{Tr}(V\ln V) \end{aligned}$$

This also holds for each convex $F(x)$ in place of $-x\ln x$. The proof is left to the reader. -

We shall now investigate the stationary equilibrium superposition, i.e., the mixture of maximum entropy, when the energy is given. The latter is, of course, to be understood to mean that the expectation value of the energy is prescribed – only this interpretation is admissible, in view of the method indicated in Note 184 for the thermodynamical investigation of statistical ensembles. Consequently, only such mixtures will be allowed, for the U of which $\mathrm{Tr}\, U = 1, \mathrm{Tr}(UH) = E$, where H is the energy operator and $\mathbf{E}$ the prescribed energy expectation value. Under these auxiliary conditions, $-\mathrm{N}_\kappa\,\mathrm{Tr}(\mathrm{U}\ln\mathrm{U})$ is to be made a maximum. We also make the simplifying assumption that H has a pure discrete spectrum; say tho cigenvalues $W_1, W_2, \ldots$ and the eigenfunctions $\phi_1, \phi_2, \ldots$ (there may also be multiple values among these).

Let $\mathfrak{R}$ be a quantity whose operator R has the eigenfunctions (of H) $\phi_1, \phi_2, \ldots$, but only distinct eigenvalues. The measurement of $\mathfrak{M}$ transforms U, by 2., into

$$U := \sum_{n=1}^{\infty} (U\phi_n, \phi_n)\, F_{[\phi_n]},$$

and therefore $-\mathrm{N}\kappa\,\mathrm{Tr}(\mathrm{U}\ln\mathrm{U})$ increases, unless $\mathrm{U} = \mathrm{U}'$. Also, Tr (U), Tr (UH) do not change – tho lattor because the Φ_n are eigenfunctions of $\mathbf{H}$, and therefore ($H\Phi_m, \Phi_n$) vanishes for $m \neq n$:

$$\begin{aligned}\mathrm{Tr}(U:H) &= \sum_{n=1}^{\infty} (U\phi_n, \phi_n)\,\mathrm{Tr}\left(P_{[\phi_n]}H\right)\\ &= \sum_{n=1}^{\infty} (U\phi_n, \phi_n)\,(H\phi_n, \phi_n)\\ &= \sum_{m,n=1}^{\infty} (U\phi_m, \phi_n)\,(H\phi_n, \phi_m) = \mathrm{Tr}(UH).\end{aligned}$$

This must also be true hecause of the commutativity of R, H (i.e., simultaneous measurability of $\mathfrak{R}$ and energy). Consequently, the desired maximum is the same if we limit ourselves to the U', i.e., to statistical operators with eigenfunctions $\phi_1, \phi_2, \ldots$, and, furthermore it is assumed only among these.

Therefore

$$U = \sum_{n=1}^{\infty} W_n P_{[\phi_n]},$$

and since $U, UH, U\ \mathrm{In}\ U$ all have the eigenfunctions Φ_n, but the respective eigenvalues $w_n, w_n w_n, w_n \ln w_n$, it suffices to make

$$-\mathrm{N_k} \sum_{\mathrm{n}=1}^{\infty} \mathrm{w_n} \ln \mathrm{w_n}$$

a maximum, with the auxiliary conditions

$$\sum_{n=1}^{\infty} w_n = 1, \sum_{n-1}^{\infty} w_n w_n = E.$$

But this is exactly the same problem as that which is obtained for the corresponding equilibrium problem of the ordinary gas theory, [201] and is solved in the same way. According to the well-known rules of extremum calculation, for the set of maximizing $w_1, w_2, \ldots$
$\frac{\partial}{\partial \bar{w}_n}\left(\sum_{m=1}^{m} w_m \ln w_m\right) + \alpha \frac{\partial}{\partial w_n}\left(\sum_{m=1}^{\infty} w_m\right) + \beta \frac{\partial}{\partial \bar{w}_m}\left(\sum_{m=1}^{\infty} w_m w_m\right) = 0$
must hold, in which α, β are sultahle constants, and $\mathrm{n} = 1, 2, \ldots$, that is,

$$(\ln W_n + 1) + \alpha + \beta W_n = 0, W_n = e^{-i-\alpha-\beta W_n} = a e^{-\beta W_n}$$

where the constant

$$a = e^{-1-\alpha}$$

is introduced in place of α. From

$$\sum_{n=1}^{\infty} w_n = 1$$

it follows that

$$a = \frac{1}{\sum_{n=1}^{\infty} e^{-\beta W_n}}$$

and therefore

$$w_n = \frac{e^{-\beta W_n}}{\sum_{\tilde{u}=1}^{\infty} e^{-\beta W_m}},$$

and because of $\sum_{n=1}^{\infty} W_n W_n = E$

$$\frac{\sum_{n=1}^{\infty} W_n e^{-\beta W_n}}{\sum_{n=1}^{\infty} e^{-\beta W_n}} = E$$

which determines β. If, as is customary, we introduce the "partition function,"

$$z(\beta) = \sum_{n=1}^{\infty} e^{-\beta W_n} = \operatorname{Tr}\left(e^{-\beta H}\right)$$

(cf. Notes 183, 184 for this and the following), then

$$z'(\beta) = -\sum_{n=1}^{\infty} W_n e^{-\beta W_n} = -\operatorname{Tr}\left(H e^{-\beta H}\right)$$

and therefore the condition for β

$$-\frac{Z(P)}{Z(\beta)} = \mathbf{E}$$

(We are making the assumption here that

$$\sum_{n=1}^{\infty} e^{-\beta W_n} \text{ and } \sum_{n=1}^{\infty} W_n c^{-\beta W_n}$$

converge for all $\beta > 0$, i.e., that $W_n \longrightarrow \infty$ for $n \longrightarrow \infty$, and in fact, with sufficient rapidity. For
example, $W_n / \ln n \longrightarrow \infty$ suffices.) We then obtain the following expression for U itself:

$$U = \sum_{n=1}^{\infty} a e^{-\beta W_n} P_{[\phi_{11}]} = a e^{-\beta H} = \frac{e^{-\beta H}}{T\Gamma^{(}e^{-\beta H})} = \frac{e^{-\beta H}}{z(\hat{\rho})}.$$

The properties of the equilibrium ensemble U (which is determined by the enumeration of the values of $\mathbf{E}$ or of β, and which therefore depends on a parameter, as it must) can now be determined with the method cusiomary in gas theory.

The entropy of our ensemble is

$$\begin{aligned}
\mathbf{s} &= -N_\kappa \operatorname{Tr}(U \ln U) = -N_\kappa \operatorname{Tr}\left(\frac{e^{-\beta H}}{Z(\beta)} \ln \frac{e^{-\beta H}}{Z(\beta)}\right) \\
&= -\frac{N_\kappa}{Z(\beta)} \operatorname{Tr}\left(e^{-\beta H}(-\beta H - \ln Z(\beta))\right) \\
&= \frac{\beta N_\kappa}{Z(\beta)} \operatorname{Tr}\left(H e^{-\beta H}\right) + \frac{\ln Z(\beta) N_\kappa}{Z(\beta)} \operatorname{Tr}\left(e^{-\beta H}\right) \\
&= N_\kappa \left[-\frac{\beta Z'(\beta)}{Z(\beta)} + \ln Z(\beta)\right],
\end{aligned}$$

[8201] Cf., for example, Planck, Theorie der Wrmestrahlung, Leipzig, 1913.

and the total energy

$$NE = -N\frac{z'(\beta)}{z(\beta)}$$

(this, and not **E** itself, is to be considered in conjunction with **s**) . Thus $U, \mathbf{s}, N\mathbf{E}$ are expressed by β. Instead of inverting the last relationship, i.e., expressing β by **E**, it is more practical to determine the temperature **T** of the equilibrium mixture, and to reduce everything to this. This is done as follows: Our equilibrium mixture is brought into contact with a heat reservoir of temperature $\mathbf{T}'$, and the energy Nd**E** is transferred to it from that reservoir. The two laws of thermodynamics imply, then, that the total energy must remain unchanged, and that the entropy must not decrease. Consequently, the heat reservoir loses the energy NdE , and therefore its entropy increase is $-\mathrm{Nd}\mathbf{E}/\mathbf{T}'$, and we must now have

$$\mathrm{d}\mathbf{s} - \frac{\mathrm{Nd}\mathbf{E}}{\mathbf{T}'} = \left(\frac{\mathrm{d}\mathbf{s}}{\mathrm{Nd}\mathbf{E}} - \frac{1}{\mathbf{T}'}\right)\mathrm{Nd}\mathbf{E} \geq 0$$

On the other hand, NdE $\gtreqless 0$ must hold according to whether $\mathbf{T} \gtreqless \mathbf{T}$, because the colder body absoris energy from the varmer – consequently $\mathbf{T}^{\mathbf{T}} < \mathbf{T}$ implies $\frac{\mathrm{d}\mathbf{S}}{\mathrm{N}d\boldsymbol{E}} - \frac{1}{\mathbf{T}^{\mathbf{T}}} < 0$ i.e.,

$$\mathbf{T} : \frac{\geq N d\mathbf{E}}{< d\mathbf{S}} = \frac{N\frac{d\mathbf{E}}{d\beta}}{\frac{d\mathbf{S}}{d\beta}}$$

Hence

$$\mathbf{T} = \frac{N\frac{d\mathbf{E}}{d\beta}}{\frac{d\mathbf{S}}{d\beta}} = -\frac{1}{\kappa}\frac{\left(\frac{L'(\hat{\beta})}{Z(\beta)}\right)^{\cdot}}{\left(\ln z(\beta) - \beta\frac{z'(\beta)}{Z(\beta)}\right)'} = -\frac{1}{\kappa}\frac{\left(\frac{z'(\hat{\beta})}{Z(\beta)}\right)^{\cdot}}{-\beta\left(\frac{z'(\beta)}{Z(\beta)}\right)'} = \frac{1}{\kappa\beta}$$

i.e.,

$$\beta = \frac{1}{\kappa\mathbf{T}}.$$

Therefore $U, S, N\mathbf{E}$ are now all expressed as functions of the temperature.

The analogy of the expressions obtained above for the entropy, equilibrium ensemble etc., with the corresponding results of the classical thermodynamical theory is striking. First, the entropy $-\mathrm{N}\kappa\mathrm{Tr}(\mathrm{U}\ln\mathrm{U})$.

$$U = \sum_{n=1}^{\infty} w_n P_{[\phi_n]}$$

is a mixture of the ensembles $P_{[\phi_1]}, P_{[\phi_2]}, \cdots$ with the relative weights $w_1, w_2, \ldots$, i.e., $N{w_1}^*{}_1$-systems, $\mathrm{N_W W_2}$ ψ_2-systems, $\cdots$. The Boltzmann entropy of this ensemble is obtained with the aid of the "thermodynamical probability" $\mathrm{N1}/\left(\mathrm{Nw_1}\right) : \left(\mathrm{Nw_2}\right)$!... . It is its κ fold logarithm. [201] Since N is large, we may approximate the factorial by the Stirling formula, $x_i \approx \sqrt{2\pi x}e^{-X_X X}$ and then $\kappa \ln \frac{N!}{N(N,N(N,\ldots}$ bocomes essentially

$$-N_\kappa \sum_{n=1}^{\infty} w_n \text{ in } w_n$$

– and this is exactly - $N\kappa\,\mathrm{Tr}(U\ln U)$.

Furthermore, if we had the equilibrium onsemble

$$U = e^{-\frac{H}{\kappa T}}$$

(we neglect the normalization factor $\frac{1}{z(B)}$), this is equal to

$$\sum_{\mathrm{n}=1}^{\infty} e^{-\frac{W_{\mathrm{n}}}{\kappa \mathbf{T}}} P_{[\phi_{\mathrm{n}}]}$$

therefore a mixture of the states $P_{[\phi_1]}, P_{[\phi_2]}, \ldots$, i.e., of the stationary states with the energies $W_1, W_2, \ldots$, and with the respective (relative) weights

$$e^{-\frac{W_1}{\kappa \mathbf{T}}}, e^{-\frac{W_2}{\kappa \mathbf{T}}}, \ldots$$

If an energy value is multiple, say $W_{n_1} = \cdots = W_{n_v} = W$, then $P_{\left[\phi_{\mathrm{n}_1}\right]} + \cdots + P_{[\phi_{\mathrm{n}_\nu}]}$ appears in the equilibrium ensemble with the weight

$$\frac{1}{v}\left(P_{\left[\phi_{n_1}\right]} + \cdots + P_{[\phi_{n_v}]}\right)$$

(cf. the beginning of IV.3.) appears with the weight

$$v e^{-\frac{W}{\kappa T}}$$

But the classical "canonical" ensemble is defined in exactly the same way (aside from the appearance of the specifically quantum mechanical form

$$\frac{1}{v}\left(P_{\left[\phi_{n_1}\right]} + \cdots + P_{[\phi_{n_\nu}]}\right)\Big) :$$

this is known as Boltzmann's Theorem. [201]
For T $\longrightarrow$ 0, the weights

$$e^{-\frac{W_n}{\kappa \mathbf{T}}}$$

approach 1 , therefore our U tends to

$$\sum_{n=1}^{\infty} P_{[\phi_n]} = 1$$

Consequently, $U \approx 1$ is the absolute equilibrium state, if no energy limitations apply – a result that we had already obtained in IV.3. We see that the "a priori equal probability of the quantum orbits" (i.e., of the simple, non-degenerate ones – in general the multiplicity of the eigenvalues is the "a priori" weight, cf. discussion above) follows automatically from this theory.

It remains to ascertain how much can be said nonthermodynamically about the equilibrium ensemble U of given energy – i.e., only from the fact that U is stationary (does not change in the course of time, process 2.), and that it remains unchanged in all measurements
which do not affect the energy (i.e., in measurements of quantities that are measurable simultaneously with the energy, process 1. with commutative R, H, i.e., $\dot{\phi}_1, \dot{\phi}_2, \cdots$ eigenfuncilons of i).

Because of the differential equation $\frac{\partial}{\partial t} U = \frac{2\pi i}{h}(UH - HU)$ the former means only that HU commute. The latter means that if $\phi_1, \phi_2, \ldots$ are usable, as a complete eigenfunction set of H, then $U = U'$, i.e., $^{\phi_1}, \phi_2, \cdots$ are also eigenfunctions of U. Let the corresponding H-cigenvalues be $W_1, W_2, \ldots$, those of U, $w_i, w_2, \ldots$. If $w_j = w_k$, then we can replace ϕ_j, ϕ_k by

$$\frac{\Phi_j + \Phi_k}{\sqrt{2}}, \qquad \frac{\Phi_j - \Phi_k}{\sqrt{2}}$$

for H, and therefore these are also eigenfunctions of U, from which it follows that $w_j = w_k$. Therefore, a function $F(x)$ with $F(W_n) = W_n \quad (n = 1, 2, \ldots)$ can be constructed, and $F(H) - U$. It is clear that this is sufficient, and also that it implies the commutativity of H and U.

Hence there results $U = F(H)$, but a determination of $F(x)$ (it is, as we know $F(x) = \frac{1}{Z(\beta)} e^{-\rho x}$, $\beta = \frac{1}{\kappa^{\top} \mathrm{T}}$) is not accomplished. From $\mathrm{Tr}\, U = 1$, $\mathrm{Tr}(\mathrm{UH}) = \mathbf{E}$, it follows that

$$\sum_{n=1}^{\infty} F(W_n) = 1, \sum_{n=1}^{\infty} W_n F(W_n) = E$$

but with this, all that this method can furnish us is exhausted.

28.2.4 4. The Macroscopic Measurement

Although our entropy expression, as we saw, is completely analogous to the classical entropy, it is still
surprising that it is invariant in the normal evolution in time of the system (process 2.), and only increases with measurements (process 1.) – in the classical theory (where the measurements in general played no role) it increased as a rule even with the ordinary mechanical evolution in time of the system. It is therefore necessary to clear up this apparently paradoxical situation.

The normal classical thermodynamical consideration runs as follows: One could take a container of volume V, in which M molecules of a gas (for simplicity, an ideal gas) of temperature $\mathbf{T}$ are present in the right half (volume $V/2$, separated by a partition from the other half). If we were to expand this gas isothermally and reversibly to the volume by driving back the partition with the gas pressure, utilizing the mechanical work that this performs, and by keeping the gas temperature constant by means of a large heat reservoir of temperature $\mathbf{T}$), then the entropy outside (in the reservoir) would decrease by $M_k \ln 2$ (cf. Note 195), and therefore the gas entropy could increase by the same amount. On the other hand, if we simply remove the partition, the gas diffuses into the free left half, the volume increases to γ– i.e., the entropy increases by $\mathrm{M}_{\kappa} \ln 2$ without the corresponding compensation taking place. The process is consequently irreversible, for the entropy has increased in the course of the simple mechanical evolution in time of the system (namely, in diffusion). Why does our theory give nothing similar?

This situation is best clarified if we set $M = 1$. Thermodynamics is still valid for such a onemolecule gas, and it is true that its entropy increases by $\kappa \ln 2$ if its volume is doubled. Nevertheless, this difference is κ ln 2 actually only so long as one knows no more about the molecule than that it is found in the volume $\gamma/2$ or γ, respectively. For example, if the molecule is in the volume $\boldsymbol{V}$, but it is known whether it
is in the right side or left side of the middle of the container, then it suffices to insert a partition in the middle and allow this to be pushed (isothermally and reversibly) by the molecule to the left or right end of the container. In this case, the mechanical work $\kappa T \ln$? is performed, i.e., this energy is taken from the heat reservoir. Consequently, at the end of the process, the molecule is again in the volume $\boldsymbol{\gamma}$, but we no longer know whether it is on the left or right of the middle. Hence there is a compensating entropy decrcasc of $i \ln 2$ (in the reservoir). That is, we have exchanged our knowledge for the entropy decrease $\kappa \ln 2$..[202] or, the entropy is the same in the volume γ as in the volume $\gamma/2$, provided that we know in the first mentioned case, in which half of the container the molecule is to be found. Therefore, if wo knew all the properties of the molecule before diffusion (position and momentum), we could calculate for each moment after the diffusion whether it is on the right or left side, i.e., the entropy has not decreased. If, however, the only information at our disposal was the macroscopic one that the volume was initially $\boldsymbol{V}/2$, then the entropy does increase upon diffusion.

For a classical observer, who knows all coordinates and momenta, the entropy is therefore constant, and is in fact 0 , since the Boltzmann "thermodynamical probability" is 1 (cf. the reference in Note 201); just

as in our theory for states, $U = P_{[\phi]}$, since these again correspond to the highest possible state of knowledge of the observer relative to the system.

The time variations of the entropy are then based on the fact that the observer does not know everything, that he cannot find out (measure) everything which is measurable in principle. His senses allow him to perceive only the so-called macroscopic quantities. But this clarification of the apparent contradiction mentioned at the outset imposes on us the obligation of investigating the precise analog of the classical macroscopic entropy for the quantum mechanical ensemble, i.e., the entropy as seen by an observer who cannot measure all quantities, but only a few special quantities, namely, the macroscopic ones, and even these, under certain circumstances, with only limited accuracy.

In III.3., we learned that all measurements with limited accuracy can be replaced by absolutely accurate measurements of other quantitics which are functions of these, and which have discrete spectra. If now $\mathfrak{R}$ is such a quantity, and R is its operator, if $\lambda^{(1)}, \lambda^{(2)}, \ldots$ are the distinct eigenvalues, then the measurement of $\mathfrak{R}$ is equivalent to the answering of the following questions: "Is $\mathfrak{R} = \lambda^{(1)}$?" "Is $\mathfrak{R} = \lambda^{(2)}$?",... . In fact, we can also say directly: Assume that $\mathfrak{E}$, with the operator S, is to be measured with limited accuracy – say one wishes to determine within which interval $c_{n-1} < \lambda \leq c_n$ (... $c_{-2} < c_{-1} < c_0 < c_1 < c_2 < \ldots$) it lies. This is then a case of answering all these questions "Does $\mathfrak{G}$ lie in $c_{n-1} < \lambda \leq c_n$?", $n = 0, \pm 1, \pm 2, \ldots$.

Such questions now correspond, by III.5., to projections E whose quantities $\boldsymbol{E}$ (which have only the two values 0,1) are actually to be measured. In our examples, the $\mathscr{G}$ are the functions $F_n(\mathfrak{R}), n = 1, 2, \ldots$, in which

$$F_n(\lambda) \begin{cases} = 1, \text{ for } \lambda = \lambda^{(n)} \\ = 0, \text{ otherwise} \end{cases}$$

or the functions $G_n(\mathrm{Im}), n = 0, \pm 1, \pm 2, \ldots$, in which

$$G_{\bar{n}}(\lambda) \begin{cases} -1, \text{ for } c_{n-1} < \lambda \leq c_n \\ = 0, \text{ otherwise} \end{cases}$$

– and the corresponding E are the $F_n(R)$ and $G_n(S)$ respoctivoly. Therefore, instead of giving the macroscopically measurable quantities $\mathfrak{E}$ (together with the (macroscopic) measurement precision obtainable, we may equivalently give the questions $\boldsymbol{E}$ which are answered by macroscopic measurements, or their projections E (cf. III.5.). This can be viewed as the characterization of a macroscopic observer the spocification of his E . (Thus, classically, one might characterize him by stating that he can measure the temperature and the pressure in each cm^3 of the gas volume (perhaps with certain limitations of precision], but nothing else). [203]

Now it is a fundamental fact wilh macroscopic measurements that everything which is measurable at all, is also simultaneously measurable, i.e., that all questions which can be answered separately can also be answered sinuitaneousiy, i.e., that all the E commute. The reason that the non-simultaneous measurability of quantum mechanical quantities has made such a paradoxical impression is just that this concept is so alien to the macroscopic method of observation. Because of the fundamental importance of this point, it is best to discuss it somewhat more in detail.

[8202] L. Szilard has (see refrerence in Note 194) shown Lhat one cannot get this "knowledge" without a compensating entropy increase $\kappa \ln 2$. In general, $\kappa \ln 2$ is the "thermodynamic value" of the knowledge, which consists of an alternative of two cases. All attempts to carry out the process described above without the knowledge of the half of the container in which the molecule is located, can be proved to be invalid, although they may occasionally lead tc very complicated automatic mechanisms.

Let us consider the method by which two nonsimultaneously measurable quantities [e.g., the coordinate q and the momentum p (cf. III.4.)] can be measured simultaneously with limited precision. Let the mean errors

[203] This characterization of the macroscopic observer is due to E. Wigner.

be ϵ, η respectively (according to the uncertainty principle, $\epsilon\eta \sim h$). The discussion in III.4. showed that with such precision requirements simultaneous measurement is indeed possible: the q (position) measurement is performed with light wave lengths which are not too short, the p (momentum) measurement is performed with light wave trains which are not too long. If everything is properly arranged, then the actual measurements consist in detecting two light quanta in some way, e.g., by photographing: one (in the q measurement) is the light quantum scattered by the compton effect, the other (in the p-measurement by means of the Doppler effect) is reflected, changed in frequency and then, in the determination of this frequency, is deflected by an optical dovico (prism, diffraction grating). At the end of the experiment therefore, there are two light quanta or two photographic plates, and from the directions of the light quanta, or the blackened places on the plates, we must calculate q and p. But wo must omphasize here that nothing prevents us from determining (with arbitrary precision) the two directions mentioned, or the blackened places, because these are obviously simultaneously measurable quantities (they are momenta or coordinates of two different objects). However, excessive precision at this point is not of much help for the measurement of q and p. As was shown in III.4., the connection of these quantities with q and p is such that the uncertainties ϵ, η remain for q and p (even if the above quantities are measured with greater precision), and the apparatus cannot be arranged so that $\epsilon\eta \ll$ h

Therefore, if we introduce the two directions mentioned, or the blackened places themselves as physical quantities (with operators Q', P'), then we see that Q', P' are commutative, but the operators Q, P belonging to q, p can be expressed by means of them with no higher precision than ϵ, η respectively. Let the quantities belonging to Q', P' be q', p'. The interpretation that the actually macroscopically measurable quantities are not the q, p themselves but the q', p' is a very plausible one (indeed the q', p' are in fact measured), and it is in accord with our postulate of the simultaneous measurability of all macroscopic quantities.

It is reasonable to attribute to this result a general significance, and to view it as disclosing a characteristic of the macroscopic method of observation. According to this, the macroscopic procedure consists of the replacing of all posaihle operators A,B,C... . which as a rule do not commute with each other, by other operators $A', B', C', \ldots$ (of which these are functions to within a certain approximation) which do commute with each other. Since we can just as well denute these functions of $A', B', C', \ldots$ themselves by $A', B', C', \ldots$, we may also say this: $A', B', C', \ldots$ are approximations of the $A, B, C, \ldots$, but commute exactly with one another. If the respective numbers $\epsilon_A, \epsilon_B, \epsilon_C, \cdots$ give a measure for the magnitudes of the operators $A' - A, B' - B, C' - C, \ldots$, then we see inal ${}^tA^tB$ will be of the order of magnitude of $AB - BA$ (that is, $\neq 0$, generally), etc. – this gives the limit of the approximations which can be achieved. It is, of course, advisable, in enumerating the $A, B, C, \ldots$ to restrict oneself to those operators whose physical quantities are inaccessible to macroscopic observation, at least within a reasonable approximation.

These wholly qualitative developments remain an empty program so long as we cannot show that they require only things which are mathematically practicable. Therefore, for the characteristic case Q, P, we shall discuss further the question of the existence of the above Q', P' on a mathematical basis. For this purpose, let ϵ, η be two positive numbers with $\epsilon\eta = \frac{h}{4\pi}$. We seek two commuting Q', P' such that $Q' - Q, P' - P$ (in a sense still to be defined more precisely), have the orders of magnitude ϵ, η respectively.

We do this with quantities q', p' which are measurable with perfect precision, i.e., Q', P' have pure discrete specira; since they commute, there is a complete orthonormal set consisting

of the eigenfunctions common to both, $\phi_1, \phi_2, \ldots$ (cf. II.10.). Let the corresponding eigenvalues of Q', P' be $a_1, a_2, \cdots$ and $b_1, b_2, \ldots$ respectively. Then

$$Q' = \sum_{n-1}^{\infty} a_n P_{[\phi_n]}, P' = \sum_{n=1}^{\infty} b_n P_{[\phi_n]}.$$

Arrange their measurement in such a manner, that it creates one of the states $\phi_1, \phi_2, \cdots$– measure a quantity *in* whose operator R has the eigenfunctions $a_1, a_2, \cdots$ and distinct eigenvalues $c_1, c_2, \ldots$, and then Q', P' are functions of R. That this measurement implies a measurement of Q and P in approximate fashion is clearly implied by this: In the state ϕ_n the values of Q, P are expressed approximately by the respective values of Q', P', i.e., λ_n=h_n. That is, their dispersions about these values are small. These dispersions are the expectation values of the quantities $(q - a_n)^2$, $(p - b_n)^2$, i.e.,
$\left((Q - a_n 1)^2 \phi_n, \phi_n\right) = ||(Q - a_n{}^1)\,\phi_n||^2 = ||Q\phi_n - a_n\phi_n||^2$,
$\left((P - b_n{}^1)^2 \phi_n, \phi_n\right) = \|(P - b_n{}^1)\,\phi_n\|^2 = \|P\phi_n - b_n\phi_n\|^2$.
They are the measures for the squares of the differences of Q' and Q, P' and P respectively, i.e., they must be approximately ϵ^2 and η^2 respectively. We therefore require

$$\left\|Q_n^{\phi} - a_n^{\phi}\phi_n\right\| \leq \epsilon, \|P\phi_n - b_n\phi_n\| \leq \eta.$$

Instead of speaking of Q', P', it is then more appropriate only to seek a complete orthonormal set $\phi_1, \phi_2, \cdots$
for which, for suitable choice of $a_1, a_2, \ldots$ and $b_1, b_2, \ldots$, the above estimates hold.

Individual (with $||\phi|| = 1$), for which (for suitable a, b)

$$||Q_\phi - a_\phi|| = \epsilon, \|P_\phi - b_\phi\| = \eta$$

are known from III.4.:

$$\phi_{\rho,\sigma,\gamma} = \phi_{\rho,\sigma,\gamma}(q) = \left(\frac{2\gamma}{h}\right)^{\frac{1}{4}} e^{-\frac{\pi\gamma}{h}(q-\sigma)^2 + \frac{2\pi\rho}{h}iq}.$$

Hence, because of $\epsilon\eta = \frac{h}{4\pi}$ we have again

$$\epsilon = \sqrt{\frac{h\gamma}{4\pi}}, \eta = \sqrt{\frac{h}{4\pi\gamma}}$$

(i.e., $\gamma = \epsilon/\eta$), and we choose $a = \sigma, b = \rho$. We now must construct a complete orthonormal set with the help of these $\phi_{\rho,\sigma,\gamma}$. Since σ is the Q - and ρ the P-expectation value, it is plausible that ρ, σ should each run through a set of numbers independently of each other, and in fact, in such a way that the ρ-set has approximately the density ϵ and the σ-set approximately the density η. It proves practical to choose the units

$$2\sqrt{\pi \cdot \epsilon} = \sqrt{h\gamma} \text{ and } 2\sqrt{\pi \cdot \eta} = \sqrt{\frac{h}{\gamma}},$$

i.e.,

$$\rho = \sqrt{\mathrm{h}\gamma}\mu, \sigma = \sqrt{\frac{\hbar}{\gamma}}v$$

($\mu, v = 0, \pm 1, \pm 2, \ldots$). The

$$\Psi_{\mu,\nu} = \Phi\left(\sqrt{\mathrm{h}\gamma}\mu, \sqrt{\frac{\hbar}{\gamma}}v, \gamma\right)$$

($\mu, v = 0, \pm 1, \pm 2, \ldots$) ought then to correspond to the Φ_n $(n = 1, 2, \ldots)$. It is obviously irrelevant that we have two indices μ, v in place of the one n.

However, these $\psi_{\mu,\nu}$ are not yet orthogonal. (They are nortualized, howevel, and liney satisfy

$$\left(\left\|Q\psi_{\mu,\nu} - \sqrt{h\gamma}\mu\psi_{\mu,\nu}\right\| = \epsilon, \left\|P\psi_{\mu,\nu} - \sqrt{\frac{h}{\gamma}}\nu\psi_{\mu,\nu}\right\| = \eta.\right)$$

If we now orthogonalize them by the E. Schmidt process (in order, cf. II.2., proof of THEOREM 8.), then we can prove the completeness of the resulting normalized orthogonal set $\psi'_{\mu,v}$ without any particular difficulties, and can also establish the estimates

$$\left\|Q\psi'_{\mu,v} - \sqrt{h\gamma}\mu\psi'_{\mu,v}\right\| \leq c\epsilon, \left\|P\psi'_{\mu,v} - \sqrt{\frac{h}{\gamma}}v\psi'_{\mu,v}\right\| \leq c\eta$$

with certain fixed C. A value $C \sim 60$ has been obtained in this way, and it could probably be reduced. The proof of this fact leads to rather tedious calculations, which require no new concepts, and we shall omit them. The factors $C \sim 60$ are not important, since $E\eta = h/4\pi$ measured in macroscopic (CGS) units is exceedingly small (c. 10^{-28}).

Summing up, we can then say that it is justified to assume the commutativity of all macroscopic operators, and in particular the commutativity of the macroscopic projections E introduced above.

The E correspond to all macroscopically answerable questions (, i.e., to all discriminations of alternatives in the system investigated, that can be carried out macroscopically. They are all commutative. We can conclude from II.5., that $1 - \mathrm{E}$ belongs to them along with E, and that $EF, E + F - EF, E - EF$ belong along with E, F. It is reasonable to assume that there are only a finite number of them: $E_1, \ldots, E_n$. We introduce the notation $\mathrm{E}^{(+)} = \mathrm{E}, \mathrm{E}^{(-)} = 1 - \mathrm{E}$ and consider all 2^n products $E_1{}^{(s_1)} \ldots E_n{}^{(s_n)}$ $(s_1, \ldots, s_n = \pm)$. Any two different ones among these have the product zero: For if $E_1{}^{(s_1)} \ldots E_n^{(s_n)}$ and $E_1^{(t_1)} \ldots F_n^{(t_n)}$ are two such, and $s_v \neq t_v$, then there appear in their product the (s) (t $_v$) factors $\mathrm{E}_v{}^{(\mathrm{S}_v)}, \mathrm{E}_v{}^{(\mathrm{t}_v)}$ i.e., $\mathrm{E}_v{}^{(+)} = \mathrm{E}$ and $\mathrm{E}_v{}^{(-)} = 1$ - E, whose product is zero. Each E_v is the sum of several such products: Indeed,

$$\mathrm{E}_v - \sum \mathrm{E}_1^{(\mathrm{s}_1)} \ldots \mathrm{E}_{v-1}^{(\mathrm{s}_{v-1})} \cdot \mathrm{E}_v^{(+)^{(\mathrm{s}_{v+1})}} \mathrm{E}_{v+1}^{(\mathrm{s}_\mathrm{n})} \ldots \mathrm{E}_\mathrm{n}.$$

$s_1, \ldots, s_{v-1}, s_{v+1}, \ldots, s_n = \pm$

Among these products consider the ones which are different from zero. Call them $E_1, \ldots, E'_m$. (Evidently $m \leq 2^n$, but actually even $m \leq n - 1$, since these must occur among the $\mathrm{E}_1, \ldots, \mathrm{E}_\mathrm{n}$ and be $\neq 0$). Now clearly: $\mathrm{E}'_\mu \neq 0$; $E'_\mu E'_\nu = 0$ for $\mu \neq \nu$; each E_μ is the sum of several E'_ν : (From the latter it also follows that $n = 2^m$.) It should be noted that $\mathrm{E}_\mu + \mathrm{E}_\nu = \mathrm{E}'_{\tilde{\rho}}$ can never occur, unless $E_\mu = 0, E_\nu = E'_\rho$ or $E_\mu = E'_\rho, E_\nu = 0$. Otherwise, E_μ, E_ν would be sums of several E'_π, and therefore E'_ρ the sum ot ≥ 2 terms E'_π (possibly with repeilitions). By II.4., THEOREMS 15, 16., these would all differ from one another, since their number is ≥ 2 and all are $\neq 0$, they also differ from E'_ρ– therefore their product with E'_ρ would be zero. Hence the product of their sum with E'_ρ would also be zero, but this contradicts the assertion that the sum is - E'_ρ.

The properties $\mathbb{E}_1, \ldots, \mathbb{E}_\mathrm{m}$ corresponding to the $\mathrm{E}_1, \ldots, \mathrm{E}'_\mathrm{m}$ are then macroscopic properties of the following type: None is absurd. Every two are mutually exclusive. Each macroscopic

property obtains by disjunction of several of them. None of them can be resolved by disjunction into two sharper macroscopic properties. $\mathfrak{E}_1, \ldots, \mathfrak{E}'_{\mathrm{m}}$ therefore represent the furthest that we can go in macroscopic discrimination, for they are macroscopically indecomposable.

In the following, we shall not require that their number be finite, but only that there exist macroscopically indecomposable properties $\mathfrak{E}_1, \mathfrak{E}_2, \ldots$. Let their projections be $\mathrm{E}_1, \mathrm{E}_2, \ldots$, all again different from zero, mutually orthogonal, and each macroscopic E the sum of several of them.

Therefore 1 is also a sum of several of them. If an E'_v did not occur in this sum, it would be orthogonal to each term and hence to the sum, that is to $1: \; E'_v = E'_v \cdot 1 = 0$, which is impossible. Therefore $E_1 + \mathrm{E}'_2 + \ldots = 1$. We drop the prime notation: $\mathbb{G}_1, \mathbb{E}_2, \ldots$ and $E_1, E_2, \ldots$. The closed linear manifolds belonging to these will be called $\mathfrak{R}_1, \mathfrak{R}_2, \ldots$, and their dimension numbers $s_1, s_2, \ldots$.

If all the $s_n = 1$, i.e., all m_n one dimonsiona. 1 , then $\mathfrak{M}_{\mathrm{n}} = [_n], \mathrm{F_n} = \mathrm{P}_{[\phi_{\mathrm{n}}]}$ and because $\mathrm{E_i} + \mathrm{E}_2 + \cdots = 1$, the $\phi_1, \phi_2, \cdots$ would form a complete orthonormal set. This would mean that macroscopic measurements would themselves make a complete determination of the state of the observed system possible. Since this is ordinarily not the case, we have in general $s_n > 1$, and in fact, $s_n \gg 1$.

In addition, it should be observed that the $\mathrm{E_n}$, which are the elementary building blocks of the macroscopic description of the world, correspond in a certain sense to the ordinary cell division of phase space in the classical theory. We have already seen that they can reproduce the behavior of non-commutative operators in an approximate fashion, in particular, that of Q, P, which are so important for phase space.

Now, what entropy does the mixture U have for a macroscopic observer whose indecomposable projections are $E_1, E_2, \ldots$? Or, more precisely, how much entropy can such an observer maximally obtain by transforming U into V – i.e., what entropy decrease (under suitable conditions, naturally this decrease may be $\gtrless 0$) can he produce, under
the most favorable circumstances, in external objects as compensation for the transition U $\longrightarrow$ V ?

First, it must be emphasized that he cannot distinguish between each two ensembles U, U', if both give the same expectation value to $\mathrm{E_n}$ for each $\mathrm{n} = 1, 2, \ldots$, that is, if $\mathrm{Tr\,(UE_n)} = \mathrm{Tr\,(U'E_n)} \quad (\mathrm{n} = 1, 2, \ldots)$. After some time, of course, the discrimination may become possible, since U, U ' change according to 2., and

$$\mathrm{irr}\left(\hat{A}\bar{U}\hat{A}^{-1}\bar{E}_n\right) = \mathrm{irr}\left(\hat{A}\bar{U}\cdot\hat{A}^{-1}\bar{E}_n\right), A = e^{-\frac{2\pi i}{h}tH}$$

must no longer hold. 204 But we considered only measurements which are carried out immediately. Under the above conditions we may therefore regard U, U' as indistinguishable. Furthermore, the observer can also use only such semi-permeable walls which transmit the ϕ of some F_n and reflect the remainder unchanged. This possibility suffices, as can be seen without difficulty. By means of the method of V.2., to transform a

$$U = \sum_{n=1}^{\infty} x_n E_n$$

[204] If E_n commutes with H, and therefore with A, the equality still holds because

$$\mathrm{Tr}\left(A \cdot UA^{-1}E_n\right) = \mathrm{Tr}\left(UA^{-1}E_n \cdot A\right) = \mathrm{Tr}\left(UA^{-1}AE_n\right) = \mathrm{Tr}\left(UE_n\right).$$

But all $\mathrm{E_n}$, i.e., all macroscopically observable quantities, are in no way all commutative with H. Indeed, many such quantities, for example, the center of gravity of a gas in diffusion, change appreciably with t, i.e., Tr ($\mathrm{UE_n}$) is not constant. Since all macroscopic quantities do

commute, H is never a macroscopic quantity, i.e., the
into a

$$V' = \sum_{n=1}^{\infty} y_n E_n$$

reversibly, so that the ontropy difference is still $\kappa \operatorname{Tr}(U' \ln U') - \kappa \operatorname{Tr}(V' \ln V')$, i.e., the entropy of U' equals $-\kappa \operatorname{Tr}(U' \ln U')$. To be sure, in order that such U' with $\operatorname{Tr} U' = 1$ exist in general, the $\operatorname{Tr} E_n$, i.e., the numbers s_n, must be finite. We therefore assume that all s_n are finite. U has the s_1-fold eigenvalue x_1, the s_2-fold eigenvalue $x_2, \ldots$. Therefore $-U' \ln U'$ has the s_1-fold eigenvalue $-x_1 \ln x_1$, the s_2-fold eigenvalue $-x_2 \ln x_2, \ldots$. Consequently $\mathrm{TrU}' = 1$ implies

$$\sum_{n=1}^{\infty} s_n x_n = 1$$

and the entropy is equal to

$$-\kappa \sum_{n=1}^{\infty} s_n x_n \ln x_n \quad .$$

Because of

$$UE_m = \sum_{n=1}^{\infty} X_n E_n E_m = X_m E_m, \operatorname{Tr}(UE_m) = X_m \operatorname{Tr} E_m = s_m x_m,$$

$X_m = \frac{\operatorname{Tr}(U^1 E_m)}{S_m}$, therefore the entropy is equal to

$$-\kappa \sum_{n=1}^{\infty} \operatorname{Tr}(U \cdot E_n) \ln \frac{\operatorname{Tr}(U \cdot E_n)}{S_n}.$$

For arbitrary $U(\operatorname{Tr} U = 1)$, the entropy must
sion. This is plausible without additional comment.
also be equal to

$$-\kappa \sum_{n=1}^{\infty} \operatorname{Tr}(UE_n) \ln \frac{\operatorname{Tr}(TE_{n1})}{S_n}$$

because, if we set

$$x_n = \frac{\operatorname{Tr}(UE_n)}{S_n}, U' = \sum_{n=1}^{\infty} x_n \bar{E}_n$$

then $\operatorname{Tr}(UE_n) = \operatorname{Tr}\left(\bar{U} \cdot E_n\right)$, and since U, U, are indistinguishable, they have the same entropy.

We must also mention the fact that this entropy always exceeds the customary entropy:

$$-\kappa \sum_{n=1}^{\infty} \operatorname{Tr}(UE_n) \ln \frac{\operatorname{Tr}(UE_n)}{S_n} \geq -\kappa \operatorname{Tr}(U \ln U)$$

and that the equality holds only for

$$U = \sum_{n=1}^{\infty} x_n E_n.$$

[8] energy is not measured macroscopically with complete preci-

By the results of V.3., this is certainly line case if

$$U' = \sum_{n=1}^{\infty} \frac{\operatorname{Tr}(UE_n)}{S_n} E_n$$

can be obtained from U by several (not necessarily macroscopic) applications of the process 1. – because on the left we have $-\kappa \operatorname{Tr}(U' \ln U')$, and

$$U = \sum_{n=1}^{\infty} x_n E_n$$

means the same as $U = U'$. We take an orthonormal set ${}_{\phi}{}^{(n)}, \ldots, \phi_s(n)$ which spans the closed linear manifold $\mathfrak{R}_n$ belonging to E_n. Because of

$$\sum_{n=1}^{\infty} E_n = 1,$$

all $\phi_v{}^{(n)}$ $(n = 1, 2, \ldots; v = 1, \ldots, s_n)$ form complete orthonormal sot. Let R be an operator belonging to these eigenfunctions (with only distinct eigenvalues) and $\mathfrak{R}$ its physical quantity. In the measurement of $\mathfrak{R}$, we get from U (by 1.)

$$U'' = \sum_{n=1}^{\infty} \sum_{v=1}^{S_n} \left(U\Phi_v{}^{(n)}, \phi_v{}^{(n)} \right) \cdot P_{[\phi_v}(n) \Big]$$

Then, if we set

$$\psi_\mu(\mathrm{n}) = \frac{1}{\sqrt{\mathrm{S_n}}} \sum_{v=1}^{\mathrm{S_n}} \mathrm{e}^{\frac{2\pi \mathrm{i}}{\mathrm{S_n}} \mu v} \phi_v(\mathrm{n}) \quad (\mu = 1, \ldots, \ \mathrm{s_n})$$

the $\psi_1{}^{(n)}, \ldots, \psi_{s_n}(n)$ form an orthonormal set which span
the same closed linear manifold as the $\psi_1{}^{(n)}, \ldots, \psi_{s_n}(n)$ the same closed linear manifold as the $\dot{\Psi}_1{}^{(n)}, \ldots, {}_{s_n}{}^{(n)} : m_n$. Therefore the $\psi_v(n) \quad (n = 1, 2, \ldots; v = 1, 2, \ldots, s_n)$ also form a courplete orthonormal sot, and we form an operator S with these eigenfunctions, and the corresponding physical quantity $\mathfrak{S}$. We must note the validity of the following formulas:

$$\left(P_{[\phi_v(n)]^{\psi_\mu(m)}, \psi_\mu{}^{(m)}} \right) \left\{ \begin{array}{ll} = 0 & \text{for } m \neq n \\ = \frac{1}{s_n} & \text{for } m = n \end{array} \right\},$$

$$\sum_{v=1}^{s_n} P_{[\phi_v(n)]} = \sum_{v=1}^{s_n} P_{[\psi_v(n)]} = E_n.$$

In the measurement of ε, therefore, U'' becomes (by 1.)
$\sum_{m=1}^{\infty} \sum_{\mu=1}^{s_m} \left(U'' \psi_\mu^{(m)}, \psi_\mu^{(m)} \right) P_{\left[\psi_\mu^{(m)}\right]}$
$= \sum_{m=1}^{\infty} \sum_{\mu=1}^{s_m} \left[\sum_{n=1}^{\infty} \sum_{v=1}^{s_n} \left(U_v^{(n)}, \phi_v^{(n)} \right) \left(P_{\left[\phi_v^{(n)}\right]} \psi_\mu^{(m)}, \psi_\mu^{(m)} \right) \right] P_{\left[\psi_\mu^{(m)}\right]}$
$= \sum_{m=1}^{\infty} \sum_{\mu=1}^{s_m} \left[\sum_{v=1}^{s_m} \frac{\left(U_v^{(m)}, \Phi_v^{(m)} \right)}{s_m} \right] P_{\left[\psi_\mu^{(m)}\right]} = \sum_{m=1}^{\infty} \sum_{v=1}^{s_m} \frac{\operatorname{Tr}(UE_m)}{s_m} P_{\left[\psi_\mu^{(m)}\right]}$
$= \sum_{m=1}^{\infty} \frac{Tr'(UE_m)}{m} F_m = U\cdot.$
Consequently, two processes 1. suffice to transform U
into U'– and this is all we needed for the proof.
This entropy for states $\left(U = P_{[\phi]}, \operatorname{Tr}(UE_m) = (E_n\phi, \phi) = ||E_n\phi||^2 \right)$,

$$-\kappa \sum_{n=1}^{\infty} ||E_n \Phi||^2 \ln \frac{||E_n \Phi||^2}{s_n}$$

is no longer subject to the inconveniences of the "macroscopic" entropy: In general, it is not constant in time (1.e., in process 2.), and not $= 0$ for all states $U = P_{[\phi]}$. In fact: that the $\mathrm{Tr}\,(U_{E_n})$, from which our entropy is formed, are not time constant in general, was discussed in Note 204. It is easy to determine when the state $U = P_{[\phi]}$ has the entropy 0 : Since

$$\frac{\|E_n \Phi\|^2}{S_n} \geq 0, \leq 1$$

all summands

$$\|E_n \phi\|^2 \ln \frac{\|E_n \Phi\|^2}{S_n}$$

in the entropy expression are ≤ 0. All these must therefore be $= 0$. That is,

$$\frac{||E_n \phi||^2}{S_n} = 0, 1$$

The former means that $\mathrm{E_n}^{\phi} = 0$, the latter that $\|E_n \Phi\| = \sqrt{s_n}$, but since

$$\|E_n \Phi\| \leq 1, s_n \geq 1$$

this implies $s_n = 1, ||E_n \phi|| = ||\phi||$: i.e., $E_n \phi = \phi$; or: $s_n = 1, \phi$ in $\mathfrak{M}_n$. The latter can certainly not hold for two different n, but also, it cannot hold at all because then $E_n \Phi = 0$ would always be true, and therefore $\phi = 0$ since

$$\sum_{n=1}^{\infty} E_n = 1.$$

Hence, for exactly one n, ϕ is in $\mathfrak{M}_\mathrm{n}$, and then $s_n = 1$. Since we determined that in general all $s_n \gg 1$, this is impossible. That is, our entropy is always > 0. Since the macroscopic entropy is time variable, the next question to be answered is this: does it behave like the entropy of the phenomenological thermodynamics in the real world, i.e., does it increase predominantly? This question is answered affirmatively in classical mechanical theory by the so-called Boltzmann H-theorem. In that, however, certain statistical assumptions, the so-called "disorder assumptions" must be made. [205] In quantum

mechanics, it was possible for the author to prove the corresponding theorem without such assumptions. [206] Since the detailed discussion of this subject, as well as of the ergodic theorem closcly connected with it (cif. the feference in Note 206, where this theorem is also proved) would go beyond the scope of this volume, we cannot report on these investigations. The reader who is interested in this problem can refer to the treatments in the references.

[206] Z. Physik, 57 (1929).

[8] [205] For the classical H-theorem, see Boltzmann, Vorlesungen ber Gastheorie, Leipzig, 1896, as well as the extremely instructive discussion by $P.$ and $T.$ Ehrenfest in the article cited in Note 185. The "disorder assumptions" which can take the place (in quantum mechanics) of those of Boltzmann

[8]have been formulated by $W.$ Pauli (Sommerfeld-Festschrift, 1928), and the H-theorem is proved there with their help. More recently, the author also succeeded in proving the classical-mechanical ergodic theorem, cf. Proc. Nat. Ac., Jan. and March, 1932, as well as the improved treatment of G. D. Birkhoff, Proc. Nat. Ac., Dec. 1931 and March, 1932.

28.3 V.2 The Measuring Process by Von Neumann

28.3.1 1. Formulation of the Problem

In the discussions so far, we have treated the relation of quantum mechanics to the various causal and statistical methods of describing nature. In the course of this we found a peculiar dual nature of the quantum mechanical procedure which could not be satisfactorily explained. Namely, we found linat on the one hand, a state $\dot{\phi}$ is transformed into the state ϕ' under the action of an energy operator H in the time interval $0 \leq t \leq t$:

$$\frac{\partial}{\partial t}\phi_\tau = -\frac{2\pi i}{h} H\phi_\tau \quad (0 \leq \tau \leq t),$$

so if we write $\phi_o = \phi, \phi_t = \phi'$, then

$$\phi' = e^{-\frac{2\pi i}{h}tH}{}_\phi$$

which is purely causal. A mixture U is correspondingly transformed into

$$U' = e^{-\frac{2\pi i}{h}tH} U e^{\frac{2\pi i}{h}tH}.$$

Therefore, as a consequence of the causal change of ϕ
into ϕ', the states $U = P_{[\phi]}$ go over into the states $U' = P_{[\phi']}$ (process 2. in V.1.). On the other hand, the state ϕ– which may measure a quantity with a pure discrete spectrum, distinct eigenvalues and eigenfunctions $\phi_1, \phi_2, \ldots$– undergoes in a measurement a non-causal change in which each of the states $\phi_1, \phi_2, \cdots$ can result, and in fact does result with the respective probabilities $|(\phi, \phi_1)|^2, |(\phi, \phi_2)|^2, \ldots$. That is, the mixture

$$U^T = \sum_{n=1}^{\infty} |(\phi, \phi_n)|^2 P_{[\phi_n]}$$

obtains. More generally, the mixture U goes over into

$$U' = \sum_{n=1}^{\infty} (U\phi_n, \quad \phi_n) P_{[\phi_n]}$$

(process 1. in V.1.). Since the states go over into mixtures, the process is not causal.

The difference between these two processes $U \longrightarrow U'$ is a very fundamental one: aside from the different behaviors in regard to the principle of causality, they are also different in that the former is (thermodynamically) reversible, while the latter is not (cf. V.3.).

Let us now compare these circumstances with those which actually exist in nature or in its observation. First, it is inherently entirely correct that the measurement or the related process of the subjective perception is a new entity relative to the physical environment and is not reducible to the latter. Indeed, subjective perception leads us into the intellectual inner life of the individual, which is extra-observational by its very nature (since it must be taken for granted by any conceivable observation or experiment). (Cf. the discussion above.) Nevertheiess, it is a fundamental requirement of the scientific viewpoint – the so-called principle of the
psycho-physical parallelism – that it must be possible so to describe the extra-physical process of the subjective perception as if it were in reality in the physical world – i.e., lo assign lo its paris equivalent physical processes in the objective environment, in ordinary space. (Of course, in this correlating procedure there arises the frequent necessity of localizing some of these processes at points which lie within the portion of space occupied by our own bodies. But this does not alter the fact of their belonging to the "world about us," the objective environment referred to above.) In a simple example, these concepts might be applied about as follows: We

wish to measure a temperature. If we want, we can pursue this process numerically until we have the temperature of the environment of the mercury container of the thermometer, and then say: this temperature is measured by the thermometer. But we can carry the calculation further, and from the properties of the mercury, which can be explained in kinetic and molecular terms, we can calculate its heating, expansion, and the resultant length of the mercury column, and then say: this length is seen by the observer. Going still further, and taking the light source into consideration, we could find out the reflection of the light quanta on the opaque mercury column, and the path of the remaining light quanta into the eye of the observer, their refraction in the eye lens, and the formation of an image on the retina, and then we would say: this image is registered by the retina of the observer. And were our physiological knowledge more precise than it is today, we could go still further, tracing the chemical reactions which produce the impression of this image on the retina, in the optic nerve tract and in the brain, and then in the end say: these chemical changes of his brain cells are perceived by the observer. But in any case, no matter how far we calculate – to the mercury vessel, to the scale of the thermometer, to the retina, or into the brain, at some
time we must say: and this is perceived by the observer. That is, we must always divide the world into two parts, the one being the observed system, the other the observer. In the former, we can follow up all physical processes (in primide at least) arbitrarily precisely. In the latter, this is meaningless. The boundary between the two is arbitrary to a very large extent. In particular we saw in the four different possibilities in the example above, that the observer in this sense needs not to become identified with the body of the actual observer: In one instance in the above example, we included even the thermometer in it, while in another instance, even the eyes and optic nerve tract were not included. That this boundary can be pushed arbitrarily deeply into the interior of the body of the actual observer is the content of the principle of the psycho-physical parallelism – but this does not change the fact that in each method of description the boundary must be put somewhere, if the method is not to proceed vacuously, i.e., if a comparison with experiment is to be possible. Indeed experience only makes statements of this type: an observer has made a certain (subjective) observation; and never any like this: a physical quantity has a certain value.

Now quantum mechanics describes the events which occur in the observed portions of the world, so long as they do not interact with the observing portion, with the aid of the process 2. (V.1.), but as soon as such an interaction occurs, i.e., a measurement, it requires the application of process 1 . The dual form is therefore justified. [207] However, the danger lies in the fact that

the principle of the psycho-physical parallelism is violated, so long as it is not shown that the boundary between the observed system and the observer can be displaced arbitrarily in the sense given above.

In order to discuss this, let us divide the world into three parts: I, II, III. Let I be the system actually observed, II the measuring instrument, and III the actual observer. [208] It is to be shown that the boundary can just as well be drawn between I and II + III as between I + II and III . (In our example above, in the comparison of the first and second cases, I was the system to be observed, II the thermometer, and III the light plus the observer; in the comparison of the second and third cases, I was the system to be observed plus the thermometer, II the light plus the eye of the observer, III the observer, from the retina on; in the comparison of the third and fourth cases, I was everything up to the retina of the observer, II his retina, nerve tracts and brain, III his abstract "ego.") l'hat is, in one case 2. is to be applied to I, and 1 . to the interaction between I and II + III ; and in the other case, 2. to I + II , and 1. to the interaction between I + II and III. (In each case, III itself remains outside of the calculation.) The proof

[8207] N. Bohr, Naturwiss. 17 (1929), was the first to point out that the dual description which is necessitated by the formalism of the quantum mechanical description of nature is fully justified by the physical nature of things that it may be connected with the principle of the psycho-physical parallelism.

of this assertion, that both procedures give the same results regarding I (this and only this belongs to the observed part of the world in both cases), is then our problem.

But in order to be able to accomplish this successfully, we must first investigate more closely the process of forming the union of two physical systems (which leads from I and II to I + II).

28.3.2 2. Composite Systems

As was stated at the end of the preceding section, we consider two physical systems I, II (which do not necessarily have the meaning of the I, II above), and their combination $I+II$. In the classical mechanical method of description, I would have k degrees of freedom, and therefore the coordinates $q_1, \ldots, q_k$, in place of which we shall use the one symbol q; correspondingly, let II have 1 degrees of freedom, and the coordinates $r_1, \ldots, r_7$ which shall be denoted by r. Therefore, I + II has $k + l$ degrees of freedom and the coordinates $q_1, \ldots, q_k, r_1, \ldots, r_1$, or, more briefly, q, r. In quantum mechanics then, the wave functions of I have the form $\phi(q)$, those of II the form $\xi(r)$ and those of $I + TT$ the form $\Phi(a, r)$. In the corresponding Hilbert spaces $\mathfrak{R}^I, \mathfrak{R}^{II}, \mathfrak{R}^{I+II}$, the inner product is defined by $\int \phi(q)\bar{\Psi}(q)dq, \int \xi(r)\overline{\eta(r)}dr$ and $\iint \Phi(q, r)\Psi(q, r)dqdr$ respectively. The physical quantities of I, II, I + II are corrospondingly the (hypermaximal) Hermitian operators A, A, and A in $\mathfrak{R}^I, \mathfrak{R}^{II}$, and $\mathfrak{R}^{\mathrm{I+II}}$ respectively.

Each physical quantity in I is naturally also one in I + II, and in fact its A is to be obtained from its A in this way: to obtain $A\Phi(q, r)$ consider r as a constant and apply A to the q function $\Phi(q, r)$.[209] This rule of transformation is correct in any case for the coordinate and momentum operators $\mathrm{Q}_1, \ldots, \mathrm{Q}_\mathrm{k}$ and $P_1, \ldots, P_k$, i.e.,

$$q_1, \ldots, q_k, \frac{h}{2\pi i}\frac{\partial}{\partial q_1}, \ldots, \frac{h}{2\pi i}\frac{\partial}{\partial q_k}$$

(cf. I.2.), and it conforms with the principles I., II. in

[209] It can easily be shown that if A is Hermitian or hypermaximal, A is also.

IV.2. [210] We therefore postulate them generally. (This is the customary procedure in quantum mechanics.)

In the same way, each physical quanility in II is also one in I + II, and its A gives its A by the same mule: $A\Phi(q, r)$ equals $A\Phi(q, r)$ if in the latter expression, q is taken as constant, and $\Phi(q, r)$ is considered as a function of r.

If $\Phi_m(q)(m = 1, 2, \ldots)$ is a complete orthunormal set in $\mathfrak{R}^I$ and $\xi_n(r) \quad (n = 1, 2, \ldots)$ one in $\mathfrak{R}$ II, then $\Phi_{m|n}(q, r) = \Phi_m(q)\xi_n(r) \quad (m, n = 1, 2, \ldots)$ is clearly one in m^{I+II}. The operators A, A, A can therefore be represented by matrices $\left\{a_{m|m}, \right\}, \left\{a_{n|n}, \right\}$, and $(\alpha_{mnm'n'})$ respectively ($m, n', n, n' = 1, 2, \ldots$). [211] We shall make frequent use of this. The matrix representation means that

$$A\Phi_m(q) = \sum_{m'=1}^{\infty} a_{m|m'}\phi_{m'}(q), A\xi_n(r) = \sum_{n'=1}^{\infty} a_{n|n'}\xi_{n'}(r)$$

and

$$A\Phi_{mn}(q; r) = \sum_{m',n'=1}^{\infty} \alpha_{m|m:_m:\Phi_{iI}:_n:}(q, r),$$

i.e.,

[210] For 1. this is clear, and for II. also, so long as only polynomials are concerned. For general

[8208] The discussion which is carried out in the following, as well as that in VI.3., contains essential elements which the author owes to conversations with L. Szilard. Cf. also the similar considerations of Heisenberg, in the reference cited in Note 181.

functions, it can be inferred from the fact that the correspondence of a resolution of the identity and a Hermitian operator is not disturbed in our transition $A \longrightarrow A$.

[211] Because of the large number and variety of indices, we use this method of denoting the matrices, which differs somewhat from the notation used thus far.

$$A\hat{q}_m(q)\xi_n(r) = \sum_{m'n'=1}^{\infty} \tilde{q}_{mn|m'n'\hat{p}_m(q)s_n(r)}$$

In particular the correspondence $A \longrightarrow A$ means that

$$A\Phi_m(q)\xi_n(r) = (A\Phi_m(q))\,\xi_n(r) = \sum_{m'=1}^{\infty} a_{m|m'}\phi_{m'}(q)\xi_n(r),$$

i.e.,

$$\alpha_{m|m'n'} = a_{m|m'}\delta_{n|n'} \left(\delta_{n|n'} \begin{cases} = 1, & \text{for } n = n' \\ = 0, & \text{for } n \neq n' \end{cases} \right)$$

In an analogous fashion, the correspondence $A \longrightarrow A$ implies that $\alpha_{mn|m'n'} = a_{n|n'}\delta_{m|m'}$.

A statistical enscmblc in $I + II$ is characterized by its statistical operator U or by its matrix $(\ v_{mn|m|n,}\ )$. This also determines the statistical properties of all quantities in I + II , and therefore the properties of the quantities in I also. Consequently there aiso corresponds to it a statistical ensemble in I alone. In fact, an observer who could perceive only I, and not II, would view the ensemble of systems I + II as one such of systems I. What is now the statistical operator U or its matrix $\left\{u_{\mathrm{m/m^*}}\right\}$, which belongs to this I ensemble? We determine it as follows: The I quantity uith the matrix $\left(a_{m/m,}\right)$ has the matrix (a_{mjm}, δ_{njn}) as an I + II quantity, and therefore, by reason of a calculation in I, it has the expectation value

$$\sum_{m,m'=1}^{\infty} u^a_{m|m'}m' \mid m$$

while the calculation in $I + II$ gives

$$\sum_{m,n,m',n'=1}^{\infty} v^{\infty}_{mn|m'n'm'|m^5n'|n} \sum_{m,m',n=1}^{\infty} v^{o}_{mn|m'n'n'}m' \mid m = \sum_{m,m'=1}^{\infty} \left(\sum_{n=1}^{\infty} v_{mn|m'n} \right)^n m'm$$

In Urder lhat bth expressions ve equal, we must have

$$\mathrm{u_{m/m'}} = \sum_{\mathrm{n=1}}^{\infty} \mathrm{v_{mn/m'n}}$$

In the same way; our $I + IT$ ensemble, if only II is considered and I is ignored, determines a II ensemble, with a statistical operator U and matrix $\left[\mu_{n|n},\right]$. By analogy, we obtain

$$u_{n|n'} = \sum_{m-1}^{\infty} v_{mn|mn'}$$

We have thus esiablished the rules of correspondence for the statistical operators of $I, II, I + II$, i.e., U, U, U. They proved to be essentially different from those which control the correspondence between the operators A, A, A of physical quantities.

It should be mentioned that our U, U, U correspondence depends only apparently on the choice of the complete orthonormal sets $\phi_m(q)$ and $\xi_n(q)$. Indeed it was derived from an invariant condition (which is satisfied by this arrangement alone): Namely, from the requirement of agreement between the expectation values of A and of A, or of those of A and of A.
U expresses the statistics in $I + II, U$ and U those statistics restricted to I or II respectively. There now arises the question: do U, U determine U uniquely or not? In general one will expect a negative
answer because all "probability dependencies" which may exist between the two systems disappear as the information is reduced to the sole knowledge of U and U, i.e., of the separated systems I and II. But if one knows the state of I precisely, as also that of II, "prohability questions" do not arise, and then I + II , too, is precisely known. An exact mathematical discussion is, however, preferable to these qualitative considerations, and we shall proceed to this.

The problem is, then: For two given definite matrices $\{'\mathrm{m} \mid \mathrm{m},\}$ and $\left\{\mu_{\mathrm{n}|\mathrm{n}},\right\}$, find a third definite matrix $\{v_{\text{majin:}}\ :\}$, such that

$$\sum_{n=1}^{\infty} v_{mn|m'n} = u_{m|m'}, \sum_{m=1}^{\infty} v_{mn|mn'} = u_{n|n'}$$

(From

$$\sum_{m=1}^{\infty} u_{m|m} = 1, \sum_{n=1}^{\infty} u_{n|n} = 1$$

it then follows directly that

$$\sum_{m,n=1}^{\infty} v_{mn|mn} = 1$$

i.e., the correct normalization is obtained.) This problem is always solvable, for example, $v_{mn|m'n'} = u_{m|m'} u_{m|n'}$ is always a solution (it can easily be seen linat this matrix is definile), but the question arises as to whether this is the only solution.

We shall show that this is the case if and only If at least one of the two matrices $\left\{u_{m|m},\right\}, \left\{u_{n|n},\right\}$ is a state. First we prove the necessity of this condition, i.e., the existence of several solutions if both matrices correspond to mixtures. In such a case (cf. IV.2.)

$$u_{m|m'} = \alpha v_{m|m'} + \beta w_{m|m'}, u_{n|n'} = \gamma v_{n|n'} + \delta w_{n|n'}$$

(^{v} m $\mid$ m$'$, ^{w} m$\mid$ m$'$ def'inite and $\mathrm{v_{n|n}}, \mathrm{w_{n|n}}$, aiso, differing by more than a constant factor,

$$\sum_{m=1}^{\infty} v_{m|m} = \sum_{m=1}^{\infty} w_{m|m} = \sum_{n=1}^{\infty} v_{n|n} = \sum_{n=1}^{\infty} w_{n|n} = 1$$

$\alpha, \beta, \gamma, \delta > 0, \alpha + \beta = 1, \gamma + \delta = 1$).
We easily verify that each
$v_{mn!m'n} = \pi v_{m|m'} v_{n|n'} + \rho w_{m|m'} v_{n|n'} + \sigma v_{m|m'} w_{n|n'} + \tau w_{m|m'} w_{n|n'}$
with

$$\pi + \sigma = \alpha, \rho + \tau = \beta, \pi + \rho = \gamma, \sigma + \tau = \delta,$$

$$\pi, \rho, \sigma, \tau > 0,$$

is a solution. Then π, ρ, σ, τ can be chosen in an infinite number of ways: Because of $\alpha + \beta = \gamma + \delta$ only three of the four equations are independent; therefore, $\rho = \gamma - \pi, \sigma = \alpha - \pi, \tau = (\bar{\delta} - \alpha) + \pi$, and in order that a.ll be > 0, we must require $\alpha - \delta = \gamma - \beta < \pi < \alpha, \gamma$, which is the case for infinitely many π. Now different π, ρ, σ, τ lead to different $v_{mn} \mid m'n'$, because the $v_{m|m'} \cdot v_{n|n'}, \cdots, w_{m|m'} \cdot w_{n|n'}$ are linearly independent, since the $v_{m/m}, \cdot w_{m/m}$, are such, as well as the $v_{n/n} \cdot$. $\mathrm{w_{n|n}}$,

Next we prove the sufficiency, and here we may assume that $'\mathrm{m}/\mathrm{m}'$ corresponds to a state (the other case is disposed of in the same way). Then $U = P_{[\phi]}$ and since the complete orthonomal set $\phi_1, \phi_2, \ldots$ was arbitrary, we can assume $\phi_1 = \phi \cdot U = P_{[\phi_1]}$ has the matrix

$$\mathrm{u_{m|m'}} \begin{cases} = 1, \text{ for } \mathrm{m} = \mathrm{m}' = 1 \\ = 0, \text{ otherwise} \end{cases}$$

Therefore

$$\sum_{n=1}^{\infty} v_{mn/m'n} \begin{cases} = 1, \text{ for } m = m' = 1 \\ = 0, \text{ otherwise} \end{cases}$$

In particular, for $m \neq 1$,

$$\sum_{n=1}^{\infty} v_{mn|mn} = 0,$$

but since all $v_{mn|mn} \geq 0$ because of the utiniteness of $u_{mn} \mid m'n', [u_{mn} \mid mn = (u_{mn}, *_{mn})]$, therefore in this case $v_{mn|mn} = 0$. That is, $\left(\tilde{u}_{mn}, \dot{\Psi}_{mn}\right) = 0$, and hence, because of the definiteness of $U, (U\Phi_{mn}, \Phi_m, ')$ also - 0 (cf. II.5., THEOPEM 19.), where m', n' are arbitrary. That is, it follows from $m \neq 1$ that $v_{mn|m'n'} = 0$, and because of the Hermitian nature, this also follows from $m' \neq 1$. For $m = m' = 1$ however, this gives

$$v_{1n|1n'} = \sum_{m=1}^{\infty} v_{mn|mn'} = u_{n|n'}.$$

Consequently, as was asserted, the solution $v_{\mathrm{mn|m \cdot n}}$ is determined uniquely.

We can thus summarize our result as follows: A statistical ensemble in $I + II$ with the operator $U = \{v_{mn} \mid m'n'\}$ is determined uniquely by the statistical ensembles determined by it in I and II individually, with the respective operators $U = \left(u_{m|m},\right)$ and $U = (\ u_{n|n},\ \}$, if and only if the following two conditions are satisfied:

1. $v_{mn|m'n'} = v_{m|m'} v_{n|n'}$. (From

$$\operatorname{Tr} U = \sum_{m,n=1}^{\infty} v_{mn|mn} = \sum_{m=1}^{\infty} v_{m|m} \sum_{n=1}^{\infty} v_{n|n} = 1$$

it follows that, by multiplication of $v_{m|m}$, and $v_{n|n}$, with two reciprocal constant factors, we can obtain

$$\sum_{m=1}^{\infty} v_{m|m} = 1, \sum_{n=1}^{\infty} v_{n|n} = 1$$

But then we see that $u_{m|m}, = v_{m|m'}, u_{n|n'} = v_{n|n'}$.) 2. Either $v_{m|m'} = \bar{x}_m x_m$, or $v_{n|n'} = \bar{x}_n x_n$. (Indeed $U = P_{[\$]}$ means that

$$\Phi = \sum_{m=1}^{\infty} y_{mm},$$

and therefore $u_m \mid m' = \bar{y}_m y_m$, and correspondingly for $v_{m|m}$, ; by analogy the same is true with $U = P_{[\xi]}$.) We shall call U and U the projections of U in I and II respectively. [212]

We now apply ourselves to the states of I + II , $U = \mathrm{P}_{[\Phi]}$. The corresponding wave functions $\Phi(\mathrm{q}, \mathrm{r})$ can be expanded according to the complete orthonormal set $\phi_{mn}(q, r) = \phi_m(q)\xi_n(r)$:

$$\Phi(q, r) = \sum_{m,n=1}^{\infty} f_{mn}\phi_m(q)\xi_n(r)$$

We can therefore replace them by the coefficients f_{mn} ($m, n = 1, 2, \dots$) which are subject only to the condition that

$$\sum_{m,n=1}^{\infty} |f_{mn}|^2 = \|\Phi\|^2$$

be finite.

(F.)

We can define two operators F, F^* by

$$F\Phi(q) = \int \Phi(q, r)\Phi(q)dq$$
$$F^*\xi(r) = \int \Phi(q, r)\xi(r)dr \quad .$$

These are linear, but have the peculiarity of being defined in $\mathfrak{R}^I$ and $\mathfrak{R}^{II}$ respectively, and of taking on values from $\mathfrak{R}^{II}$ and $\mathfrak{R}^I$ respectively. Their relation is that of adjoints, since obviously $(F\phi, \xi) = (\phi, F^*\xi)$ (the inner product on the left is to be formed in $\widetilde{\mathfrak{N}}^{TI}$ and that on the right is to be formed in m^I). Since the difference of $\mathfrak{R}^I$ and $\mathfrak{R}^{II}$ is mathematically unimportant, we can apply the results of II.11: then, since we are dealing with integral operators, $\Sigma(F)$ and $\Sigma\left(F^*\right)$ are equal to

$$\iint |\Phi(q, r)|^2 dqdr - ||\varpi||^2 = 1 \left(||\Phi \text{ }|! \text{ in } \mathfrak{R}^{I+II_!}\right),$$

and are therefore finite. Consequently F, F^* are continuous, in fact are completely continuous operators, and F^*F as well as FF^* are definite operaturs, $TF^*\left(F^*F\right) = \Sigma(F) = 1, \mathrm{Tr}\left(FF^*\right) - \Sigma\left(F^*\right) = 1$.

If we again consider the difference between $\mathfrak{R}^I$ and $\mathfrak{R}II$ then we see that F^*F is defined and assumes values in $\mathfrak{R}^I$, and FF^* similarly in $\mathfrak{R}^{II}$.

Since $F\phi_m(q)$ comes out equal. to

$$\sum_{n=1}^{\infty} \bar{f}_{mn}\xi_n(r)$$

F has the matrix $\left(\bar{f}_{mn}\right.$) [by use of the complete orthonormal sets $\phi_m(q)$ and $\bar{\xi}_n(r)$ respectively – note that the latter is a complete orthonormal set along with $\xi_n(r)$], likewise F^* has the matrix $\{f_{mn}\}$ (with the same complete orthonormal systems). Therefore F^*F, F^* have the matrices

$$\left\{\sum_{n=1}^{\infty} \bar{f}_{mn^0}n^0{}_{\cdot n}\right\}$$

[8212] The projections of a state of $I + II$ are in general mixtures in I or II ; cf. above. This circumstance was discovered by Landau, Z. Physik 45 (1927).

(using the complete orthonormal set $\Phi_m(q)$ in $\mathfrak{R}^I$) and

$$\left\{\sum_{n=1}^{\infty} \bar{f}'_{\overline{un}} f_{\overline{wn}},\right\}$$

(using the complete orthonormal set $\overline{\xi_n(r)}$ in $\mathfrak{R}^{II}$).
On the other hand, $U = \mathrm{P}_{[\phi]}$ has the matrix ($\bar{f}'_{mn} f'_{m'n'}$) (using the complete orthonormal set $\Phi_{mn}(q,r) = \Phi_m(q)\xi_n(r)$ in $\mathfrak{R}^{T+TT}$), so that its projeclions in I and II, U and U have the matrices

$$\left\{\sum_{n=1}^{\infty} \bar{f}_{mn} f_m : n\right\}$$

and

$$\left\{\sum_{m=1}^{\infty} \tilde{r}_{mn^1}{}^n n'\right\}$$

respecidvely (with the complete orthonormal sets given above). [213] Consequently

$$U = F^* F, U = F F^* \qquad (U\cdot)$$

Note that the definitions (F.) and the equations (**U**.) make no use of the Φ_{m}, ξ_{11}– hence they are valid independently of these.

The operators U, U are completely continuous, and by II.11. and IV.3., they can be written in the form

$$U = \sum_{k-1}^{\infty} w_k^i \bar{P}_{[\psi_k]}, \quad \bar{U} = \sum_{k=1}^{\infty} w''_k \bar{P}_{[\eta_k]},$$

in which the ψ_k form a complete orthonormal set in $\mathfrak{R}^I$, Lise η_k one in π^{TT} and all $w_k, w_k^{\cdot\cdot} \geq 0$. We now neglect the terms in each ot the two formulas with $w_k = 0$ or $w''_k = 0$ respectively, and number the remaining terms with $k = 1, 2, \ldots$. Then the ψ_k and η_k again form orthonormal, but not necessarily complete sets; the sums

$$\sum_{k=1}^{M'}, \sum_{k=1}^{M''}$$

appear in place of the two

$$\sum_{k=1}^{\infty}$$

where M', M'' can be equal to ∞ or finite. Also, all w'_k, w''_k are now > 0.

Let us now consider a ${}^*_K \quad {}^*_K - {}^*_{\substack{K\\V}} K$ and therefore $F^* F \psi_k = w'_k \psi_k, F F^* F \psi_k = w'_k F \psi_k, U F \psi_k = w'_k F \psi_k$. Furthermore

$$\begin{aligned}(F\psi_k, F\psi_l) &= (F^* F \psi_k, \psi_l) = (U\psi_k, \psi_l) \\ &= w'_k (\psi_k, \psi_l) \begin{cases} = w'_k, & \text{for } k = 1 \\ = 0, & \text{for } k \neq 1 \end{cases}\end{aligned}$$

[213] The mathematical discussion is based on a paper by E. Schmidt, Math. Ann. 83 (1907).

therefore, in particular, $||F\psi_k||^2 = w'_k$. The $\frac{1}{\sqrt{w'_k}} F w_k$
then form an orthonormal set in R^{II} and they are eigenfunctions of U, with the same eigenvalues as the ψ_k for U (i.e., w'_k). That is, each eigenvalue of u is
also one of U with at least the same multiplicity. Interchanging U, U shows that they have the same eigenvalues with the same multiplicities. The w'_k and w''_k therefore coincide except for their order. Hence $M'\ M'' = M$, and by re-enumeration of the w''_k we can obtain $\mathrm{w'_k} = \mathrm{w''_k} = \mathrm{w_k}$. And if this occurs, then we can clearly choose

$$\eta_k = \frac{1}{\sqrt{w_k}} F\psi_k$$

in general. Then

$$\frac{1}{\sqrt{w_k}} F^* \eta_k = \frac{i}{w_k} F^* F \psi_k = \frac{i}{w_k} \quad U\psi_k = \psi_k$$

Therefore

$$\eta_k = \frac{1}{\sqrt{w_k}} F\psi_k, \quad \psi_k = \frac{1}{\sqrt{w_k}} F^* \eta_k \cdot 212 \tag{$v\cdot$}$$

Let us now extend the orthonormal set $\psi_1, \psi_2, \ldots$ to a complete $\psi_1, \psi_2, \ldots, \psi'_1, \psi'_2, \ldots$ and likewise $\eta_1, \eta_2, \ldots$ to $\eta_1, \eta_2, \ldots, \eta_1, \eta_2, \ldots$ (each of the two sets $\psi'_1, \psi'_2, \cdots$ and $\eta'_1, \eta'_2, \ldots$ can be empty, finite or infinite, and in addition each set independently of the other set). We have observed before, that (F.), (U.) make no reference to the Φ_m, ξ_n. We may therefore use (**v**.), as well as the above construction, and let them determine the choice of the complete orthonormal sets $\phi_1, \phi_2, \cdots$ and $\xi_1, \xi_2, \ldots$. Specifically we let these coincide with the $\psi_1, \psi_2, \ldots, \psi'_1, \psi'_2, \ldots$ and $\bar\eta_1, \bar\eta_2, \ldots, \bar\eta'_1, \bar\eta'_2, \ldots$ respectively. Now let ψ_k correspond to ϕ_{μ_k}, η_k to ${}^{\xi}\nu_k$ ($k = 1, \ldots, M$) ($\mu_1, \mu_2, \ldots$ different from one another, $v_1, v_2, \ldots$ likewise). Then

$$F\phi_{\mu_\mathrm{K}} = \sqrt{w_\mathrm{k}}\xi_{\nu_\mathrm{k}},$$
$$F\phi_\mathrm{m} = 0 \text{ for } m \neq \mu_1, \mu_2, \ldots.$$

Therefore

$$\mathrm{f_{mn}} \begin{cases} = \sqrt{w_k}, \text{ for } m = \mu_k, n = v_k, k = 1, 2, \ldots \\ = 0, \text{ otherwise} \end{cases}$$

or equivalently

$$\Phi(q, r) = \sum_{k=1}^{M} \sqrt{w}_k \Phi_{\mu_k}(q) \xi_{v_k}(r).$$

By suitable choice of the complete orthonormal sets $\phi_m(q)$ and $\xi_n(r)$ we have thus established that each column of the matrix $\{f_{mn}\}$ contains at most one element $\neq 0$ (hat this is real and > 0, namely $\sqrt{w}_k$, is unimportant for what follows). What is the physical meaning of this mathematical statement?

Let A be an operator with the eigenfunctions $\phi_1, \phi_2, \cdots$ and with only distinct eigenvalues, say $a_1, a_2, \ldots$; likewise B with $\xi_1, \xi_2, \ldots$ and $b_1, b_2, \ldots$. A corresponds to a physical quantity in I, B to one in II. They are therefore simultaneously measurable. It is easily seen that the statement "A has the value a_m and B has the value b_n " determines the state $\Phi_{mn}(q, r) = \Phi_m(q)\xi_n(r)$, and that this has the probability $\left(P_{[\Phi_{mn}]}\Phi, \Phi\right) = |(\Phi, \Phi_{mn})|^2 = |f_{mn}|^2$ in the state $\Phi(q, r)$. Consequently, our statement means that A, B are simultaneously measurable, and that if one of them was measured in Φ, then the value of the other is determined by it uniquely. (An a with all $f_{mn} = 0$ cannot result, because its total probability

$$\sum_{n=1}^{\infty} |f_{mn}|^2$$

cannot be 0 , if a_m is ever observed
therefore for
exactly one $\mathrm{n}, \mathrm{f_{mn}} \neq 0$; likewise for $\mathrm{b_n}$.) That is, there are several possible A values in the state Φ (namely, those a_m for which

$$\sum_{n=1}^{\infty} |f_{mn}|^2 > 0$$

i.e., for which there exists an n with $f_{\mathrm{III}} \neq 0$-usually all a_m are such), and an equal number of possible B values (those b_n for which

$$\sum_{n=1}^{\infty} |f_{mn}|^2 > 0$$

i.e., for which there exists an m with $f_{mn} \neq 0$), but Φ establishes a one-to-one correspondence between the possible A values and the possible B values.

If we call the possible m values $\mu_1, \mu_2, \ldots$ and the corresponding possible n values $v_1, v_2, \ldots$, then

$$\mathrm{f_{mn}} \begin{cases} = \mathrm{c_k} \neq 0, & \text{for } \mathrm{m} = \mu_{\mathrm{k}}, \mathrm{n} = v_{\mathrm{k}}, \mathrm{k} = 1, 2, \ldots \\ = 0, & \text{otherwise} \end{cases}$$

therefore (M finite or ∞)

$$\Phi(q, r) = \sum_{\underline{k}=1}^{M} c_{k^{\phi}\mu_k}(q) \xi_{v_k}(r),$$

hence

$u_{mm'} = \sum_{n=1}^{\infty} \tilde{f}_{mn'} f_{m'n} \begin{cases} = |c_k|^2, \text{ for } m = m' = \mu_k, k = 1, 2, \cdots \\ = 0, \text{ otherwise} \end{cases}$,

$u_{nn'} = \sum_{\overline{II}-1}^{\infty} \bar{f}_{mn'mn'} \begin{cases} = |c_k|^2, \text{ for } n = n' = v_k, k = 1, 2, \ldots \\ = 0, \text{ otherwise} \end{cases}$

and therefore

$$U = \sum_{k=1}^{M} |c_k|^2 P_{\left[\phi_{\mu_k}\right]}, U = \sum_{k=1}^{M} |c_k|^2 P_{\left[\xi_{v_k}\right]}.$$

Hence, when Φ is projected in I or II, it in general becomes a mixture, while it is a state in $I + II$ only. Indeed, it involves certain information regarding I + II which cannot be made use of in I alone or in II alone, namely the one-to-one correspondence of the A and B values with each other.

For each Φ we can therefore so choose A, B, i.e., the $\oplus_m$ and the ξ_n; that our condition is satisfied; for arbitrary A, B, it may of course be violated. Each state Φ then establishes a particular relation between I and II, while the related quantities A, B depend on Φ. How far φ determines them, i.e., the †m and the ξ_n, is not difficult to answer. If all $|c_k|$ are different and $\neq 0$, then U, U (which are determined by Φ) determine the respective ϕ_m, ξ_n uniquely (cf. IV.3.). The general discussion is left to the reader. Finally, let us mention the fact that for $\mathrm{M} \neq 1$ neither U nor U is a state (because all $|c_K|^2 > 0$). For $M = 1$ they both are:

$U = P_{[\phi_{\mu_1}]}, U = P_{[\xi_{\nu_1}]}$. Then $\Phi(q,r) = c_1\phi_{\mu_1}(q)\xi_{\nu_1}(r)$. We can absorb c_1 in $\phi_{\mu_1}(q)$. Therefore U, U are states if and only if $\phi(q,r)$ has the form $\phi(q)\xi(r)$, and in that case they are equal to $P_{[\Phi]}$ and $P_{[\xi]}$ respectively.

On the basis of the above results, we note: If

I is in the state $\phi(q)$ and II in the state $\xi(r)$, then $I+II$ is in the state $\Phi(q,r) = \phi(q)\xi(r)$. If on the other hand $I+II$ is in a state $\phi(q,r)$ which is not a product $*(q)\xi(r)$, then I and II are mixtures and not states, but Φ establishes a one-to-one correspondence between the possible values of certain quantities in I and in II.

28.3.3 3. Discussion of the Measuring Process

Before we complete the discussion of the measuring process in the sense of the ideas developed in VI. 1. (with the aid of the formal tools developed in VI.2.), we shall make use of the results of VI.2. to exclude a possible explanation often proposed for the statistical character of the process 1. (V.1.). This rests on the following idea: Let I be the observed system, II the observer. If I is in a state $U = P_{[\Phi]}$ before the measurement, while II on the other hand is in a mixture

$$U = \sum_{n=1}^{\infty} w_n P\left[\xi_n\right],$$

then I + II is a uniquely determined mixture U, and in fact, as we can easily calculate from VI.2.,

$$U = \sum_{n=1}^{\infty} w_n P\left[\Phi_n\right], \quad \Phi_n(q,r) = \phi(q)\xi_n(r)$$

If now a measurement of a quantity A takes place in I, then this is to be regarded as an interaction of I and II. This is a process 2. (V.1.), with an energy operator H. If it has the time duration t, then we obtain

$$U' = e^{-\frac{2\pi i}{h}tH} U e^{\frac{2\pi i}{h}tH}$$

from U, and in fact,

$$\boldsymbol{U'} = \sum_{n=1}^{\infty} W_n P \left[\begin{array}{ll} -\frac{2\pi i}{h} t\boldsymbol{H} & \\ e^{-\frac{2\pi}{2}} & \Phi_n \end{array} \right]$$

If now each

$$e^{-\frac{2\pi i}{n}+H}\Phi_n(q,r)$$

were of the furm $\Psi_n(q)\eta_n(r)$, where the Ψ_n are the cigenfunctions of A, and the η_{11} any fixed complete orthonormal set, then this intervention would have the character of a measurement. For it transforms each state ϕ of I into a mixture of the eigenfunctions ψ_n of $\dot{A}$. The statistical character therefore arises in this way: Before the mossurement I was in a (unique) state, but II was a mixture – and the mixture character of II has, in the course of the interaction, associated itself with I + II, and in particular, it has made a mixture of the projection in I. 'hat is, the result of the measurement is indeterminate, because the state of the observer before the measurement is not known exactly. It is conceivable that such a mechanism might function, because the state of information of the observer regarding his own state could have absolute limitations, by the laws of nature. These limitations would be expressed in the values of the w_n, which are characteristic of the observer alone (and therefore independent of ϕ)

At this point, the attempted explanation breaks down. For quantum mechanics requires that $w_n = (P_{\psi_n}\phi, \phi) = |(\phi, \psi_n)|^2$, i.e., w_n dependent on ϕ : There might exist another decomposition

$$U' = \sum_{\mathrm{n}=1}^{\infty} \mathrm{w}'_{\mathrm{n}} \mathrm{P}\left[\varphi'_{\mathrm{n}}\right],$$

(the $\Phi'_n(q,r) = \psi_n(q)\eta_n(r)$ are orthonormal) but this is of no use either; because the w'_n are (except for order) determined uniquely by U' (IV.3.), and are therefore equal to the w_n.[214]

Therefore, the non-causal nature of the process 1. is not produced by any incomplete knowledge of the state of the observer, and we shall therefore assume in all that follows that this state is completely known.

Let us now apply ourselves again to the problom formulated at the end of VI.1. T, TT. III shall have the meanings given there, and, for the quantum mechanical investigation of I, II, we shall use the notation of VI.2., while III remains outside of the calculations (cf. the discussion of this in VI.|.). Lei A ve the quantity (in I) actually to be measured, $\phi_1(q), \phi_2(q), \ldots$ its eigenfunctions. Let I be in the state $\phi(q)$.

If I is the observed system, II + III the observer, then we must apply the process 1., and we find that the measurement transforms I from the state $\dot{\phi}$ into one of the states ${}^{\dagger}\mathrm{n}(\mathrm{n} = 1, 2, \ldots)$, the probabilities for which are respectively $|(\Phi, \Phi_n)|^2$ $(n = 1, 2, \ldots)$. Now, what is the method of description if $I + II$ is the observed system, and only III the observer?

In this case we must say that. II is a measuring. instrument which shows on a scale the value of A (in I): the position of the pointer on this scale is a physical quantity B (in II) which is actually observed by III (if II is already within the body of the observer, we have the corresponding physiological concepts in piace of the scale and pointer, e.g., retina and image on the retina, etc.) Let A have the values $a_1, a_2, \ldots, b$ the values $\mathrm{b}_1,\ \mathrm{b}_2, \ldots$, and let the numbering be such that $\mathrm{a_n}$ is associated with b_n.

Initially, I is in the (unknown) state $\varphi(q)$ and II in the (known) state $\xi(r)$, therefore $I + II$ is in the state $\Phi(q,r) = \Phi(q)\xi(r)$. The measurement (so far as it is performed by II on I) is, as in the earlier example, carried out by an energy oporator H (in I+ II) in the time t : This is the process 2., which transforms the Φ into

$$\Phi' = e^{-\frac{2\pi \mathrm{i}}{\mathrm{h}} \mathrm{t} H}\Phi.$$

Viewed by the observer III, one has a measurement only if the following is the case: If III were to measure (hy process 1.) the simultaneously measurable quantities A, B (in I or II respectively, or both in $I + II$), then the pair of values a_n, b_n would have the probability 0 for $m \neq n$, and the probability w_n for $m = n$. That is, it suffices "to look at" II, and A is measured in I. Quantum mechanics then requires in addition $W_n = |(\phi, \phi_n)|^2$.

If this is established, then the measuring process so far as it occurs in II, is "explained" theoretically, i.e., the division of $I \mid II\ +\ III$ *discusscd* in VI.1. is shifted to I + II | III .

The mathematical problem is then the following. A complete orthonormal set $\phi_1, \phi_2, \cdots$ is given in I. Such a set $\xi_1, \xi_2, \ldots$ in $\mathfrak{R}^{\mathrm{II}}$ as well as a state ξ in R^I, also an (energy) operator H in $\mathfrak{R}^{I+II}$, and a t, are to be found so that the following holds. If Φ is an arbitrary state in R^I and

$$\Phi(\mathrm{q}, \mathrm{r}) = \Phi(\mathrm{q})\xi(\mathrm{r}), \Phi'(\mathrm{q}, \mathrm{r}) = \mathrm{e}^{-\frac{2\pi \mathrm{i}}{\mathrm{h}} \mathrm{t} H}\Phi(\mathrm{q}, \mathrm{r}),$$

then $\Phi'(q,r)$ must have the form

$$\sum_{n=1}^{\infty} c_n \phi_n(q)\xi_n(r)$$

[214] This approach is capable of still more variants, which must be rejected for similar reasons.

(the c_n are naturally dependent on ϕ). Therefore $|c_{i1}|^2 = |(\phi, \phi_{i1})|^2$. (That the latter is equivalent to the physical requirement formulated above was discussed in VI.2.)

In the following we shall use a flxed set $\xi_1, \xi_2, \ldots$ and a fixed ξ along with the fixed $\phi_1, \phi_2, \ldots$, and shall investigate the unitary operator

$$\Delta = e^{-\frac{2\pi i}{h} tH}$$

instead of H.

The mainematical problem leads us back to the problem solved in VI.2.: there the quantity corresponding to our present Φ was given, and we showed the existence of c_n, ϕ_n, ξ_n. Now ϕ_n, ξ_n are fixed and Φ, c_n are given dependent on ϕ, and it remains so to determine a fixed Δ that for $\Phi' = \Delta\Phi$ these c_n, Φ_n, ξ_n result. Wo shall show that such a determination of Δ is indeed possible. In this case only the principle is of importance to us, i.e., the existence of any such Δ. The further question, whether the

$$\Delta = e^{-\frac{2\pi i}{h} tH}$$

corresponding to simple and plausible measuring arrangoments also have this property, shall not concern us. Indeed, we saw that our requirements coincide with a plausible intuitive criterion of the measurement character in an intervention. Furthermore the arrangements in question are to possess the characteristics of the measurement. Hence quantum mechanics, as applied to observation would be in blatant contradiction with experience, if these Δ did not satisfy the requirements in question (at least approximately). [215] Therefore, in the following, only an abstract

Δ which satisfies our conditions exactly, shall be given. Therefore, let the $\phi_m (m = 0, \pm 1, \pm 2, \ldots)$ and the $\xi_{\mathrm{n}} (\mathrm{n} = 0, \pm 1, \pm 2, \ldots)$ respectively be two given complete orthonormal sets in π^T and π^{TT} respectively. (We do not lot m, n run over 1,2,..., but over $0, \pm 1, \pm 2, \ldots$. This is purely for technical convenience, and is in principle equivalent to the former). Let the state ξ be, for simplicity, ξ_0. We define the operator Δ by

$$\Delta \sum_{m,n-m}^{\infty} x_{mn} \varphi_m(q) \xi_n(r) = \sum_{m,n=-\infty}^{\infty} x_{mn}{}^{\phi} m^{(\varphi)\xi_{m+n}}(r),$$

since the $\phi_m(q)\xi_n(r)$ as well as the $\phi_m(q)\xi_{m+n}(r)$ form a complete orthonormal set in $\mathfrak{R}^{I+II}$, this Δ is unitary. Now

$$\phi(q) = \sum_{m=-\infty}^{\infty} (\phi . \phi_{\overline{iII}}) \cdot \phi_{\overline{iI}}(q), \xi(r) = \xi_0(r),$$

therefore

$$\Phi(q, r) = \Phi(q)\xi(r) = \sum_{m=-\infty}^{\infty} (\phi, \Phi_m) \cdot \Phi_m(q)\xi_o(r)$$

$$\Phi'(q, r) = \Delta\Phi(q, r) = \sum_{m=-\infty}^{\infty} (\phi, \Phi_m) \cdot \Phi_m(q)\xi_m(r)$$

Hence our purpose is accomplished. We have in addition $c_n = (\phi, \phi_n)$.

A better overall view of the mechanism of this process can be obtained if we exemplify it by concrete Schrödinger wave functions, and give H in place of Δ. The observed object, as well as the observer

[8]215 The corresponding calculation for the case of the posi-

[8]tion measurement discussed in III.4, is contained in a paper by Weizscker, Z. Physik 70 (1931).

(i.e., I and II respectively) may be characterized by a single variable q and r respectively, running continuously from $-\infty$ to : ∞. That is, let both be thought of as points which can move along a line. Their wave functions then have always the form $\psi(q)$ and $\eta(r)$ respectively. We assume that their masses m_1 and m_2 are so large that the kinetic energy portion of the energy uperator (i.e., $\frac{1}{2m_1}\left(\frac{h}{2\pi i}\frac{\partial}{\partial q}\right)^2+\frac{1}{2m_2}\left(\frac{h}{2\pi i}\frac{\partial}{\partial r}\right)^2\Big)$ can bo neglected. Then there remains of H only the interaction energy part which is decisive for the measurement. For this we choose the particular form $\frac{h}{2\pi j}q\frac{\partial}{\partial r}$.

The Schrödinger time dependent differential equation then is (for the $I+II$ wave functions $\psi_t=\psi_t(q,r)$) :

$$\frac{h}{2\pi i}\frac{\partial}{\partial t}\psi_t(q,r)=-\frac{h}{2\pi i}q\frac{\partial}{\partial r}\psi_t(q,r),$$

$$\left(\frac{\partial}{\partial t}+q\frac{\partial}{\partial r}\right)\psi_t(q,r)=0$$

i.e.,

$$\psi_t(q,r)=f(q,r-tq)$$

If, for $t=0,\psi_0(q,r)=\Phi(q,r)$, then we have $f(q,r)=\Phi(q,r)$, and therefore

$$\psi_t(q,r)=\Phi(q,r-tq)$$

In particular, if the initial statos of I, II are represented by $\phi(q)$ and $\xi(r)$ respectively, then, in the sense of our calculation scheme (if the time t appearing therein is chosen to be 1)

$$\Phi(q,r)=\Phi(q)\xi(r),$$
$$\Phi'(q,r)=\psi_1(q,r)=\Phi(q)\xi(r-q).$$

We now wish to show that this can be used by II for a position measurement of I, i.e., that the coordinates are tied to each other. (Since q,r have continuous spectra, they are therefore measurable with only arbitrary precision, but not with absolute precision. Hence this can be accomplished only approximately.)

For this purpose, we wish to assume that $\xi(r)$ is different from 0 only in a very small interval $-\epsilon<r<\epsilon$ (i.e., the coordinate r of the observer before the measurement is very accurately known), in addition ξ should of course be normalized:

$$||\xi||=1,\text{ i.e., }\int|\xi(r)|^2dr=1.$$

The probability therefore that q lics in the interval $q_0\quad\delta<q<q_0+\delta$, and r in the interval $r_C-\delta'<r<r_o+\delta'$ is
$\int_{q_0-\delta}^{q_0+\delta}\int_{r_0-\delta}^{r_0^{+\delta}}\left|\phi'(q,r)\right|^2dqdr=\int_{q_0-\delta}^{q_0^{+\delta}}\int_{r_0-\delta}^{r^{+\delta}}|\phi(q)|^2|\xi(r-q)|^2dqdr.$
If q_0,r_0 are to differ by more than $\delta^+\delta'+\epsilon$, then this is 0 , i.e., q,r are so very closely tied to each other that the difference can never be greater than $\delta+\delta'+\epsilon$. And for $r_0=q_0$ this is, equal to

$$\int_{q_0-\delta}^{q_0+\delta}|\phi(q)|^2dq$$

if we choose $\delta'\geq\delta+\epsilon$, because of the assumptions on ξ. But since we can choose δ,δ',ϵ arbitrarily small (they must be different from zero, however), this means that q,r are tied to each other with arbitrary closeness, and the probability density has the value furnished

by quantum mechanics, $|\phi(q)|^2$.
That is, the relations of the measurement, as we had discussed them in IV.1., and in this section, are realized.

The discussion of more complicated examples, say of an analog to our four-term example of IV.1., or the control determination of the validity of a measurement which II carried out on I, effected by a second observer III, can also be carried out in this fashion. It is left to the reader.

28.4 V.3 The Ergodic Behavior of Qntumm Many-body Systems by Van Hove

Synopsis

By a pertubation technique adapted to the actual properties of gases and solids (and possibly also of liquids) we have established in previous papers that under suitapproaches statistical equilibrium as anperturbed far as those physical quantities are concerned representation. This result is now extended to non-diagonal quantion enough to include all observables of actual interest. A general discussion of ergodic theorem is given, and its implications for classical statistics are brieny analyzed. The paper ends with a discussion of a recent article by Ingraham on the application of our methods to the case of a very small perturbation. The main arguments of Ingraham are shown to be in error, and the inconsistencies he derives from them are thereby disproved.

1. Introduction. The approach of a quantum many-body system to statistical equilibrium has been studied in two previous papers [1]), to be referred to hereafter as S and S', on the basis of a separation of the hamiltonian H' into a main term H describing non-interacting plane wave ex citations (like phonons or Bloch electrons in solids, free particles in gases) and a perturbation λV representing their mutual interaction. Using as basic representation the eigenstates $|\alpha\rangle$ of H, each of which describes a set of plane wave excitations, we founded our tratment on the recognition that the matrix elements to be calculated according to perturbation theory exhibit remarkable diagonal singularities, i.e. singularities of the form $\delta(\alpha - \alpha')$. A systematic analysis of these singularities made it possible to study the time evolution of certain physical quantities A under the assumption of incoherent phases for the amplitudes $c(\alpha)$ of the initial state φ_0 of the system *)

$$\psi_0 = \int |\alpha\rangle dac(\alpha). \tag{1.1}$$

Under proper conditions it could be established that in the course of time the expectation value of A, which is (we put $\hbar = 1$)

$$\langle A\rangle_t = \langle\varphi_0|\, U_{-t} A U_t\, |\varphi_0\rangle\,, U_t = \exp[-i(H + \lambda V)t], \tag{1.2}$$

*) A detailed definition of our notation is found in S'.
tends to the equilibrium value $\langle A\rangle_{eq}$ calculated on the basis of microcanonical ensemble theory. This was established for operators A diagonal in the α >-representation, in the case of very small perturbation in S and for finite λV, i.e to general order in the dimensionless parameter λ, in S'.

Our present aim is to extend the general order treatment of S' to a wide class of non-diagonal operators B^{**}). This class is composed of the nondiagonal operators B given by a convergent series, each term of which is a product of creation and destruction operators for individual plane wave excitations. We assume the number of creation and destruction operators in each term of the series to be finite and independent of the large number N of particles in the system.

In contrast to the diagonal operators A, the class of operators B just defined is broad enough to contain all quantities of practical interest. Since we will again be able to establish that the expectation value

$$\langle B\rangle_t = \langle\varphi_0|\, U_{-t}BU_t\,|\varphi_0\rangle \tag{1.3}$$

tends to the microcanonical equilibrium value $\langle B\rangle_{eq}$ we will have established, for all practical purposes, the ergodic behaviour of our system, using only the properties of the hamiltonian postulated in S' (sections 2 and 7) and the incoherent phase assumption for the initial state (1.1).

The rather broad scope of this result makes it desirable to discuss its significance, also in relation to classical statistics. Whereas the derivation of our main result

$$\langle B\rangle_t \to \langle B\rangle_{eq} \text{ for } t \to \pm\infty \tag{1.4}$$

is presented in the next section, section 3 will be devoted to this general discussion. Section 2 will make free use of the formal technique developed and applied in S'. Although the author is fully aware of the complication of this technique, he believes that the scope of the results may justify at least partially the involved nature of the mathematical methods. Section 3 gives a nontechnical discussion which can be largely followed without knowledge of the detailed formalism of section 2 and S'. Section 4 presents a refutation of a critical discussion of S recently published by Ingraham.

2. Approach to equilibrium for non-diagonal operators. For any operator B of the type described above and for any set of diagonal operators $A_1, \ldots, A_n$ the matrix element

$$\langle\alpha|VA_1VA_2V\ldots A_\nu BA_{\nu+1}V\ldots A_nV\,|\alpha'\rangle \tag{2.1}$$

can have a $\delta(\alpha-\alpha')$-singularity for the same reasons and with the same properties as was the case for the matrix elements $\langle\alpha|VA_1V\ldots A_nV\,|\alpha'\rangle$

considered in S' (see S', section 2). The discussion of this singularity requires that (2.1) be written out as a sum over intermediate states α_j. In addition to having one V replaced by B this sum may differ from the sum (S'.2.6) *) by the fact that additional intermediate states may have to be introduced in between various factors of a single term of B. This would for example be the case if $B = V_1V_2, V_1$ and V_2 being individual terms in the expansion of V in products of creation and destruction operators. In this particular case one would obviously insert an additional intermediate state between V_1 and V_2. All considerations presented in S' (section 2) can be repeated for this slightly more general case, however, and we can define in addition the concept of B-irreducible diagonal part. It is the diagonal part, i.e. the $\delta(\alpha-\alpha')$-singular part. of (2.1) which is obtained when in the calculation of (2.1) one leaves out the diagonal part of each subproduct of the following type

$$\left.\begin{array}{l} VA_jV\ldots A_kV, (1\le j\le k<\nu \text{ or } \nu+1<j\le k\le n) \\ VA_jV\ldots A_\nu BA_{\nu+1}V\ldots A_kV, (1\le j\le \nu<k\le n, k-j<n-1, \\ VA_jV\ldots A_\nu B, (1\le j\le\nu), \quad BA_{\nu+1}V\ldots A_kV, (\nu+1\le k\le n) \end{array}\right\} \tag{2.2}$$

We denote by $\{VA_1V\ldots A_\nu BA_{\nu+1}V\ldots A_nV\}_{Bd}$ the diagonal operator defined by the B-irreducible diagonal part of (2.1). This concept may differ from the irreducible diagonal part defined in S' because of the possible occurrence of additional intermediate states inside B (these states are allowed to become equal to each other, to other intermediate states, to α or to α', and the corresponding subproducts, in contrast to the subproducts (2.2), may therefore contribute

[8]**) As in S and S' the adjectives diagonal and non-diagonal will always refer to the $|\alpha\rangle$-representation.

their diagonal part). The new concept can be extended in an obvious way to products of the type

$$BA_1V\ldots A_nV,\quad VA_1\ldots VA_nD. \tag{2.3}$$

Its importance will appear presently.
In analogy to our analysis in S', which made essential use of the quantity $X_{ll'}(\alpha\alpha')$ defined by (S'.4.14), we must consider the quantity $Y_{ll'}(\alpha)$ defined by

$$\{R_iBR_{i'}\}_a \,|\propto> -|\approx> Y_{u'}(\alpha) \tag{2.4}$$

where R_l is the resolvent (S'. 4.1). Reduction of diagonal parts, using (S'. 4. 4) and our definition of B-irreducible diagonal part, readily gives

$$\{R_lBR_{l'}\}_d = \{R_lB_{ll'}R_{l'}\}_d \tag{2.5}$$

with

$$B_{ll'} = \left\{\left(1-\lambda VD_l+\lambda^2VD_lVD_l\ldots\right)B\left(1-\lambda D_{l'}V+\lambda^2D_{l'}VD_{l'}V\ldots\right)\right\}_{Bd} \tag{2.6}$$

Hence, using (S'.4.14),

$$Y_{ll'}(\alpha) = \int B_{ll'}(\alpha')\,d\alpha' X_{ll'}(\alpha'\alpha) \tag{2.7}$$

where $B_{ll'}(\alpha')$ is the eigenvalue of the diagonal operator $B_{ll'}$ for the state α'.
In analogy to (S'. 4.13) we have

$$U_{-t}BU_t = -(2\pi)^{-2}f_\gamma dl\, f_\gamma dl' \exp\left[i\left(l-l'\right)t\right]R_lBR_{l'} \tag{2.8}$$

where the contour γ in the complex plane encircles an interval of the real axis sufficiently large to include the whole energy spectrum of the system and is described counterclockwise. Calculating the expectation value of (2.8) for the initial state $\varphi 0$, and using the incoherent phase assumption for the amplitudes $c(\alpha)$ of φ_0 one obtains

$$\langle B\rangle_t = -(2\pi)^{-2}\int_\gamma dl\int_\gamma dl' \exp\left[i\left(l-l'\right)t\right]Y_{ll'}(\alpha)d\alpha|c(\alpha)|^2 \tag{2.9}$$

The long time limit of this quantity is found by repeating for $Y_{ll'}$ the discussion carried our for $X_{ll'}$ in section 6 of S'. No new difficulty occurs in this discussion because the quantity $B_{ll'}(\alpha')$ by virtue of its definition remains finite and has only finite discontinuities for l and l' crossing the real axis. According to (2.7) the pseudopoles of $Y_{E+l,E-l}$ therefore coincide with those of $X_{E+l,E-l}$. In analogy with (S'.6.18) one finds for the limit of (2.9) as $t\to\pm\infty$

$$\langle B\rangle_{\pm\infty} = \pi^{-1}\int_{-\infty}^{\infty}dE\int\lim_{0<\eta-\eta}\{\eta Y_{EFi\eta,E+i\eta}(\alpha)\}\,d\alpha\mid c(\alpha).$$

We go back to (2.7) and remember that $B_{ll'}$ remains finite when l and l' approach the real axis. This gives

$$\lim\eta Y_{E\mp i\eta,E\pm i\eta}(\alpha) = \int B_{E\mp i0,E\pm i0}(\alpha')\,d\alpha'\lim\eta X_{E\mp i\eta,E\pm i\eta}(\alpha'\alpha) \tag{2.11}$$

The limit on the righthand side has been calculated in section 7 of S', with the result (see (S'.7.9) and (S'.7.17) and the third equation therefter)

$$\pi^{-1} \lim \eta X_{\bar{E}\pm i\eta, \bar{E}+i\eta}(\alpha'\alpha) = \Delta_E(\alpha')\,\Delta_E(\alpha) \left[\int \Delta_E(\alpha'')\, d\alpha''\right]^{-1}. \tag{2.12}$$

We obtain by substitution

$$\langle B\rangle_{\pm\infty} = \int_{-\infty}^{\infty} \langle B\rangle_E p_E dE. \tag{2.13}$$

$p_E dE$, defined by (S'.7.22), is the probability that the total energy $H + \lambda V$ bf included between E and $E + dE$ for the system in its initial state φ_0, unde1 the incoherent phase assumption. The quantity $\langle B\rangle_E$ is defined by

$$\langle B\rangle_E = \left[\int \Delta_E(\alpha'')\, d\alpha''\right]^{-1} \int B_{E\mp i0, E\pm i0}(\alpha')\, d\alpha' \Delta_E(\alpha'). \tag{(2.14}$$

As will now be shown, it is equal to the microcanonical average of B or the energy shell $H + \lambda V = E$ and its value is independent of the double sign appearing in the definition.

The microcanonical average of B is

$$Sp(BQ_E)/Sp(Q_E), \tag{(2.15}$$

Q_E being the projection operator on the energy shell $H + \lambda V = E$. One ha

$$Q_F = \delta(H + \lambda V - E) = (2\pi i)^{-1} \lim_{0<\eta\nabla\cdot 0} (R_{F+i\eta} - R_{F-i\eta}).$$

But the resolvent verifies

$$R_{E+i\eta} - R_{E-i\eta} - 2i\eta R_{E+i\eta} R_{E-i\eta}$$

a relation which cnables us to write

$$S\dot{p}(BQ_E) = \pi^1 \lim \eta S\dot{p}(R_{E\mp i\eta} B R_{E\pm i\eta}) = \pi^1 f d\alpha \lim \eta Y_{E\mp i\eta, E\pm i\eta}(\alpha)$$

Here we have calculated the trace in the $|\alpha\rangle$-representation. The limit under the integral sign has been found in (2.11) and (2.12). It gives

$$Sp(BQ_E) = \int B_{E\mp i0, E\pm i0}(\alpha')\, d\alpha' \Delta_E(\alpha') \tag{2.16}$$

If one now remembers that $Sp(Q_E)$ is $\int A_E(\alpha'')\, d\alpha''$ as remarked in S', one reaches the announced identity of (2.14) and (2.15) for either value of the double sign appearing in the former expression. Returning to (2.13) we see that the long time limit of $\langle \bar{B}\rangle_t$ agrees with the equilibrium value

$$\langle B\rangle_{eq} = \int \langle B\rangle_E p_E dE \tag{2.17}$$

of the quantity B as deduced from microcanonical ensemble theory. The ergodic behaviour of our system is thereby established for all observable quantities B of the type described in section 1 and for initial states with incoherent phases. It may be noted that the main difference between the derivation just given and the treatment of diagonal quantities A in S and S' lies in the replacement of A by the diagonal operator $B_{ll'}$.

3. Discussion. We have been able to establish that under specified conditions an isolated many-body system approaches microcanonical equilibrium. This has been achieved in the quant11m description and we have made essential use of very special properties of the system in this

description. In the first place, our analysis is entirely based on the existence of a special orthonormal set of states α, composed of plane wave excitations. In this special representation the total hamiltonian is assumed to split into a diagonal part H and an off-diagonal part λV, and matrix elements of the form (2.1) are supposed to exhibit diagonal singularities with very definite properties. Secondly, we establish the approach to microcanonical equilibrium in a slightly unusual way. What we do is to study physical quantities represented by operators O with definite properties in the α-representation, and establish that their expectation value $\langle O\rangle_t$ tends in the course of time toward the equilibrium average value $\langle O\rangle_{eq}$ calculated from microcanonical theory. Finally our analysis follows the time evolution of the system for $t \to \pm\infty$ beginning with an initial state $\varphi_0 = \int \mid \alpha > d\alpha c(\alpha)$. We show that $\langle O\rangle_t$ splits into two terms, one depending on the $|c(\alpha)|^2$ only, and the second depending on the relative phases of $c(\alpha)$ for different α 's. We simply leave out the phase-dependent term on the ground that it will vanish for all times of practical interest if the initial amplitudes $c(\alpha)$ have incoherent phases.

Our result $\langle O\rangle_t \to \langle O\rangle_{\bar{c}\bar{q}}$ is established for the phase-independent part of $\langle O\rangle_t$. This result, being truly non-trivial and involving quite subtle properties of the diagonal singularities mentioned above, seems to us in itself to give additional support to the soundness of the incoherent phase assumption.

Obviously the systems we study are quite special, we use a special representation in expressing their properties and we discuss the approach to equilibrium for special operators O. All these special features, however, are realized in the most common physical examples of ergodic systems, solids, gases and liquids (although for the latter the large size of λV may make our treatment more doubtful). We feel therefore confident that despite its apparent lack of generality our method is quite well adapted to the difficult problem of establishing ergodicity for realistic systems. In fact it is only by complete exploitation of the special conditions assumed that we have been able to study our system in so much greater detail than is the case in the conventional investigations of the ergodic problem *) and to actually carry out a true proof of ergodic behaviour.

Although quantum-mechanical in nature, our analysis applies also to the physical situations one usually calls classical, i.e. when the values of all observable quantities of interest depend on Planck's constant only through negligibly small corrections. For such situations it is important to translate our results into the language of classical theory. The main point in this translation is that the state of the system at any time, although a single quantum state $\varphi_t = U_{t\varphi_0}$, must be described classically by an ensemble of points in $6N$-dimensional phase space (N being the number of particles). This cannot be otherwise, because the quantum-mechanical wave function corresponding to a single point in classical phase space is a very special type of wave packet and cannot possess the incoherent phases we require φ_t to have for $t = 0$ in our analysis**). This correspondence between single quantum states and classical ensembles leads to certain consequences which we now want to describe.

According to our theory, for sufficiently large times t the expectation value $\langle O\rangle_t$ of a physical quantity O becomes equal to the equilibrium value $\langle O\rangle_{\mathrm{eq}}$. This holds equally well for the quantity O^2,

$$\left\langle O^2\right\rangle_t = \left\langle O^2\right\rangle_{v\tilde{q}} \text{ for large } t$$

In general, of course, $\langle O^2\rangle_{eq}$ and $\langle O\rangle_{eq}{}^2$ are different, so that for large t the quantities $\langle O^2\rangle_t$ and $\langle O\rangle_t{}^2$ will be both constant in time and have different values, a fact which makes it quite clear that the classical analogue to the

[8]*) The unsatisfactory nature of Von Neumann's approach [2]) to the quantum ergodic problem has now been clearly revealed [3]). It stems from the fact that Von Neumann's form of ergodic property actually imposes no restriction at all on the dynamical system.

single quantum state φ_t of our system has to be an enscmble. If now measurements of O are made on one and the same system at various times, the measured values q_t will show a time dependence even for large t and, in classical situations (as defined above), the time averages of q_t and $(q_t)^2$ must be equal to $\langle O\rangle_t$ and $\langle O^2\rangle_i$ respectively, because the measuring process then cannot affect the observable properties of the system.

In our theory, a measurement of O at time t must be described in the conventional quantum-mechanical fashion as giving rise to a reduction of the state vector φ_t to another vector $\varphi_t{}'$. This interpretation holds always, even in classical situations. For the latter case we can translate it by saying that the measurement gives rise to a reduction of the classical ensembe assuciated with $\bar{\varphi}t$ to the smaller ensemble associated with $\bar{\varphi}_i'$. Although there is nothing wrong with this description, it differs in a non-trivial way from the picture conventionally adopted for a classical many-body system, in which at every instant t the system is regarded as being in one single point of $6N$-dimensional phase space. If our theory is valid, a gas, liquid or solid in thermal equilibrium can never be said to be in one single point of its classical phase space, even at high temperatures where all measurable quantum effects are numerically negligible. It is in a single quantum state, the classical analogue of which is an ensemble.

It should be stressed that this unorthodox view cannot lead to any observable discrepancy with the conventional picture of a classical system. Let us verify for example in our quantum description that for a classical situation (as defined above) a measurement carried out at time t does not affect the result of observations at later times $t' = t + \tau$. Let the quantity U be measured at time i, and the quantity O' at time t'. Assuming for simplicity O to have discrete eigenvalue O_n, all we have to establish is the identity

$$\langle\varphi_t|\, U_{-\tau}O'U_\tau O\,|\varphi_t\rangle = \sum_n O_n\,\langle\varphi_t|\, P_nU_{-\tau}O'U_\tau P_n\,|\varphi_t\rangle \tag{3.1}$$

where the P_n 's are the projection operators verifying $O = \sum_n O_nP_n$. The righthand side of (3.1) includes the reduction of the state vector due to the first measurement, the lefthand side neglects it. Since ${P_n}^2 = P_n$ the difference between the two is

$$\Sigma_n O_n\,\langle\varphi_t|\,[P_n, U_{-\tau}O'U_\tau]\,P_n\,|\varphi_t\rangle\,.$$

The commutator being proportional to h, this difference is indeed negligible in a classical situation.

4. Refutation of Ingraham's criticism. In a recent paper [6]) Ingraham has presented a severely critical discussion of our derivation in S of the master equation describing the approach to equilibrium in the case of a very small perturbation (limiting case $\lambda \to 0.i \to \infty, \lambda^2 t$ finite). In fact, if

this discussion were correct, it would imply complete invalidity of the cortents of S, S' and the present paper. Ingraham's analysis, however, is based on a tew patently wrong assertions and arguments. If these assertions and arguments are replaced by their corrected versions, the whole criticism of Ingraham becomes groundless and his considerations reduce to those of S and lead to the same conclusions. We would like to devote the last section of the present paper to a refutation of Ingraham's criticism, to which end it will be sufficient to indicate which basic arguments of this author are incorrect. We can concentrate on section 3 of Ingraham's paper, which contains the actual discussion of our work.

The first argument of Ingraham is developed on pp. 107 to 111 of his paper. It tends to show that our method of calculation violates the unitarity of the operator of motion

$$U(t) = \exp[-i(H + \lambda V)t].$$

**) Starting from a different standpoint [4]) Van Kampen has been led some time ago to take the same view concerning the relation between classical and quantum statistics [5]).

The essential step is that unitarity of $U(t)$ would imply In(3.20)*), which itself entails In (3.22), i.e. the vanishing of all transition rates. The central error is In (3.20). In deriving this equation, Ingraham tacitly assumes that for $\lambda \to 0, t \to \infty, \lambda^2 t$ finite, the limit of a product of operators (in the case at hand ${U_2}^* U_2$) is equal to the product of the limits. This assumption is incorrect. Explicit calculation of the limit of the product gives an additional term in the righthand side of In (3.20), removing the inconsistency. Incidentally, while "deriving" In (3.20), Ingraham states that our use of a well known asymptotic formula, In (3.16), would result from a choice. This is patently wrong, because In (3.16) is a mathematical identity for $f(\varepsilon)$ continuously differentiable and vanishing at least as fast as $|\epsilon|^\nu, \nu < 0$ for $\epsilon \to \infty$. No other formula would be correct, and no choice can therefore be made.

The second criticism of Ingraham is that ambiguities exist in our calculations, because in products containing 3 or more factors V several prescriptions could be followed in replacing sub-products VAV by their diagonal parts: various choices could be made for these subproducts leading to different results for the total expression (see pp. 112 and 113 of Ingraham's paper). Ingraham has not understood that all choices have to be made, and that in the limit $\lambda \to 0, t \to \infty, \lambda^2 t$ finite, the total expression is the sum of the contributions of all possible choices. Among the latter only a few give non-vanishing contributions in the limiting case considered; all these have been calculated in S, ensuring the correctness of our results in the weak coupling limit.

Misled by the errors just mentioned, Ingraham concludes to the invalidity of the fundamental property on which our work is based, to know the occurrence of diagonal singularities, In (3.1) in his paper. His misunderstanding of this property becomes quite clear when he states it to be

equivalent to the property In (3.30), where no summation is carried out on the intermediate state q_1. The summation is absolutely essential for the occurrence of the diagonal singularity. Consequently the operator A in In (3. I) must have eigenvalues $A\,(E''\alpha'') - A''$ varying smo parameters F'', α'', and In (3.30) is incorrect. For the master equation established in S conerns the probabil same reason, the our large system in unperturbed find a very large number of neighboriates, i.e. the probability averaged over bility distribution. Therefore-grained probaobtain irreversible effectement that we "want to permitted by statistical while retaining the maximum information the very motivation mechanics" (p. 101), according to his introduction native diagonal of his critical study, is incorrect. Concerning the altersufficient to property In (3.33) proposed by Ingraham, it will be on the exas that it does not hold for actual systems, as is easily verified of S'.

Having thus concluded to the invalidity of Ingraham's criticism, we may finally remark that this author seems to be quite confused concerning the order in which the various limiting processes $N \to \infty, \lambda \to 0, t \to \infty$ must be considered for obtaining the region of validity of a master or transport equation. The number of particles N must go to infinity first, λ and t being finite. When this limiting process, which is necessary e.g. to eliminate surface and shape-dependent effects, is completed, one can consider the limiting case $\lambda \to 0, t \to \infty, \lambda^2 t$ finite. One then obtains the master equation as derived in S. One can treat also, however, the case of finite λ and t, as was done in S' and the present paper.

Received 7-1-59

References

1. Van Hove, L., Physica 21 (1955) 517 and 23 (1957) 441.

2. Von Neumann, J., Z. Phys. 57 (1929) 30; Pauli, W. and Fierz, M., Z. Phys. 106 (1937) 572. 3) Fierz, M., Helv. Phys. Acta, 28 (1955) 705; Farquhar, I. E. and Landsberg, P. T., Proc. ro. Soc. A239 (1957) 134; Bocchieri, P. and Loinger, A., Phys Rev. 111 (1958)

668. Van Kampen, N. G., Physica 20 (1954) 603.

3. Van Kampen, N. G., Proc. Int. Symposium on Transport Processes in Statistical Mechanics (Brussels, Aug. 1956), Interscience, New York and London (1958) p. 239. ngraam, R., Nuvvo Cimento 3 (1958) 92.

28.5 V.4 Quantum Theory of Measurement and Ergodicity Conditions

Abstract: Some criticisms to von Neumann's treatment of the measuring process are recalled and discussed.
The problem is reconsidered and reinvestigated, in the spirit of the "philosophy" of Jordan and Ludwig, on the basis of an ergodic theorem recently given.
The measuring apparatus is schematized as a macroscopic system which possesses, besides the energy, at least another macroscopic constant of the motion. The value of this constant characenergy, an invariant manifold ("channel"). In each manifold certain ergodicity conditions hold and there exists an equilibrium macro-state towards which the system evolves spontaneously. Tic afppatatus is assumed to be initially in the equilibrium state belonging to a given channel and the interaction with the observed system determines a transition of the apparatus towards a siate belonging to another channel, which depends on the initial state of the observed system. Then the apparatus evolves towards a new equilibrium state.

The ergodicity conditions employed are sufficiently realistic, since it has been proved that they are in particular satisfied by that class of Hamiltonians for which Van Hove succeeded in deriving a master equation.

28.5.1 1. Introduction

As is well known, the measuring process plays a central role in quantum mechanics. Its formal mathematical theory was developed by von Neumann [1]) in 1932. In recent years von Neumann's point of view and results have been criticized under different aspects by many authors (Jordan [2]), Bohm [3]), Wigner, Araki and Yanase [4]), Ludwig [5]), Feyerabend [6]), H. S. Green [7]), Durand [8]), Wakita [9])). Various attempts have been made (see refs. [4,5,7–10])) to obtain a more satisfactory soiution of the problem than that of von Neumann. In our opinion, the treatment given by Ludwig [5,10]) is the most complete and satisfactory from a physical point of view. However, its mathematical elaboration is still in a preliminary stage.

Originally published in Nuclear Physics, 33, 297-319 (1962).

In the present article, following essentially Jordan and Ludwig's "philosophy" †, we give a treatment of the measuring process based on a recent formulation of the ergodic problem [11,12]). In the course of our exposition we shall also re-examine some points of Ludwig's work, which, in our opinion, deserve a more detailed analysis.

An idea of the point of view adopted can be given in the following terms.
Performing an observation on a microscopic system amounts to putting the system itself in interaction with another large system, which has the property of undergoing, as a result of the interaction, macroscopic modifications which are dependent on the state of the micro-system.

If we assume that an objective meaning can be attributed to the macro-states of a large system, the aim of quantum mechanics is then essentially to make predictions on the trace that our microscopic body will leave in the macroscopic world, when the trace left at a certain time is known. In this line of thought, the measuring process has to be considered - rather than as an "untrennbare Kette zwischen Objekt und Subjekt" (Weizscker [13])) - as an "untrennbare Kette zwischen Mikro- und Makrokosmos" (Ludwig).

In order that an objective meaning may be attributed to the macro-states of the large bodies, it is of course necessary that - by virtue of the laws of quantum mechanics and of the structure of the macroscopic bodies - states incompatible with the macroscopic observations be actually impossible. In our opinion, this impossibility should be a consequence of the fact that the result of the interaction of two macrosystems must always be macroscopically determined.

After these premisses it is clear that, in order to build up a satisfactory quantum theory of measurement, it is necessary to have a theory, at least schematic, of the large bodies, i.e. a theory which gives the connection between the macroproperties of these bodies and their microscopic structure described by quantum mechanics.

We notice that in the measuring process the energy of the apparatus is enormously larger than the energy of the micro-object, which should suffer, during the measuring process, the least possible perturbation. Therefore the apparatus must be a macrosystem in a thermodynamically metastable state, such that a very small perturbation makes it evolve towards a thermo-dynamically stable state, dependent on the state of the micro-object.

It is therefore clear that the measuring process is closely connected with the problem of the evolution of a large body towards its state of thermodynamic equilibrium and, consequently, with the ergodic problem.

28.5.2 2. Macro-states of the Measuring Apparatus

It follows from the preceding considerations that a measuring apparatus must be a macroscopic system possessing many states of macroscopic equilibrium compatible with a given value of the macroscopic energy. A system of this kind possesses, besides the energy, other macroscopic constants of the motion. We characterize schematically the macroscopic state of this system in a way analogous to that followed in ref. [12]).

We introduce a suitable basis $\{\Omega_{akvi}\}$ of vectors and assume that the manifolds $\mathbf{C}_{akv}$ spanned by the Ω_{akvi} corresponding to given sets of values for a, k, v represent the macro-states of the system. The indices a and k denote, respectively, the value of the macro-energy and the set of values of the other macroscopic constants of the motion which are relative to the macroscopic state considered. These quantities do not change during the free evolution of the system. The index v denotes the value of the macrovariables which do change during the time evolution. We denote by $\mathbf{C}_{ak}$ the manifold ("channel") spanned by the vectors Ω_{akvi} corresponding to given values of a and k. We assume that within the manifold $\mathbf{C}_{ak}$ ergodicity conditions are verified, analogous to those formulated for the whole energy shell in refs. [12]); we assume further that for given a and k there exists a manifold $\mathbf{C}_{ake_k}$ having a number of dimensions much larger than that of the other manifolds $\mathbf{C}_{akv}$ $(v \neq e_k)$. If the system is initially in a state belonging to the channel $\mathbf{C}_{ak}$, it then evolves spontaneously towards the state $\mathbf{C}_{ak_k}$. The manifolds $\mathbf{C}_{\text{ake }k}$ represent the various states of macroscopic equilibrium.

Let the measuring apparatus be initially in the equilibrium state $\mathbf{C}_{a0_0}$ of a given channcl $\mathbf{C}_{a0}$ and suppose that the interaction of the object system with the apparatus induces a transition of the state of the latter from the channel $\mathbf{C}_{a0}$ to another channel $\mathbf{C}_{ak}$ of the same energy shell,

[8†] As will appear presently, this "philosophy" and, consequently, any technical development founded on it are in harmony with the ideas of Bohr. More exactly, as Prof. Rosenfeld has kindly pointed out to us, the situation is the following: "Bohr's epistemological analysis, which is complete in itself, disposes of von Neumann's infinite regress" (cf. sects. 3 and 4) "by appealing to the logical necessity of making a sharp distinction between object and measuring instrument. No formal treatment can replace Bohr's argument, for the simple reason that the physical meaning of any mathematical elaboration can only be expressed by means of the classical concepts to which Bohr appeals directly, and which are (in the last resort) not formalizable, but immediately given (as part of common experience)." The significance of our treatment (and of the treatment of Ludwig) is rather to establish rigorously the logical consistency of the way in which the mathematical formalism is connected with he unanalyzed basic concepts.

depending upon the particular state of the object system. At the end of the measuring process the apparatus is in a final equilibrium macrostate $\mathbf{C}_{\text{akek}}$.

28.5.3 3. Basic Assumptions of Quantum Theory

We recall very briefly the assumptions on which quantum theory is founded.
(i) The physical state of a system is represented by a vector (properly by a ray) of a Hilbert space.
(ii) The time evolution of a state is governed, in the Schrödinger picture, by the Schrödinger equation

$$\psi_t = T(t)\psi_0, \quad i\hbar\frac{\mathrm{d}T}{\mathrm{d}t} = HT, \quad T(0) = 1 \tag{3.1}$$

(iii) An observable A is represented by a Hermitian hypermaximal operator α. The eigenvalues a_r of α give the possible † values of A. An eigenvector $\phi_r^{(s)}$ corresponding to the eigenvalue a_r represents a state in which A has the value a_r. If the system is in the state ψ, the probability p_r of finding the value a_r for A, when a measurement is performed, is given by

$$p_r = (\psi, P_{v_r}\psi) = \sum_s \left|\left(\phi_r^{(s)}, \psi\right)\right|^2 \tag{3.2}$$

where $P_{\mathbf{v}_r}$ is the projection operator on the eigenmanifold $\mathbf{V}_r$ corresponding to a_r, and the sum $\sum_s$ is taken over a complete orthonormal set $\left\{\phi_r^{(s)}\right\}$ $(s = 1, 2, \ldots)$ of $\mathbf{V}_r$.
(iv) Let us suppose we have performed a measurement of a quantity A and that this measurement is a maximal one. If the result is a_r, we postulate that the state of the system immediately after the observation is described by the (unique) eigenvector ϕ_r, corresponding to the eigenvalue a_r. If the measurement of A is not a maximal one - i.e. if the spectrum of α is degenerate - it is commonly assumed (cf. e.g. ref. [14])) that the state after the measurement is

$$N^{-1}\sum_s \left(\phi_r^{(s)}, \psi\right)\phi_r^{(s)} \tag{3.3}$$

where $N^2 \equiv \sum_s \left|\left(\phi_r^{(s)}, \psi\right)\right|^2$ is a normalization factor. This assumption, however, as it could be derived from what follows, implies a hypothesis on the measuring apparatus which cannot always be considered to be verified. As is well known, the preceding assumptions may be formulated also in the language of the statistical (density) operators. In this way, we have in particular the advantage of obtaining formulae which are valid not only for the pure cases, but also for the mixtures. The statistical operator W of a system changes in time according to the equation (Schrödinger picture)

$$W(t) = T(t)W(0)T^*(t) \tag{3.4}$$

The probability p_r of finding the result a_r for the observable A is

$$p_r = \mathrm{Tr}\left(P_{\mathbf{v}_r}W\right) \tag{3.5}$$

[8†] We suppose here that the spectrum of α is discrete. We recall that it is physically impossible to measure with absolute accuracy an observable C having a continuous spectrum. However, it is possible to measure such an observable with an arbitrarily good accuracy. It is in fact sufficient to choose a step function $F(x)$ - which approximates the function x with the wanted accuracy - and measure $F(C)$, which is an observable with a discrete spectrum. Notice that the introduction of $F(C)$ is not a mathematical trick but is essential for reasons of principle.

and the statistical operator of the system for which the eigenvalue a_r has been found, is

$$\frac{P_{\mathbf{v}_r} W P_{\mathbf{v}_r}}{\mathrm{Tr}\,(P_{\mathbf{v}_r} W)}. \tag{3.6}$$

28.5.4 4. Consequences of the Preceding Assumptions

Let A and B be two observables, whose operators are respectively α and β. Let us suppose that the spectra of α and β are discrete and non-degenerate and that

$$\alpha\phi_r = a_r\phi_r; \quad \beta\chi_s = b_s\chi_s,$$

where ϕ_r and χ_s are normalized eigenvectors. If the (normalized) state vector at $t = 0$ is

$$\psi_0 = \sum_r c_r\phi_r \tag{4.1}$$

the probability of finding the value a_r of A, when a measurement of A is performed at $t = 0$, is, by virtue of postulate (iii),

$$p_{[A=a_r]}(0) = |c_r|^2$$

If the value a_r has been found, the probability of finding the value b_s of B at a later time t, is

$$p_{[B=b_s]}(t) = \left|\left(\chi_s, \exp\left[-\frac{i}{\hbar}Ht\right]\phi_r\right)\right|^2.$$

If we perform the measurement of A at $t = 0$ without "looking at" the result, the probability of finding at the time t the value b_s for B is evidently given by

$$\sum_r \left|\left(\chi_s, \exp\left[-\frac{i}{\hbar}Ht\right]\phi_r\right)\right|^2 |c_r|^2. \tag{4.2}$$

If no measurement is performed at $t = 0$, the above probability is

$$\begin{aligned}
&\left|\sum_r c_r\left(\chi_s, \exp\left[-\frac{i}{\hbar}Ht\right]\phi_r\right)\right|^2 \\
&= \sum_r |c_r|^2 \left|\left(\chi_s, \exp\left[-\frac{i}{\hbar}Ht\right]\phi_r\right)\right|^2 \\
&+ \sum_{r\neq r'} c_r^* c_{r'} \left(\chi_s, \exp\left[-\frac{i}{\hbar}Ht\right]\phi_r\right)^* \left(\chi_s, \exp\left[-\frac{i}{\hbar}Ht\right]\phi_{r'}\right).
\end{aligned} \tag{4.3}$$

The second term of the right-hand side of (4.3) is the so-called interference term; owing to its existence, we are not allowed to think that, when the system is in the state (4.1), the observable A has a value which is well determined even if it cannot be theoretically calculated (this assumption would furnish indeed an expression analogous to (4.2)). We may therefore assert that A has a given value only when it has been actually measured.

Considering that even the measuring apparatus is a physical system describable with the quantum laws, a first consistency problem of the theory consists in trying to prove that the apparatus acts on the object in such a way that the results of a later measurement are given by formula (4.2) rather than by formula (4.3).

28.5.5 5. Von Neumann's Theory of the Measuring Process

Let us denote by I and II the system we are considering and the apparatus for the measurement of A, respectively. Let the Hamiltonian of the total system I + II be

$$H = H_{\mathrm{I}} + H_{\mathrm{II}} + H_{\mathrm{int}}. \tag{5.1}$$

In order that II can actually act as an apparatus for the measurement of A, it is necessary that H_{int} be such that (a) I and II are coupled only during a very small time interval τ; (b) if I is in an eigenstate ϕ_r of α, at the end of the interaction a change depending on ϕ_r has taken place in the apparatus, while the state ϕ_r of I is practically not changed. More precisely, if II is initially in a state $\mathbf{\Phi_0}$ belonging to a manifold $\mathbf{V_0}$, we assume that H_{int} is such that

$$\exp\left[-\frac{i}{\hbar}H\tau\right]\phi_r\Phi_0 \approx \exp\left[-\frac{i}{\hbar}H_{\mathrm{int}}\tau\right]\phi_r\Phi_0 = \phi_r\Phi_r \tag{5.2}$$

where $\mathbf{\Phi_r}$ belongs to a manifold $\mathbf{V_r}$ and is dependent on the particular $\mathbf{\Phi_0}$ of $\mathbf{V_0}$. $\mathbf{V_0}, \mathbf{V_1}, \mathbf{V_2}, \ldots$ are supposed mutually orthogonal in order that the results of the measurement be distinct †.

The measurement of the quantity A of I is thus reduced to the measurement of a quantity $\mathscr{A}$ of II, which has as eigenmanifolds the orthogonal manifolds $\mathbf{V_0}, \mathbf{V_1}, \mathbf{V_2}, \ldots$ If $\mathbf{I}$ is at the time $t = 0$ in the state (4.1), one obtains by virtue of the linearity of the time evolution operator

$$\begin{aligned}\exp\left(-\frac{i}{\hbar}H_{\mathrm{int}}\tau\right)\psi_0\Phi_0 &= \exp\left(-\frac{i}{\hbar}H_{\mathrm{int}}\tau\right)\sum_r c_r\phi_r\Phi_0 \\ &= \sum_r c_r\phi_r\Phi_r\end{aligned} \tag{5.3}$$

- The probability of finding II in a state belonging to the manifold $\mathbf{V}_r$ is then equal to $|c_r|^2$, i.e. coincides with the probability given by the fundamental assumption (iii), when the measuring apparatus is considered as external to the studied system.

From eq. (5.3) it follows that the probability of finding at a time $t > \tau$ the system I + II in a state $\chi_s X_h$ (where the X_h 's are eigenstates of some observable of II) is

$$\begin{aligned}&\left|\left(\chi_s X_h, \exp\left[-\frac{i}{\hbar}\left(H_{\mathrm{I}} + H_{\mathrm{II}}\right)t\right]\sum_r c_r\phi_r\Phi_r\right)\right|^2 \\ &= \sum_r |c_r|^2\left|\left(\chi_s, \exp\left[-\frac{i}{\hbar}H_{\mathrm{I}}t\right]\phi_r\right)\right|^2\left|\left(X_h, \exp\left[-\frac{i}{\hbar}H_{\mathrm{II}}t\right]\Phi_r\right)\right|^2 \\ &\quad + \sum_{r\neq r'} c_r^* c_{r'}\left(\chi_s, \exp\left[-\frac{i}{\hbar}H_{\mathrm{I}}t\right]\phi_r\right)^*\left(\chi_s, \exp\left[-\frac{i}{\hbar}H_{\mathrm{I}}t\right]\phi_{r'}\right) \\ &\quad \cdot\left(X_h, \exp\left[-\frac{i}{\hbar}H_{\mathrm{II}}t\right]\Phi_r\right)^*\left(X_h, \exp\left[-\frac{i}{\hbar}H_{\mathrm{II}}t\right]\Phi_{r'}\right).\end{aligned} \tag{5.4}$$

Let us now suppose that the second measurement is performed on the system I only. The operator β, considered as an operator in the Hilbert space of I + II, is degene, ite and the eigenvectors belonging to an eigenvalue b_s are of the kind $\chi_s X_h$. Owing to postulate (iii) we must sum over the index h both sides of (5.4); since we have obviously

$$\sum_h \left(X_h, \exp\left[-\frac{i}{\hbar}H_{\rm II}t\right]\Phi_r\right)^* \left(X_h, \exp\left[-\frac{i}{\hbar}H_{\rm II}t\right]\Phi_{r'}\right) = (\Phi_r, \Phi_{r'}) = \delta_{rr'}$$

the probability of finding for B the value b_s, when no other measurement is performed on II, is

$$\sum_r |c_r|^2 \left|\left(\chi_s, \exp\left[-\frac{i}{\hbar}H_{\rm I}t\right]\phi_r\right)\right|^2. \tag{5.5}$$

This relation coincides with (4.2); the interaction with the measuring apparatus explains the replacement of (4.3) by (4.2).

The interference terms, which have been deleted from (4.3), reappear obviously in (5.4). In order to remove them, it would actually be necessary, according to von Neumann, to perform on the system II a measurement with another apparatus III. The system I + II would then be, with respect to III, in the same situation in which I was with respect to II. In particular, we have consistency between the results given by the theory for the two cases in which (a) I is considered as object and II + III as apparatus, (b) I + II is considered as object and III as apparatus. According to von Neumann, this is sufficient to prove the adequacy of the theory because in von Neumann's opinion any statement on the system II makes sense only when it corresponds to an actual observation made by means of III, any statement concerning III makes sense only when a further observation is performed on it by means of another system IV, and so on. In this chain of instruments we must include, according to von Neumann, besides the apparatus stricto sensu, also the sense organs with which the observer observes the apparatus, the nervous system sending to the brain the data of the sense organs, and so on. From the preceding considerations it follows that the point at which one makes the separation between observed system and observer (Heisenberg's "Schnitt") does not matter; in other words, we can put the "boundary" between system and apparatus or between apparatus and sense organs or between sensc organs and nervous system, and so on. This is the so-called principle of the psycho-physical parallelism. In this line of thought the transition from one state to another, and consequently the passage from (4.3) to (4.2) would be determined, in the last analysis, by the "abstract ego" becoming conscious of the result.

28.5.6 6. Criticism of Von Neumann's Point of View

6.1. SUBJECTIVISM

It is clear that von Neumann's theory is founded on a radically subjectivistic (solipsistic) philosophy. From an objectivistic point of view, the difference between (4.3) and (5.3) ought to be explained by taking explicitly into account the fact that the aim of quantum mechanics is to describe the behaviour of the micro-objects only through their relations with the macroscopic world. But it is then necessary, for obvious consistency reasons, to construct a quantum theory of the large bodies, which explains the objective nature of their macroscopic properties and the changes induced by the micro-objects on the macro-properties of the measuring apparatus.

[8†] Note that from a purely mathematical point of view, it is always possible to find a unitary operator $T(\tau)$ satisfying the relation

$$T(\tau)\phi_r\Phi_0 = \phi_r\Phi_r$$

In order that T be unitary it is in fact necessary (and sufficient) that it transforms the vectors forming with the $\phi_r\Phi_0$ a complete orthonormal basis of the Hilbert space of $\mathbf{I}+\mathbf{II}$, into vectors orthogonal to each other and to the vectors of the manifold spanned by the $\phi_r\Phi_r$. Now, this is possible in an infinite number of ways. From a physical point of view this result is not significant since the problem consists in ascertaining whether there actually exists in nature a measuring apparatus such that the Hamiltonian $H_{\rm int}$ satisfies the above relation.

6.2. INFINITE REGRESS

It is commonly assumed that to any observable there corresponds a given Hermitian operator. However, a real physical meaning can only be given to this mathematical
symbol when the procedure by which the quantity studied is measured, is defined at least conceptually. According to von Neumann's theory of measurement, the meaning of a quantity of a given system I is given by the modifications produced by I on some quantity of the system II. The meaning of the latter quantity is given by the modifications determined by II on some quantity of a system III, and so on. Evidently, if von Neumann's chain is never truncated, the physical meaning of an abstract observable of the system I is referred to that of some observable of the system II, he meaning of this abservable of II is referred to the meaning of some observable of III and so on indefinitely, the meaning in question being never attained. If, in line with the considerations of subsect. 6.1, we could give an objective character to the macroscopic states of a large system and consider its macro-observables as the quantities to which a meaning is given from the very beginning, a meaning could be given to any other abstract observable by defining the procedure with which it can be measured. This procedure is uniquely defined once the macro-states of a large system have been defined and the nature of the forces between the systems is known.

6.3. WIGNER'S OBJECTION

An objection of a more particular nature to von Neumann's theory was presented by Wigner [4]). He proved that, if the state of the system object + apparatus is described at the end of the measurement by eq. (5.3), results which are in contradiction with conservation principles can be obtained. A way out, however, was found by Wigner himself, who demonstrated that if one takes properly into account the macroscopic nature of the measuring apparatus the difficulty can be overcome.

Wigner considered the following example. Let I be a system describable only with spin variables; let σ_x be the observable to be measured. We shall denote by $\phi_{\sigma' x}$ and $\phi_{\sigma'' x}$ the eigenstates of σ_x corresponding to the eigenvalues +1 and -1 respectively. If we put ψ_0 equal to $\phi_{\sigma' x}$ or $\phi_{\sigma'' x}$ we get from eq. (5.2)

$$\exp\left(-\frac{i}{\hbar}H\tau\right)\phi_{\sigma' x}\Phi_0 = \phi_{\sigma' x}\Phi', \tag{6.1}$$
$$\exp\left(-\frac{i}{\hbar}H\tau\right)\phi_{\sigma'' x}\Phi_0 = \phi_{\sigma'' x}\Phi''.$$

Let us now consider a conservative observable of the total system I + II, not compatible with σ_x : for instance the component M_z of the angular momentum of $\mathrm{I}+\mathrm{II}$. We have

$$M_z = L_z + \sigma_z,$$

where L_z acts in the Hilbert space of II. It is well known that a representation can be chosen in such a way that the eigenstates of σ_x be written as linear combinations of the eigenstates of σ_z, in the following way:

$$\phi_{\sigma' x} = \frac{1}{\sqrt{2}}\left(\phi_{\sigma' x} + \phi_{\sigma'' z}\right), \quad \phi_{\sigma'' x} = \frac{1}{\sqrt{2}}\left(\phi_{\sigma' x} - \phi_{\pi'' -}\right).$$

where $\phi_{\sigma' z}$ and $\phi_{\sigma'' z}$ are normalized vectors. Adding and subtracting the equations obtained by substituting the above expressions into eqs. (6.1), we get

$$2\exp\left(-\frac{i}{h}H_{\text{int}}\tau\right)\phi_{\sigma_z}\Phi_0 = \phi_{\sigma_z}(\Phi' + \Phi'') + \phi_{\sigma''_z}(\Phi' - \Phi'') \tag{6.2}$$
$$2\exp\left(--\frac{i}{h}H_{\text{int}}\tau\right)\phi_{\sigma''_z}\Phi_0 = \phi_{\sigma'_z}(\Phi' - \Phi'') + \phi_{\sigma''_z}(\Phi' + \Phi'')$$

We now observe that the expectation values of M_z corresponding to the states described by the right-hand sides of eqs. (6.2) are the same, while the expectation values corresponding to $\phi_{\sigma' z}\Phi_0$ and to $\phi_{\sigma'' z}\Phi_0$ differ by $2\hbar$. Therefore in this case eq. (5.2) is in contradiction with the conservation theorem of angular momentum. Wigner however showed that the difficulty can be overcome if eqs. (6.1) are replaced by the following:

$$\exp\left(-\frac{i}{\hbar}H\tau\right)\phi_{\sigma' x}\Phi_0 = \phi_{\sigma' x}\Phi' + \phi_{\sigma'' x}\Theta \tag{6.3}$$
$$\exp\left(-\frac{i}{\hbar}H\tau\right)\phi_{\sigma'' x}\Phi_0 = \phi_{\sigma'' x}\Phi'' - \phi_{\sigma' x}\Theta$$

where $(\Phi', \Theta) = 0 = (\Phi'', \Theta)$, and $\|\Theta\|$ can be supposed to be very small if the states Φ_0, Φ', Φ'' are superpositions of many states corresponding to different eigenvalues of L_z. This fact can be considered as actually occurring since Φ_0, Φ', Φ'' correspond to macroscopic states of the apparatus. We have a similar situation for any observable of the system I not compatible with a conservative observable of the total system I + II (Araki and Yanase [4])).

28.5.7 7. Hints for an Objectivistic Interpretation of the Measuring Process

As emphasized in the preceding section, a satisfactory theory of the measuring process must start from a characterization of the macroscopic properties of a large body. Such properties must have an objective character; it is therefore necessary that no interference terms appear in the relations concerning them. Such terms must be absent essentially by virtue of the complexity of the considered system.

In particular, it must be allowed to truncate von Neumann's chain immediately after the first macroscopic system $S^{(i)}$. The interference terms must disappear owing to the nature of the macroscopic observations and to the properties of the Hamiltonian of the system $S^{(1)} + S^{(2)} + \ldots + S^{(i)}$. A first hint for a way out may be obtained from the following rough considerations.

Let us suppose for the sake of simplicity, as it is almost always the case in practice, that the system II is already macroscopic and consider the manifolds $\mathbf{V}_0, \mathbf{V}_1, \ldots \mathbf{V}_r, \ldots$ of II as corresponding to the macroscopic properties. Observe now that in order that the measurement may be performed it is necessary that the changes undergone by the system II owing to its coupling with I persist for a sufficiently long time;
we shall suppose therefore that the above manifolds are invariant with respect to the operator $\exp[-(i/\hbar)H_{\text{II}}\,t]$, i.e. that for any t

$$\exp\left(-\frac{i}{\hbar}H_{11}t\right)\Phi_r \in \mathbf{V}_r$$

and that transitions from one manifold to another occur only by virtue of the interaction with I. Any macroscopic observation on the system II consists then in determining the manifold $\mathbf{V}_r$ to which the state vector belongs. Any observation compatible with the macroscopic observation

determines a set of manifolds which may be spanned by vectors $X_h (h = 1, 2, \ldots)$ every one of which belongs to a single manifold $\mathbf{V}_r$.

In (5.4) only one of the expressions ($X_h, \exp[-(i/\hbar)H_{\mathrm{II}}t]\,\Phi_r$) is different from zero, say that containing Φ_n; eq. (5.4) therefore becomes

$$|c_n|^2 \left| \left(\chi_s, \exp\left[-\frac{i}{\hbar} H_1 t \right] \phi_n \right) \right|^2 \left| \left(X_h, \exp\left[-\frac{i}{\hbar} H_{\mathrm{II}} t \right] \Phi_n \right) \right|^2 . \tag{7.1}$$

Eq. (7.1) is a relation of the kind (4.2) and is in accordance with the objective character attributed to the macroscopic properties of the system II.

If the considered observation on II is not only compatible with a macroscopic observation, but is itself a macroscopic observation, we must sum in (7.1) over all the states X_h which belong to $\mathbf{V}_n$. We obtain in this way

$$|c_n|^2 \left| \left(\chi_s, \exp\left[-\frac{i}{\hbar} H_{\mathrm{I}} t \right] \phi_n \right) \right|^2 \tag{7.2}$$

this expression is obviously in agreement with (4.2).

The present schematization of the macro-observations and of the measuring apparatus is too rough and will be re-examined in the following; the essential elements to the solution of the measurement problem are, however, already contained in it. The success of this viewpoint rests of course on the fact that the observations which can be actually performed on the system II must be compatible with the macroscopic ones. In other words, it would be impossible to construct an instrument capable of measuring a quantity such that its eigenstates X_h have projections different from zero on distinct manifolds $\mathbf{V}_r$.

From a mathematical point of view it is of course always possible to find a unitary operator $\exp[-(i/\hbar)H_{\mathrm{int}}\,\tau]$ corresponding to such a measurement performed on II. From the point of view of physics, however, H_{int} is not arbitrary, but depends upon the nature of the systems; therefore it is likely that the above possibility does not exist. The plausibility of the assumption will be discussed in the following (sect. 5).

28.5.8 8. Analysis of the Physical Characteristics of Some Typical Measuring Apparatus

Let us first suppose that we want to measure the energy of a charged particle with a proportional counter.

The counter is assumed to be initially charged to a given potential; we may assume that there is thermal equilibrium within the gas of the counter, electrostatic and thermal equilibrium within the electrodes. When a charged particle goes through the counter, a practically determined number of ions is produced, which is a function of the particle velocity and consequently, for a given mass, of its energy.

Under the influence of the electric field the electrons migrate. Since the wire is at a positive potential, the electrons go towards it. The gas pressure and the potential are fixed in such a way that in a very small region around the central wire, where the field is stronger, the energy gained by the electron in covering a distance equal to the mean free path is larger than the ionization energy of the gas molecules. In this region secondary ions are created at a rate such that the ratio of their number to the number of initially produced ions is practically constant. When the electrons reach the wire, the electronic instruments connected to the counter record a sudden reduction of the potential, proportional to the number of ions originally created by our particle and therefore a function of its energy. In order to avoid unessential complications, we omit considering the electronic instruments and suppose the counter to be connected to

the electrodes of a capacitor. (This is certainly correct for the time intervals of the order of the discharge time.) Then, if there was initially a given voltage between the electrodes of the condenser, and consequently between the electrodes of the counter, after the discharge this voltage decreases and the decrease is a function of the energy of the particle that crossed the counter.

We may distinguish the following phases:
(a) The apparatus is initially in a macroscopic state of metastable equilibrium in which it remains practically for an indefinite time, if no external perturbation intervenes. (Strictly speaking, it is of coursc possible that some ions are produced by thermal fluctuations inside the gas and it is consequently possible that the apparatus discharges spontaneously; however the interval of time needed for a spontaneous discharge is much larger than that during which a discharge induced by the passage of a particle may occur.)
(b) The particle goes through the counter; if its energy is practically determined, the number of ions generated is practically determined. The passage of the particle removes the system from the state of metastable equilibrium and brings it into a state which can already be considered as macroscopic (and characterized by the number of the generated ions and by the voltage between the electrodes); this state is no longer a state of equilibrium and depends essentially on the particle energy.
(c) The apparatus goes spontaneously towards a new equilibrium situation (no ions present, a smaller voltage between the electrodes), which depends on the state corresponding to phase (b) (on the number of the generated ions) and therefore on the energy of the particle.
One gets easily convinced that all the processes that occur in the ordinary measuring apparatus are reducible to the above scheme. Examples: the formation of a trace in a Wilson chamber, in a bubbie chamber, in a photographic emulsion.

In order to clarify the question further, we analyze another measuring apparatus. Consider first a Geiger counter. As is well known, it differs from the proportional counter because the potential and the gas pressure are fixed in such a way that the ion multiplication spreads along all the wire; consequently the production even
of a small number of ions induces a discharge which is self-sustaining if the voltage does not decrease.

In the apparatus actually employed in practice there is a resistor in series with the counter, or the discharge is interrupted at a given time by some suitable trick. The pulse-height given by the Geiger counter is independent of the number of ions primarily created and therefore of the energy of the incident particle. In our simplified apparatus the passage of a particle through the counter induces a discharge, at the end of which the voltage falls practically to zero. The counter is a "yes or no" apparatus: the particle has passed through, the particle has not passed through.

Let us suppose that a beam of practically monokinetic particles impinges on some target T and let us study the angular distribution of the scattered particles by means of a set of counters. If the particle is scattered within the angle (θ'_k, θ''_k) under which the k-th counter is viewed from T (i.e. if the particle is represented by a wave-packet with propagation vectors within this angle), it produces a given number of ions inside the k-th counter; the k-th counter then discharges while the remaining counters stay unaltered. Here the initial metastable state is the state in which all the counters are charged, the intermediate state (depending on the direction in which the particle is scattered) is the state in which ions are created inside the k-th counter, the final state (also depending on the direction of scattering) is a state in which the k-th counter has been triggered while the other counters undergo no change.

28.5.9 9. Outline of a Theory of the Macroscopic Bodies

It is now evident that if we want to build up a theory of the measuring apparatus, we must first of all construct a theory of the macroscopic bodies and give a solution to the problem of the time evolution of a macroscopic body towards its thermodynamic equilibrium state, i.e. give a solution to the crgodic problem.

To this end, we shall recall briefly the characterization of the macroscopic states of large bodies given by statistical mechanics.

Obviously the macroscopic obscrvations performed on a large body cannot define completely its quantal state. In order to characterize formally the macro-observations, one decomposes suitably the state space of the body into a given number of orthogonal manifolds having a very large number of dimensions. The various possible macrostates correspond to these manifolds.

A first interesting quantity is the energy; it is measured macroscopically with a certain inaccuracy. Let us subdivide the set of the possible energy values into intervals ($E_a, E_{a+1} = E_a + \Delta E$) and denote by $\mathbf{C}_a$ the manifold of the eigenvectors, corresponding to the a-th energy interval. Since a macroscopic body is a system spatially bounded, its energy spectrum is a purely discrete one. Let us indicate by S_a the number of dimensions of the manifold $\mathbf{C}_a$. Let us suppose that there exists another macroscopic constant of the motion J, or, more generally, a set of such constants. (Consider, e.g., a system composed of two non-intcracting parts, each of which possesses its own energy. In this case the constants of the motion are the total energy and the energy of one of the subsystems.) The spectrum of J can also be decomposed into intervals (J_k, J_{k+1}) and consequently each manifold $\mathbf{C}_a$ can be decomposed into a set of orthogonal manifoids
$\mathbf{C}_{ak}$, which are spanned by the eigenvectors of J belonging to $\mathbf{C}_a$ and to the eigenvalues of (J_k, J_{k+1}). We call $\mathbf{C}_{ak}$ the $\dot{k}$-th channel of $\mathbf{C}_a$ and denote by S_{ak} its number of dimensions.

In order to define completely the macroscopic state of the body it is necessary to take account also of other quantities. We represent mathematically this situation by decomposing the manifolds $\mathbf{C}_{ak}$ into submanifolds $\mathbf{C}_{akv}$ $(v = 1, 2, \ldots, N_{ak})$. Let $\{\Omega_{akvi}\}$ $(i = 1, 2, \ldots, s_{akv})$ be a basis adapted to the cells $\mathbf{C}_{akv}$.

We omit a detailed discussion of the characterization of the cells $\mathbf{C}_{akv}$, since it would require more precise assumptions on the nature of the system considered. By way of example, we recall here how the manifolds $\mathbf{C}_{akv}$ are defined for an ideal gas or solid.

In a gas one may take as basis $\{\Omega_{akvi}\}$ the set of eigenstates of the unperturbed energy, i.e. the states composed of direct products, suitably symmetrized, of the single particle states. The energy shell $\mathbf{C}_a$ is the manifold spanned by the set of the unperturbed eigenstates corresponding to a given interval of unperturbed energy; in fact, if this interval is sufficiently large, the above manifold coincides practically with the manifold spanned by the corresponding perturbed energy states. The cells $\mathbf{C}_{akv}$ are defined in the following way. One subdivides the single particle energy spectrum into intervals ($\varepsilon_r, \varepsilon_r + \Delta E/n$) where n is the number of molecules contained in the gas. The number of molecules whose energy lies in the r-th interval, when the system is in a given unperturbed eigenstate, is then denoted by n_r. The energy shell $\mathbf{C}_a$ is the manifold spanned by the set of vectors corresponding to given values of the numbers $n_1, n_2, \ldots$.

In the case of a non-conducting solid, we may take a basis formed by the eigenstates of the phonon unperturbed energy and repeat for the phonon gas the above treatment, taking into account that now the total number of phonons is also allowed to change and must be considered as a dynamical variable.

In the case of a conducting solid, one must characterize analogously, besides the state of the phonon gas, the state of the conducting electron gas.

This characterization of the macro-state of a gas or of a solid suffices to account for several macroscopic properties of the system. For a somewhat more complete characterization, it is necessary to know also the spatial distributions of the particles. To this end it would be sufficient

to repeat the preceding arguments taking in lieu of the above single particle states, which correspond to a complete indeterminacy of the particle positions, a set of states corresponding to given position and momentum indeterminacies †.

Going back to the general case, let us refer to a fixed energy shell, dropping accordingly the index a.

We suppose that the Hamiltonian H_{II} of the macro-system and the basis $\{\Omega_{kvi}\}$ are such that the following ergodicity conditions are satisfied [12]):

$$\mathbf{M}\left\{\sum_{i=1}^{s_{kv}}\left|\left(\Omega_{kvi},\exp\left[-\frac{i}{h}H_{\mathrm{II}}t\right]\Omega_{k\mu j}\right)\right|^2\right\}-\sum_{\rho}\sum_{i}|(\Omega_{kvi},T_\rho\Omega_{k\mu j})|^2\approx\frac{s_{kv}}{S_k} \tag{9.1}$$

$$\left|\mathbf{M}\left\{\sum_{i=1}^{s_{kv}}\left|\left(\Omega_{kvi},\exp\left[-\frac{i}{\hbar}H_{\mathrm{II}}t\right]\Omega_{k\mu j}\right)^*\left(\Omega_{kvi},\exp\left[-\frac{i}{\hbar}H_{11}t\right]\Omega_{k\mu' j'}\right)\right\}\right|$$

$$=\left|\sum_{\rho}\sum_{i}\left(\Omega_{kvi},P_\rho\Omega_{k\mu j}\right)^*\left(\Omega_{kvi},P_\rho\Omega_{k\mu' j'}\right)\right|<\frac{s_{kv}}{S_k}\,(\mu\neq\mu')$$

where $\sum_\rho E_\rho P_\rho$ is the spectral representation of H_{II} and $\mathbf{M}$ denotes the operation of time averaging

$$\lim_{T\to\infty}\frac{1}{T}\int_0^T \mathrm{d}t\ldots$$

Let us suppose that the initial state Ψ_0 is a superposition of states belonging to different channels $\boldsymbol{C}_k$:

$$\Psi_0=\sum_{k,\mu,i}\left(\Omega_{k\mu i},\Psi_0\right)\Omega_{k\mu i} \tag{9.2}$$

If $u_{kv}(t)$ denotes the probability of finding the system in the macrostate $\mathbf{C}_{kv}$ at the time t :

$$u_{kv}(t)=\sum_{i=1}^{s_{kv}}\left|\left(\Omega_{kvi},\exp\left[-\frac{i}{\hbar}H_{\mathrm{II}}t\right]\Psi_0\right)\right|^2, \tag{9.3}$$

we have, by virtue of eqs. (9.1),

$$\mathbf{M}u_{kv}(t)\approx p_k\frac{S_{kv}}{S_k}, \tag{9.4}$$

where

$$p_k=\sum_{\mu,i}|(\Omega_{k\mu i},\Psi_0)|^2 \tag{9.5}$$

In particular, if Ψ_0 is assumed to belong to a given cell $\mathbf{C}_{k\mu}$, i.e. if the system is initially assumed to be in a given macro-state, we have

$$\mathbf{M}u_{kv}(t)\approx\frac{S_{kv}}{S_k}. \tag{$\prime$}$$

By virtuc of this result, we are allowed to consider s_{kv}/S_k as the probability (in the sense of statistical mechanics) of finding the system, at any time, in the macrostate $\mathbf{C}_{kv}$.

Let us suppose that, as is the case in practice, there exists in every channel C_k a cell $\mathbf{C}_{ke_k}$ with a number of dimensions enormously larger than that of the other cells, in such a way that

[8†] Cf. von Neumann [1]), p. 404 and ff.

$$1 - \frac{s_{ke_k}}{S_k} < 1, \quad \frac{s_{kv}}{S_k} < 1 \quad (v \neq e_k) \tag{9.6}$$

(For boson or fermion systems for which the interaction energy between the particles is negligible, as in the examples investigated above, the cells relative to Bose-Einstein or Fermi-Dirac distributions possess this property.)

From (9.4') it follows, by virtue of the inequalities (9.6), that

$$\begin{aligned}
&\mathbf{M}\left\{\left[\sum_{i=1}^{s_{kv}}\left|\left(\Omega_{kvi}, \exp\left[-\frac{i}{\hbar}H_{\mathrm{II}}t\right]\Psi_0\right)\right|^2\right]^2\right\} \\
&\leqslant \mathbf{M}\left\{\sum_{i=1}^{s_{kv}}\left|\left(\Omega_{kvi}, \exp\left[-\frac{i}{\hbar}H_{\mathrm{II}}t\right]\Psi_0\right)\right|^2\right\} \approx \frac{s_{kv}}{S_k} \ll 1, \text{ for } v \neq e_k \qquad (9.7) \\
&\mathbf{M}\left\{\left[\sum_{i=1}^{s_{ka_k}}\left|\left(\Omega_{ke_ki}, \exp\left[-\frac{i}{\hbar}H_{\mathrm{II}}t\right]\Psi_0\right)\right|^2 - 1\right]^2\right\} \\
&\leqslant \mathbf{M}\left\{1 - \sum_{i=1}^{s_{kk_k}}\left|\left(\Omega_{ke_ki}, \exp\left[-\frac{i}{h}H_{\mathrm{II}}t\right]\Psi_0\right)\right|^2\right\} \approx 1 - \frac{s_{ke_k}}{S_k} < 1
\end{aligned}$$

Relations (9.7) entail that, for every initial state $\Psi_0 \in \mathbf{C}_{k\mu}$, the probability $u_{kv}(t)$ is, for the overwhelming majority of the time, very small or very near to 1 (for $v \neq e_k$ and for $v = e_k$, respectively). Consequently, whatever the value of $u_{kv}(t_0)$, we may think that, after a time t sufficiently long, $u_{kv}(t)$ has assumed the values 0 or 1 , i.e.

$$u_{kv}(t) \approx \delta_{ve_k} \tag{9.8}$$

and the system is practically in the macro-state $\mathbf{C}_{ke_k}$. The cell $\mathbf{C}_{ke_k}$ represents precisely the state of macroscopic equilibrium relative to the channel $\mathbf{C}_k$.

If Ψ_0 is given by (9.2) we obtain

$$u_{kv}(t) \approx p_k \delta_{ve_k}. \tag{9.9}$$

In the statistical operator language, after a sufficiently long time the system is macroscopically characterized by the following respective operators:

$$\frac{1}{s_{ke_k}} P_{\mathrm{C}_{k\theta_k}}, \tag{$\prime$}$$

$$\sum_k p_k \frac{1}{s_{ke_k}} P_{\mathrm{C}_{ke_k}}. \tag{$\prime$}$$

28.5.10 10. Schematization of the Measuring Apparatus and Mathematical Theory of the Measuring Process

We want now to consider a schematization of the measuring apparatus more accurate than that given in sect. 7 .

We consider the apparatus as an isolated macro-system (the energy exchanged with the micro-object during the measurement is certainly negligible compared with the internal energy), having an energy macroscopically determined, i.e. lying in a given interval ($E, E + \Delta E$). All

the considerations of the preceding section are assumed to be applicable to the apparatus; in particular, contrary to the assumptions of sect. 7 , we do not suppose here that the channels $\mathbf{C}_k$ correspond to macro-observations, but that each $\mathbf{C}_k$ may be further decomposed into mutually orthogonal submanifolds $\mathbf{C}_{kv}$, everyone of which corresponds to a macro-observation.

In the previously considered example of the proportional counter, the macroscopic state of the system is essentially characterized by the average potential of the counter, by the number of ions, by the spatial and energetic distributions of the neutral molecules and ions, by the charge distribution over the electrodes.

The channels are characterized by the values of the constant of the motion

$$U' = U - \frac{e\lambda}{C}N,$$

where U is the voltage between the electrodes, N is the number of ions, e, λ and C are the elementary charge, the ion multiplication coefficient and the electrostatic capacity of the global system counter + condenser respectively. If U_k is the value of U' characteristic of the k-th channel $\mathbf{C}_k$, the equilibrium manifold $\mathbf{C}_{ke_k}$ corresponds to a
situation in which there is thermal equilibrium within the gas and within the electrodes, there are no ions within the gas and the voltage is U_k. The non-equilibrium manifolds $\mathbf{C}_{kv}$ correspond to situations in which the voltage is still U_k and no ion is present within the gas, but the gas or the electrodes are not in thermal equilibrium, or to situations in which there is a fixed number N of electrons and the voltage has the value $U_k + (e\lambda/C)N$.

In the case of the set of Geiger counters measuring the angular distribution of the scattered particles studied in sect. 8, the channel $\mathbf{C}_0$ corresponds to a situation in which the counters are ali charged and no ion is present and the state $\overline{\mathbf{C}}_{0e_0}$ corresponds to a situation in which gas and electrodes are in thermal equilibrium. The other equilibrium states of interest $\mathbf{C}_{ke_k}$ correspond to situations in which the k-th counter has discharged and there is thermal equilibrium, and the other states of the channel $\mathbf{C}_k$ correspond to situations in which there is no thermal equilibrium or, even if the k-th counter is still charged, there are ions within it.

The macro-system is initially assumed to be in a state Φ_0 belonging to the manifold $\mathbf{C}_{0e_0}$; if the particle is in the state ϕ_k, the interaction brings the apparatus, as supposed in sect. 7 , into a state $\Phi_k \in \mathbf{C}_k$; since the system is assumed to be ergodic inside $\mathbf{C}_k$, it then goes spontaneously into $\mathbf{C}_{ke_k}$ (cf. sect. 9). The latter phase is a process of approach towards an equilibrium situation in the thermodynamical sense.

From the considerations developed in sects. 7 and 9, we obtain immediately the following result:
Initial state of the system I + II:

$$\sum_r c_r \phi_r \Phi_0 \tag{10.1}$$

State after the end of the interaction:

$$\exp\left[-\frac{i}{\hbar}H_{\text{int}}\tau\right]\sum_r c_r\phi_r\Phi_0 = \sum_r c_r\phi_r\Phi_r$$
$$(\Phi_0 \in \mathbf{C}_0; \Phi_r \in \mathbf{C}_r) \tag{10.2}$$

Probability of finding the system I in the state χ_s and the system II in the macrostate $\mathbf{C}_{kv}$ at the time t :

$$\sum_{i=1}^{s_{kv}} \left| \left(\chi_s \Omega_{kvi}, \exp\left[-\frac{i}{\hbar} (H_{\mathrm{I}} + H_{\mathrm{II}})\, t \right] \sum_r c_r \phi_r \Phi_r \right) \right|^2$$
$$= |c_k|^2 \left| \left(\chi_s, \exp\left[-\frac{i}{\hbar} H_{\mathrm{I}} t \right] \phi_k \right) \right|^2 \sum_{i=1}^{s_{kv}} \left| \left(\Omega_{kvi}, \exp\left[-\frac{i}{\hbar} H_{\mathrm{II}} t \right] \Phi_k \right) \right|^2$$
$$\to |c_k|^2 \left| \left(\chi_s, \exp\left[-\frac{i}{\hbar} H_{\mathrm{I}} t \right] \phi_k \right) \right|^2 \delta_{ve_k}. \tag{10.3}$$

Eq. (10.3) is of the type desired, the interference terms which appeared in (5.4) are not present in it; their elimination has been performed without the intervention of a system III observing II. In the statistical operator language, eqs. (10.1), (10.2) and (10.3) may be rewritten as follows:

Statistical operator before the measurement:

$$W_0 = P^{\mathrm{I}}_{[\Sigma_r c_r \phi_r]} P^{\mathrm{II}}_{[\Phi_0]}. \tag{1'}$$

Statistical operator immediately after the end of the interaction:

$$W' = P_{[\Sigma_r c_r \phi_r \Phi_r]}. \tag{10.2'}$$

The time-evolved of this operator after a large time t can be identified, as far as the macroscopic quantities of II are concerned, with

$$\widetilde{W_t} = \sum_r |c_r|^2 P^{\mathrm{I}}_{\{\exp[-(i/h)H_1 t]\phi_r\}} \frac{1}{s_{re_r}} P^{\mathrm{II}}_{\mathrm{C}_{re_r}}. \tag{1'}$$

28.5.11 11. Limitations on the Kind of Quantities Actually Observable; Measurements on Macroscopic Bodies

It follows from the preceding considerations that a given Hermitian operator represents an observable only if it is actually possible to construct an experimental device according to the above scheme. We shall now discuss the various limitations imposed on such a possibility by the structure of the laws of motion. A first restriction is given by the so-called superselection rules [15]). There exist some universal constants of the motion as the electric charge, the baryon number, etc. They determine a decomposition of the Hilbert space of the total system object + apparatus into superselection spaces, which are invariant with respect to the equations of motion. It is never possible therefore to satisfy conditions (5.3) for a Hermitian operator whose eigenstates are superpositions of states corresponding to different values of the above universal constants. Even for the Hermitian operators for which the superselection spaces are invariant, there exist further restrictions. Of this kind are for instance those pointed out by Wigner [4]), which, however, can be overcome, as has been emphasized, by taking into account the fact that the apparatus is a macroscopic system.

Other restrictions are supplied by the following considerations.

If τ is the coupling time between system and apparatus and δt_{I} is the time during which the system I remains in a given eigenstate of α, in order that the quantity A be actually observable, we must obviously have, according to the analysis of the preceding section,

$$\delta t_1 \gg \tau. \tag{11.1}$$

If we denote respectively by $\delta\varepsilon_1$ the energy indeterminacy of the system I when it is in an eigenstate of α, and by $\delta\varepsilon$ the energy indeterminacy of I + II corresponding to an unperturbed energy eigenstate, we have

$$\delta t_1 \approx \hbar/\delta\varepsilon_1 \tag{11.2}$$

and

$$\tau \approx \hbar/\delta\varepsilon. \tag{11.3}$$

From (11.1) it follows that

$$\delta\varepsilon_I \ll \delta\varepsilon \tag{11.4}$$

This relation implies a strong restriction on the nature of the quantities actually observable. In general only quantities quasi-diagonal in the energy representation are observable. An exception is given by the quantities having a very strong degeneracy, as the macroscopic ones.

The indeterminacy $\delta\varepsilon_1$ of the macro-observables is of the order of the width $\Delta\varepsilon_1$ of the energy shell; however, the relaxation time $\tilde{t}_1$ relative to these observables is certainly very large. This is essentially due to the fact that the occupation probability of a macro-state can be written as a sum of a large number of terms, among which some cancellations occur. Consequently the frequency width in the Fourier series expansion of the above probability turns out to be, as a matter of fact, much smaller than $\Delta\varepsilon_1/\hbar$.

As has been previously emphasized, an objective character can be given to the macroscopic quantities only if observations incompatible with these cannot actually be performed, i.e. if quantities whose eigenstates are superpositions of vectors belonging to different $\mathbf{C}_{akv}$ are not observable. (Otherwise, it would not be possible to eliminate the interference terms among the macro-states.)

The above considerations circumscribe the class of the actually observable quantities of a large body, but are not sufficient to exclude the possibility of observations incompatible with macro-observations.

To this end, considerations of a different nature are needed. We notice that in this case the systems I and II of the preceding sections are both macroscopic systems, for every one of which certain ergodicity conditions are satisfied, and it is plausible that similar conditions are satisfied also for the whole system I + II. (Indeed the ergodicity conditions must be a consequence of the very large number of elementary constituents - atoms or molecules - of the systems I and II and of the nature of the forces between these constituents.) If the system I + II satisfies the above ergodicity relations, its final situation is macroscopically represented by a statistical operator (10.3') which is a mixture of the equilibrium states corresponding to the single channels, with weights equal to the initial occupation weights of these channels. Therefore, a statistical operator at the time $t = 0$ for the system I, which corresponds to a pure state, described by a superposition of vectors belonging to different $\mathbf{C}_{akv}$, is equivalent, so far as the macroscopic observations on II are concerned, to a statistical operator which is a mixture of the above macroscopic states. Consequently it is not possible to put any correspondence between final macrostates of II and initial eigenstates of I corresponding to an observable which is not a macroscopic quantity.

It follows from the preceding considerations that there is a fundamental difference between the characteristics of an apparatus for observations on a microscopic system and those of an apparatus for observations on a macroscopic one.

In the first case, the measuring apparatus has a number of degrees of freedom very large with respect to that of the object system; the fact that the apparatus does not perturb appreciably

the system (at least insofar as the quantity considered is concerned) is due to the nature of the interaction system-apparatus and to its short duration. An apparatus for observations on a large body must be, on the contrary, a system small with respect to the body, since in this case the nature of the interaction is very special and the coupling times are long. Moreover it is clear that if one wishes to perform measurements of quantities which change during the time evolution of
the system, it is necessary that the relaxation time of the apparatus be small with respect to that of the system.

By way of example, we consider the case of temperature measurements inside a body. The apparatus is given by a set of thermometers distributed inside the body, the thermal capacities of which are very small with respect to that of the body. In order that these thermometers should make it possible to study how the temperature distribution changes with time, one must assume that each thermometer goes towards the equilibrium, together with the region around it, much more rapidly than the temperature changes with time, i.e. in a time small with respect to the time needed in order that a sensible displacement of heat inside the body takes place.

One could think that the following objection can be raised against our point of view. Consider an hyperapparatus composed of as many measuring apparatus as there are particles constituting a given macroscopic body and suppose we perform on these particles a very accurate measurement, for instance of the energy. We should have in this case an observation much more accurate than a macroscopic one, an observation which could even be incompatible with the macro-observations.

Let us observe, however, that in this way the body would be dissolved into its constituents; the ergodicity conditions, by virtue of which we have been able to exhibit the impossibility of non-macroscopic measurements on a large body are, on the contrary, just a consequence of the interactions which exist between the particles of the macroscopic body and which have the effect of lumping the particles into a single whole.

The meaning of our considerations is precisely the following: when the particles of a system do interact so strongly that a body is formed, it is no longer possible to think of observing them independently.

28.5.12 12. Theory of the Measuring Process under "weak" Ergodicity Conditions

In order to reach the result (9.9) we have used rather restrictive ergodicity conditions. In this section we want to show how, using some plausible assumptions, the same result can be obtained starting from much weaker ergodicity conditions.

We assumed that the initial configuration of the measuring apparatus corresponds to a state belonging to the manifold $\mathbf{C}_{0e_0}$, and that after the end of the interaction the apparatus is in a state belonging to a channel determined by the particular eigenstate of the observable of the micro-object which has been measured. The particular state in this channel depends on the state of the manifold $\mathbf{C}_{\mathbf{0e_0}}$ in which the apparatus was before the measurement. Obviously not all the states of the final channel $\mathbf{C}_k$ can actually be reached by the macro-system since the number of dimensions of the channel is different from (in general larger than) the number of dimensions of the manifold $\mathbf{C}_{0e_0}$. We may even add that not all the macro-states of the system can actually be reached. For instance, in a proportional or Geiger counter the positions of the ions which are created when the particle goes through the apparatus are correlated. If we know the positions of some ions the remaining ones must be more or less aligned with these.

We shall then suppose that the state-vector of the apparatus can actually go only into a given manifold $\mathbf{C}$, union of a given class of manifolds $\mathbf{C}_{kv}$, such that its number of dimensions is equal to the number of dimensions s_{0e_0} of $\mathbf{C}_{0e_0}$. The above class of manifolds corresponds to

the macrostates in which the apparatus can actually be found after the end of the interaction. If Ω_{0e_0i} is the initial state of the apparatus, and if the system is in the state ϕ_k, we assume that, owing to the interaction, the apparatus goes into the state

$$U^{(k)}\Omega_{0e_0t} - \sum_{v}{}' \sum_{j=1}^{s_{kv}} U^{(k)}_{vj,e_0!}\Omega_{kvj} \tag{12.1}$$

$$\sum_{v}{}' s_{kv} = s_{0e_0} \tag{12.2}$$

where $\sum_v'$ denotes the sum taken over the above class of cells. The square matrix $\left\{U^{(k)}_{vj,e_0i}\right\}$ is unitary, i.e. satisfies the conditions

$$\begin{aligned} &\sum_{v}{}' \sum_{j=1}^{s_{kv}} U^{(k)*}_{vj,e_0i'} U^{(k)}_{vj,e_0i} = \delta_{ii'}, \\ &\sum_{i=1}^{s_{0e_0}} U^{(k)\cdot}_{vj,e_0i} U^{(k)}_{v'j',e_0i} = \delta_{vv'}\delta_{jj'}. \end{aligned} \tag{12.3}$$

If, more generally, the initial state of the apparatus is given by

$$\Phi_0 = \sum_{i=1}^{s_0\sigma_0} a_i \Omega_{0e_0i}, \tag{12.4}$$

owing to the interaction with the system the apparatus will go into the state

$$\Phi_k = U^{(k)}\Phi_0 = \sum_{i=1}^{s_0e_0} \sum_{v} \sum_{j=1}^{s_{kv}} a_i U^{(k)}_{vj,e_0i}\Omega_{kvj}. \tag{$\prime$}$$

Thus we obtain

$$\begin{aligned} u_{kv}(t) &= \sum_{i=1}^{s_{kv}} \left| \left(\Omega_{kvi}, \exp\left[-\frac{i}{\hbar}H_{\mathrm{II}}t\right] \Phi_k \right) \right|^2 \\ &= \sum_{i=1}^{s_{kv}} \left| \sum_{\mu}{}' \sum_{j=1}^{s_{k\mu}} \left(\Omega_{kvi}, \exp\left[-\frac{i}{\hbar}H_{\mathrm{II}}t\right] \Omega_{k\mu j} \right) \sum_{l=1}^{s_{0e0}} a_l U^{(k)}_{\mu j,e_0l} \right|^2 \\ &= \sum_{i=1}^{s_{kv}} \sum_{\mu}{}' \sum_{j=1}^{s_{k\mu}} \sum_{\mu'}{}' \sum_{j'=1}^{s_{kv'}} \left(\Omega_{kvi}, \exp\left[-\frac{i}{\hbar}H_{\mathrm{II}}t\right] \Omega_{k\mu j} \right)^* \\ &\quad \cdot \left(\Omega_{kvi}, \exp\left[-\frac{i}{\hbar}H_{\mathrm{II}}t\right] \Omega_{k\mu' j'} \right) \sum_{l'} U^{(k)*}_{\mu j,e_0l} U^{(k)}_{\mu' j',e_0l'} a^*_l a_{l'}. \end{aligned} \tag{12.5}$$

If we put

$$L^{(kv)}_{\mu j,\mu' j'} = \frac{S_k}{S_{kv}} \left\{ \mathbf{M} \sum_{i=1}^{s_{kv}} \left[\left(\Omega_{kvi}, \exp\left[-\frac{i}{\hbar} H_{II} t \right] \Omega_{k\mu j} \right)^* \cdot \left(\Omega_{kvi}, \exp\left[-\frac{i}{\hbar} H_{II} t \right] \Omega_{k\mu' j'} \right) \right] - \frac{s_{kv}}{S_k} \delta_{\mu\mu'} \delta_{jj'} \right\}$$
$$= \frac{S_k}{s_{kv}} \left\{ \sum_{i=1}^{s_{kv}} \frac{\sum_\rho}{\rho} \left(\Omega_{kvi}, P_\rho \Omega_{k\mu j} \right)^* \left(\Omega_{kvi}, P_\rho \Omega_{k\mu' j'} \right) - \frac{s_{kv}}{S_k} \delta_{\mu m'} \delta_{jj'} \right\}, \tag{12.6}$$

we have

$$\frac{\left(\mathrm{M} u_{kv}(t) - s_{kv}/S_k \right)^2}{s^2_{kv}/S^2_k} = \sum_{\mu\mu'\lambda\lambda'}{}' \sum_{j=1}^{s_{k\mu}} \sum_{j'=1}^{s_{k\mu'}} \sum_{i=1}^{s_{k\lambda}} \sum_{l'=1}^{s_{k\lambda'}} L^{(kv)*}_{\mu j,\mu' j'} L^{(kv)}_{\lambda l',\lambda' l'}$$
$$\cdot \sum_{uu'vv'} U^{(k)}_{\mu j,\ \mathrm{eo}\ u} U^{(k)*}_{\mu' j',\ \mathrm{eo}\ u'} U^{(k)*}_{\lambda l,\ \mathrm{eov}} U^{(k)}_{\lambda' l',\ \mathrm{e}\ vv'} a_u a^*_{u'} a^*_v a_{v'}. \tag{12.7}$$

We denote now by $\mathfrak{B}_0$ an averaging operation over the initial states Φ_0 performed with the following criterion. We attribute to any set of vectors Φ_0 a weight proportional to the area of the surface determined by them over the complex s_{0e_0}-dimensional spherical surface of equation

$$\sum_{i=1}^{s_0 s_0} |a_i|^2 = 1. \tag{12.8}$$

One then obtains (cf. Prosperi and Scotti [12]))

$$\mathfrak{B}_0 \left(a_u a^*_{u'} a^*_v a_{v'} \right) = \frac{\delta_{uu'}\delta_{vv'} + \delta_{uv}\delta_{u'v'}}{s^2_{0e_0}} \tag{12.9}$$

By virtue of eqs. (12.3) it follows that

$$\mathfrak{B}_0 \left(\sum_{\mu u' v v'} U^{(k)}_{\mu j, e_0 u} U^{(k)*}_{\mu' j', e_0 u'} U^{(k)*}_{\lambda l, e_0 v} U^{(k)}_{\lambda' l', e_0 v'} a_u a^*_{u'} a^*_v a_{v'} \right)$$
$$= \frac{1}{s^2_{0e_0}} \left(\sum_u U^{(k)}_{\mu j, e_0 u} U^{(k)*}_{\mu' j', e_0 u} \cdot \sum_v U^{(k)*}_{\lambda l, e_0 v} U^{(k)}_{\lambda' l', e_0 v} \right.$$
$$\left. + \sum_u U^{(k)}_{\mu j, e_0 u} U^{(k)*}_{\lambda l, e_0 u} \cdot \sum_{u'} U^{(k)*}_{\mu' j', e_0 u'} U^{(k)}_{\lambda' l', e_0 u'} \right)$$
$$= \frac{1}{s^2_{0e_0}} \left(\delta_{\mu\mu'}\delta_{jj'}\delta_{\lambda\lambda'}\delta_{ll'} + \delta_{\mu\lambda}\delta_{jl}\delta_{\mu'\lambda'}\delta_{j'i'} \right), \tag{12.10}$$

from which

$$\sum_{kv} \frac{\mathfrak{B}_0 \left(\mathrm{M} u_{kv}(t) - s_{kv}/S_k \right)^2}{s^2_{kv}/S^2_k} = \frac{1}{s^2_{0e_0}} \sum_{kv}{}' \left(\sum_{\mu\lambda}{}' \sum_j \sum_l L^{(kv)}_{\mu j,\mu j} L^{(kv)}_{\lambda l,\lambda l} \right.$$
$$\left. + \sum_{\mu\mu'}{}' \sum_{jj'} L^{(kv)*}_{\mu j,\mu' j'} L^{(kv)}_{\mu j,\mu' j'} \right) = \sum_{k\nu} \left[\left(\frac{1}{s_{0e_0}} \sum_\mu{}' \sum_j L^{(kv)}_{\mu j,\mu j} \right)^2 \right.$$
$$\left. + \frac{1}{s^2_{0e_0}} \frac{\sum'_{\mu\mu'}}{\sum_{jj'}} \left| L^{(kv)}_{\mu j,\mu' j'} \right|^2 \right]. \tag{12.11}$$

We now assume the following ergodicity conditions:

$$\frac{1}{s_{k\mu}}\left|\sum_{j=1}^{s_{k\mu}} L^{(kv)}_{\mu j,\mu j}\right| < \frac{1}{\sqrt{N}}, \tag{12.12}$$

$$\frac{1}{s_{k\mu}}\sum_{j=1}^{s_{k\mu}}\frac{1}{s_{k\mu'}}\sum_{j'=1}^{s'_{k\mu'}}\left|L^{(kv)}_{\mu j,\mu' j'}\right|^2 < \frac{1}{N}$$

(where $N - \sum_k N_k$), which are much less strong than conditions (9.1) (cf. Prosperi and Scotti [12])). From these relations and from (12.2) it follows that

$$\begin{aligned}
&\left|\frac{1}{s_{0e_0}}\sum_{\mu}{}'\sum_{j=1}^{s_{k\mu}} L^{(kv)}_{\mu j,\mu j}\right| \leqslant \frac{1}{s_{0e_0}}\sum_{\mu}{}'\left|\sum_{j=1}^{s_{k\mu}} L^{(kv)}_{\mu j,\mu j}\right| \\
&= \frac{1}{s_{0e_0}}\sum_{\mu}{}' s_{k\mu}\frac{1}{s_{k\mu}}\left|\sum_{j=1}^{s_{k\mu}} L^{(kv)}_{\mu j,\mu j}\right| < \frac{1}{\sqrt{N}}\frac{1}{s_{0e_0}}\sum_{\mu}{}' s_{k\mu} = \frac{1}{\sqrt{N}} \\
&= \frac{1}{s^2_{0e_0}}\sum_{\mu\mu'}{}' s_{k\mu}s_{k\mu'}\frac{1}{s_{k\mu}}\sum_{j}\frac{1}{s_{k\mu'}}\sum_{j'}\left|L^{(kv)}_{\mu j,\mu' j'}\right|^{\frac{1}{s^2_{0e_0}}\sum'_{\mu\mu'}\sum_{j=1}^{s_{k\mu}}\sum_{j'=1}^{s_{k\mu'}}\left|L^{(kv)}_{\mu j,\mu' j'}\right|^2} \\
&< \frac{1}{N}\frac{1}{s^2_{0e_0}}\left(\sum_{\mu}{}' s_{k\mu}\right)^2 = \frac{1}{N}
\end{aligned}$$

and in conclusion

$$\sum_{kv}\frac{\mathfrak{B}_0\left(\mathbf{M}u_{kv}(t) - s_{kv}/S_k\right)^2}{s^2_{kv}/S^2_k} \ll \sum_{kv}\frac{2}{N} = 2. \tag{12.14}$$

Owing to the replacement of the ergodicity conditions (9.1) by the conditions (12.12), we are no longer allowed to conclude that relations (9.4') and (9.8) are verified for every initial microstate Φ_0 of the apparatus. However, as follows from relation (12.14), the ergodicity conditions (12.12) allow us to assert that the set of the initial exceptional states for which (9.4') and (9.8) are not verified has a very small measure. But this is the only result needed in order to be able to draw the conclusion of sect. 10 .

We finally remark that in the case in which the energy is the only macroscopic constant of the motion (and hence the channels coincide with the energy shells), the following result can be proved (cf. Prosperi [16])): Ergodicity conditions of the kind (12.12) are satisfied, under suitable restrictive conditions, by the Hamiltonians for which Van Hove [17]) has derived a master equation. These Hamiltonians already represent some physically significant examples and it is very likely that most of the macro-systems belong to this class. Consequently relations (12.12) are much more representative of the physical nature of the systems studied than would appear at first sight.

We cordially thank our friends P. Bocchieri, A. Scotti and G. Stabilini for helpful discussions.

References

1. J. von Neumann, Mathematical foundations of quantum mechanics (Princeton University Press, Princeton, 1955) chapts. 5 and 6

2. P. Jordan, Phil. Sci. 16 (1949) 269

3. D. Bohm, Quantum theory (Prentice-Hall, New York, 1952), part VI

4. E. P. Wigner, Z. Phys. 133 (1952) 101: H. Araki and M. M. Yanase, Phys. Rev. 120 (1960) 622

5. G. Ludwig, Z. Phys. 135 (1953) 483 ; Die Grundlagen der Quantenmechanik (Springer-Verlag, Berlin, 1954) chapt. 5; Festschrift z. 200. Jahrfeier d. Columbia Univ. (Colloquium-Verlag, Berlin) p. 262; Phys. Bl. 11 (1955) 489

6. P. K. Feyerabend, Z. Phys. 148 (1957) 551; Proc. Nineth Symp. Colston Research Soc. (Butterworths Publishers, London, 1957) p. 121

7. H. S. Green, Nuovo Cim. 9 (1958) 880

8. L. Durand III, unpublished preprint (1958)

9. H. Wakita, Prog. Theor. Phys. 23 (1960) 32

10. G. Ludwig, Z. Naturfors. 12 (1957) 662; Z. Phys. 150 (1958) 346; 152 (1958) 98;
J. Schroeter, Z. Naturfors. 14 (1959) 750;
G. Ludwig in Reports of the Varenna Summer School 1960 (to be published);
N. G. van Kampen, Physica 20 (1954) 603; Fortschr. d. Phys. 4 (1956) 405;
II. Kucmmel, Nuovo Cim. 1 (1955) 1057

11. P. Bocchieri and A. Loinger, Phys. Rev. 114 (1959) 948;
G. M. Prosperi and A. Scotti, Nuovo Cim. 13 (1959) 100; 17 (1960) 267

12. G. M. Prosperi and A. Scotti, J. Math. Phys. 1 (1960) 218;
A. Loinger in Reports of the Varenna Summer School 1960 (to be published)

13. C. F. von Weizscker, Z. Phys. 118 (1941) 480

14. G. Lueders, Ann. Phys. 8 (1951) 322

15. G. C. Wick, A. S. Wightman and E. P. Wigner, Phys. Rev. 88 (1952) 101

16. G. M. Prosperi, J. of Math. Phys., in course of publication

17. L. Van Hove, Physica 21 (1955) 517; 23 (1957) 441; 25 (1959) 268

28.6 V.5 Time Symmetry in the Quantum Process of Measurement*

Abstract

We examine the assertion that the "reduction of the wave packet," implicit in the quantum theory of measurement introduces into the foundations of quantum physics a time-asymmetric element, which in turn leads to irreversibility. We argue that this time asymmetry is actually related to the manner in which statistical ensembles are constructed. If we construct an ensemble time symmetrically by using both initial and final states of the system to delimit the sample, then the resulting probability distribution turns out to be time symmetric as well. The conventional expressions for prediction as well as those for "retrodiction" may be recovered from the time-symmetric expressions formally by separating the final (or the initial) selection procedure from the measurements under consideration by sequences of "coherence destroying" manipulations. We can proceed from this situation, which resembles prediction, to true prediction (which does not involve

any postselection) by adding to the time-symmetric theory a postulate which asserts that ensembles with unambiguous probability distributions may be constructed on the basis of preselection only. If, as we believe, the validity of this postulate and the falsity of its time reverse result from the macroscopic irreversibility of our universe as a whole, then the basic laws of quantum physics, including those referring to measurements, are as completely time symmetric as the laws of classical physics. As a by-product of our analysis, we also find that during the time interval between two noncommuting observations, we may assign to a system the quantum state corresponding to the observation that follows with as much justification as we assign, ordinarily, the state corresponding to the preceding measurement.

28.6.1 I. Introduction

ONE of the perennially challenging problems of theoretical physics is that of the "arrow of time." Everyday experience teaches us that the future is qualitatively different from the past, that our practical powers of prediction differ vastly from those of memory, and that complex physical systems tend to develop in the course of time in patterns distinct from those of their antecedents. On the other hand, all the "microscopic" laws of physics ever seriously propounded and widely accepted are entirely symmetric with respect to the direction of time; they are form-invariant with respect to time reversal. [1,2]

The de facto absence of time symmetry in nature enters the formal statement of the laws of nature principally in two areas. One of these is thermodynamics, particularly the second law of thermodynamics; the latter proclaims that the entropy of a thermally isolated system can only increase toward the future. The other area is that of cosmogony; our universe is expanding toward the future. Gold [1] has suggested that these two asymmetric phenomena may well be causally related to each other. A third timeasymmetric effect, the preponderance of outgoing radiation in nature over incoming radiation, may be considered to be a special aspect of the second law.

In quantum theory the dynamical laws of motion,

either the Schrödinger or the Heisenberg equations, are time symmetric as are their classical counterparts, Hamilton's equations of motion. It has been suggested, though, that asymmetry in the direction of time, and even thermodynamic irreversibility, enters into quantum theory through the theory of measurement. [3,4] Any measurement performed on a quantum system changes its state discontinuously and in a manner not to be described by the Schrödinger or Heisenberg equations of the isolated system. The performance of a measurement leads to the "reduction of the wave packet." That is to say, if the result of the measurement is known, then the quantum state of the system preceding the measurement has been replaced by the eigenvector of the observable that belongs to the eigenvalue recorded. If the outcome of the measurement is not known, the original state vector must now be replaced by a density matrix diagonal with respect to the eigenvectors of the observables measured, each diagonal element equaling the absolute square of the corresponding component of the original state vector. This density matrix is inequivalent to the original state vector in that all phase relations between the components have been destroyed by the act of measurement, though their noms survive in the density matrix.

Quite aside from entropy considerations, the conventional quantum theory of measurements

[8]*This research was supported by the U. S. Air Force Office of Scientific Research, Aerospace Research Laboratories, the National Science Foundation, and the National Aeronautics and Space Administration.

[1] T. Gold, in Onzime Conseil de l'Institut International de Physique Solvay, La Structure et l'Evolution de l'Universe (Edition Stoops, Brusselis, 1958), p. 81; Am. J. Phys. 30, 403 (1962); Proceedings of the Conference on the Arrow of Time, Cornell University, 1963 (to be published).

[2] See, however, O. Penrose and I. C. Percival, Proc. Phys. Soc. (London) 79, 605 (1962).

is concerned exclusively with the prediction of probabilities of specific outcomes of future measurements on the basis of the results of earlier observations. Indeed the reduction of the wave packet has as its operational

contents nothing but this probabilistic connection between successive observations. [5]

In this paper we propose to examine the nature of the time symmetry in the quantum theory of measurement. Rather than delve into the measurement process itself, which involves a specialized interaction between the atomic system and a macroscopic device, [3–5] we shall simply accept the standard expressions for probabilities of values furnished by the conventional theory. Whereas the conventional theory deals with ensembles of quantum systems that have been "preselected" on the basis of somc initial observation, we shall deduce from it probability expressions that refer to ensembles that have been selected from combinations of data favoring neither past nor future. A theory that concerns itself exclusively with such symmetrically selected ensembles (the "time-symmetric theory") will contain only timesymmetric expressions for the probabilities of observations. Logically this time-symmetric theory is contained in the conventional theory but lacks one of the latter's postulates. It will be developed in Sec. II.

In Sec. III we shall consider the case that prior to the final selection some observations are performed that completely destroy coherence of any state previously existing; we shall find that any earlier observations obey probability laws that formally resemble the conventional prediction formula. Likewise, if the initial selection ("preselection") is followed by coherence destroying measurements to be succeeded in turn by some other observations, then these latter observations obey the precise time-reflected expression of the conventional prediction formula. This reflected relationship might be called a "retrodiction" formula. Finally, in Sec. IV we shall return to the true prediction and "retrodiction" situations, i.e., to the consideration of ensembles that have been either strictly preselected or postselected. By adding to the time-symmetric theory one postulate that appears to portray accurately the conditions of our universe (and whose time-reflected proposition does not hold), we are able to recover the conventional asymmetric theory. We present an argument that this asymmetry represents the intrusion of the irreversibility of macroscopic processes into the microscopic domain, so that the totality of the basic (microscopic) laws of nature emerges completely time symmetric.

28.6.2 II. Sequences of Observations

We shall begin by considering systems which are subjected to sequences of measurements, each of which is individually "complete"; that is to say, that each observation determines a quantum state of the system. We make the conventional assumption about the selection of ensembles of such systems (and of their histories), which is to the effect that initially all systems of the ensemble have yielded a specified nondegenerate eigenvalue of an observable J; no other conditions are

imposed. Under these circumstances the conventional quantum theory of measurements states that, given two successive measurements, the probability of a particular outcome of the later observation depends on the outcome of the earlier observation by being the absolute square of the scalar product of the two statevectors belonging to the two respective eigenvalues. We shall denote the observables to be measured by symbols $A_1, A_2, \cdots, A_k, \cdots$, all of whose eigenvalues are nondegenerate; let the eigenvalues of A_k be denoted by d_k. Only when necessary will distinct eigenvalues of A_k be denoted by Greek superscripts ${d_k}^{(\alpha)}, {d_k}^{(\beta)}, \cdots$. For the sake of simplicity we shall work in a Heisenberg representation and assume further that all the A_k are

[83] J. von Ncumann, Mathematical Foundations of Quantum Mechanics, transl. by R. T. Beyer (Princeton University Press, Princeton, 1955).

[4] D. Bohm, Quantum Theory (Prentice-Hall Inc., Englewood Cliffs, New Jersey, 1951), cf. in particular, p. 608.

[85] E. P. Wigner, Am. J. Phys. 31, 6 (1963).

constants of the motion, not necessarily explicitly timeindependent. At any rate, between measurements both the quantum states of our systems and the matrix elements of our observables will be constant. If the observables A_k are to be measured in any particular sequence, which, in general, will not correspond to the order of the subscripts $\cdots, k, \cdots$, we shall indicate the scquonce of measurements by Latin superscripts, thus: ${A_k}^m$.

Suppose now that we perform a sequence of observations, ${A_m}^{-M}, \cdots, {A_i}^{j-1}$, yielding the measurements $d_m, \cdots, d_i$; then the probability that the next measurement ${A_k}^i$ will yield the eigenvalue d_k is

$$p\left(d_h/d_m, \cdots, d_i\right) = \left|\langle d_i \mid d_k\rangle\right|^2 = \mathrm{Tr}\left(D_i D_k\right) \tag{2.1}$$

where the symbol D_k denotes the idempotent operator

$$D_k \equiv |d_k\rangle \langle d_k| \tag{2.2}$$

etc. If the measurement ${A_k}^j$ is to be followed by ${A_l}^{j+1}, {A_n}^{j+2}, \cdots, {A_r}^{N-1}, {A_s}^N$, the probability that the respective outcomes will be $d_k, d_l, \cdots, d_r, d_s$ is

$$\begin{aligned} p\left(d_k, \cdots, d_r, d_s/d_m, \ \cdots, d_i\right) & \\ = \mathrm{Tr}\left(D_s D_r \cdots D_k D_i D_k \cdots D_r\right). & \end{aligned} \tag{2.3}$$

Equations (2.1) and (2.3) hold irrespective of the outcome of the measurements ${A_m}^{-M}, \cdots, {A_h}^{j-2}$, and irrespective of the outcome of the members of the ensemble subsequent to the performance of the specified observation(s). These expressions summarize the quantitative content of the conventional theory of measurement in quantum physics.

In passing let us briefly comment on the need in quantum theory for constructing ensembles with welldefined probability characteristics. If, in classical mechanics, we had to deal with a system possessing a phase space with a finite volume Ω, then we could define an a priori probability density on that phase space that would be invariant with respect to canonical transformations: the constant probability density Ω^{-1}. One could then modify this density in conformity with any restrictions imposed on the physical system, so as to obtain contingency probabilities by purely deductive methods. In other words, in a finite phase space one might construct statistical mechanics employing a
standard ensemble as the point of departure. Because in every realistic physical system the phase space has an infinite volume, a transformation-invariant standard probability density does not exist, and one is led into constructing or conjecturing probability distributions to fit various conditions imposed on the ensemble.
The situation in quantum theory is analogous. If Hilbert space were finite-dimensional, then there would be one density matrix distinguished as being representation-invariant, the normalized multiple of the unit matrix, from which all other density matrices could be derived in response to various contingencies. But again, for all realistic physical systems Hilbert space is infinite-dimensional; hence, there is no "standard ensemble" existing a priori and independently of any information about our physical system. Thus, formally, we are forced to construct ensembles of systems having certain restrictive properties. Whether particular classes of restrictions lead to ensembles with unambiguous probability characteristics cannot be decided affirmatively by formal analysis alone, though internal inconsistencies might rule out some conjectures. It is clear that the assumptions underlying the conventional theory of quantum measurements are logically admissible.

Next we shall consider a sequence of measurements $J, {A_k}^{-M}, \cdots, {A_j}^{-1}, {A_i}^0, {A_l}^1, {A_m}^2, \cdots, {A_n}^N, F$, in that order. J and F are to be nondegenerate observables like the others, and their eigenvalues are denoted respectively by a and b. We

shall now consider an ensemble of systems whose initial and final states are fixed to correspond to the particular eigenvalues a and b, respectively; we ask for the probability that the outcome of the intervening measurements are $d_j, \cdots, d_n$, respectively. This probability, on the strength of Eq. (2.3), is found to be

$$p\,(d_j, \cdots, d_n/a, b) = \frac{p\,(d_j, \cdots, d_n, b/a)}{p(b/a)} = \frac{1}{H(a,b)}\,\mathrm{Tr}\,(AD_j \cdots D_n B D_n \cdots D_j) \tag{2.4}$$

where

$$H(a,b) = \sum_{j'} \cdots \sum_{n'} \mathrm{Tr}\,(AD_{j'} \cdots D_{n'} B D_{n'} \cdots D_{j'}) \qquad A = |a\rangle\langle a|, \quad B = |b\rangle\langle b| \tag{2.5}$$

This expression is manifestly time symmetric. If we change the sequence of measurements to F, ${A_n}^{-N}, \cdots, {A_k}^{M}, J$, Eqs. (2.4), (2.5) remain unchanged. In the exceptional case $H(a,b) = 0$ the probability $p\,(d_j \cdots d_n/a, b)$ is not defined.

The probabilities (2.4), (2.5) refer to a sample that has been selected on the basis of required outcomes of specified initial and final observations. This procedure may appear artificial compared to the usual prescription: "Prepare a system so that the value of J (at the beginning) be a." But from a formal point of view we may legitimately specify any selection that could be performed with physical equipment, however complex.

As a matter of fact, in experimental physics selections are frequently based on combinations of initial and final characteristics. Consider a beam of particles that enters a cloud chamber or similar device controlled by a master pulse. For the device to select an event as belonging to a sample to be evaluated statistically, the particle must enter the chamber and, prior to the onset of any manipulation by magnetic fields, etc., satisfy certain requirements. But in order to be counted the particle must also activate the circuits of counters placed below the chamber; thus, we make the selection on the basis of both the initial and the final state. In scme experiments even intermediate specifications may be imposed in addition to initial and final conditions. Thus, our formal treatment of initial and final states on an equivalent footing is not inconsistent with experimental procedures used in some investigations.

Equations (2.4), (2.5) may be thought of as providing the foundation for a time-symmetric theory of measurement. If we assumed the existence of ensembles with well-defined probabilities only if selected on the basis of both initial and final states, we should have a logically closed theory, though one that would never permit extrapolations to time intervals lying outside the interstice between initial and final determination. Given ensembles of any kind with well-defined probability dispersions, we can always form subensembles obeying additional restrictions and hence the time-symmetric ensembles can be obtained from those of the conventional theory by means of a deductive process. The reverse does not hold, i.e., we cannot infer the characteristics of broadly defined ensembles from those of more narrowly defined ensembles.

On the basis of Eqs. (2.4), (2.5) we may calculate probabilities involving only some of the measurements between J and F, or we may calculate contingent probabilities referring to partial samples in which the outcomes of some of these measurements are fixed. In particular we can calculate the contingent probability of the outcome ${d_l}^1$, given the outcome ${d_i}^0$. To obtain this probability we must, of course, sum over all the possible outcomes of the measurements preceding ${A_i}^0$ and over all the possible outcomes following ${A_l}^1$, keeping, as before, the outcomes of J and F fixed. The result is

$$p'(d_l/d_i;a,b) = \frac{\sum_{m'}\cdots\sum_{n'}\mathrm{Tr}\,(D_iD_lD_{m'}\cdots D_{n'}BD_{n'}\cdots D_{m'}D_l)}{\sum_{l'}\sum_{m'}\cdots\sum_{n'}\mathrm{Tr}\,(D_lD_{l'}D_{m'}\cdots D_{n'}BD_{n'}\cdots D_{m'}D_{l'})}$$
$$= |\langle d_i \mid d_l\rangle|^2 \frac{\sum_{m'}\cdots\sum_{n'}\mathrm{Tr}\,(D_lD_{m'}\cdots D_{n'}BD_{n'}\cdots D_{m'})}{\sum_{l'}\cdots\sum_{n'}\mathrm{Tr}\,(D_iD_{l'}D_{m'}\cdots B\cdots D_{m'}D_{l'})} \tag{2.6}$$

As expected, the history preceding the measurement ${A_i}^0$ drops out of our expression, but the coefficient of the squared matrix element of the conventional prediction (2.1) is sensitive to d_i and to d_l as well as to the subsequent history. In other words, postselection will affect the transition probability from d_i to d_l. That this is unavoidable can be understood easily by the consideration of the extreme case in which all observables $A_m,\cdots,A_n,F$ commute with each other as well as with A_l. Depending on the selection of the eigenvalue b, the transition probability in that case will be either 0 or 1.

It is obvious that the time-reflected relationship to (2.6) also holds. That is to say, if we calculate the contingent probability of d_i knowing the outcome d_l of the observation immediately following, we shall obtain an expression that is independent of the whole history subsequent to the measurement ${A_l}^1$, but which will depend on the initial selection a as well as observations scheduled prior to ${A_i}^0$.

Let us now consider incomplete measurements. The result (2.4), (2.5) can be generalized immediately if we drop the requirement that each intermediate measurement be complete. According to von Neumann, [3] an incomplete observation projects the initial state not on a particular direction but on a particular (multidimensional) linear subspace of the Hilbert space, and may be represented by an idempotent operator D_k. The form of Eqs. (2.4), (2.5) will remain unchanged under this reinterpretation of the symbols D_k. It should be noted, however, that Eq. (2.6) holds only if A_i is nondegenerate.

The replacement of the initial and final states by mixtures is a bit more involved. If we form an ensemble in which histories beginning with state $|a\rangle$ and ending with state $|b\rangle$ form a fraction c_{ab} of the whole

$$c_{ab}\geq 0,\quad \sum_{a'}\sum_{b'}c_{a'b'}=1, \tag{2.7}$$

then the probability $p(d_j,\cdots,d_n/\{c\})$ will be

$$p(d_j,\cdots,d_n/\{c\}) = \sum_{a'}\sum_{b'}c_{a'b'}p(d_j,\cdots,d_n/a',b') \tag{2.8}$$

There exists no simple expression that would depend on the initial and final density matrices. The probabilities (2.8) depend on the fractions of systems within the ensemble passing from specified initial to specified final states, not merely on the initial distribution $\sum_{b'}c_{ab'}$ and the final distribution $\sum_{a'}c_{a'b}$.

28.6.3 III. Asymptotic Procedures

Whereas we have been able to obtain time-symmetric ensembles from those depending only on initial selection, the reverse procedure is impossible without an additional postulate; that is to say, given a theory of ensembles based on time-symmetric double-selection procedures, we cannot obtain probabilities for ensembles in which the selection is based only on initial (or only on final) observations by deduction alone. In this sense,

the time-symmetric theory of Sec. II is more restricted than the conventional theory of measurements.

There is, however, a way to blunt the effects of either pre- or postselection. The method to be described in this section rests on the fact that in quantum theory the type of interference that we call an observation destroys the "coherence" of the state of a system, producing a new situation that is connected with the original situation only by stochastic laws. This stochastic connection, or the lack of a/tighter relationship, may be expressed either in terms of the state vector, or its replacement by a density matrix, or purely in terms of probabilistic assertions. Whatever the mode of description, it is possible to sever different portions of the history of a system from each other by the interposition of certain types of measurements. By preceding the final selection in the time-symmetric theory by such "coherence destroying" manipulations, we may formally recover the prediction formula (2.1); by scheduling such procedures following the initial selection of a timesymmetric ensemble, we may obtain the time-reverse of Eq. (2.1), a "retrodiction" formula.

These possibilities are of considerable interest because they present us with a relatively large class of possible procedures all of which lead, asymptotically in most cases, to substantially similar results. Though the interpolation of coherence destroying manipulations, say before the act of final selection within the framework of the time-symmetric theory, does not relieve us of the logical necessity of performing the act of final selection, the particular choice of observable and of its numerical value used for that final selection has no effect on the probabilities of events preceding the coherence destroying acts.

We shall first indicate particular sets of measurements which destroy coherence more or less completely. Such sets of two consecutive measurements may be constructed in closed form if the Hilbert space of a system is finite dimensional, e.g., if the particles in a monochromatic and well-collimated beam can differ only in their states of polarization. Consider, in this case, two observables A_i and A_j whose eigenvectors are related to each other by a unitary matrix U and whose matrix elements all have the same absolute square $1/n, n$ being the number of dimensions of the Hilbert space. One possible unitary matrix with this property is, for instance, the following:

$$U_{kl} = \left[1/(n)^{1/2}\right] e^{i\theta_{kl}}, \quad \theta_{kl} = (2\pi/n)kl. \tag{3.1}$$

Let us denote the idempotent operators to be constructed from the respective eigenvectors of the two observables by D_1 and D_2, respectively, each of these symbols representing n such different operators. Then the following expression constructed with any density matrix M whatsoever is always a multiple of the unit matrix I :

$$\sum_{d_1} \sum_{d_2} D_1' D_2' M D_2' D_1' = (1/n) I. \tag{(3.2)}$$

As for the infinite-dimensional case, the situation is insofar more involved as there exists no density matrix which is precisely a multiple of the unit matrix. We shall assume that the Hilbert space admits a complete set of commuting operators, each having a continuous range of eigenvalues from $-\infty$ to ∞. We shall call these operators x_s and construct by the usual methods a set of operators p_s which satisfy standard canonical commutation relations with each other and with the x_s. In a somewhat symbolic sense the unitary operators leading from the improper joint eigenfunctions of the x_s to the improper joint eigenfunctions of the p_s, i.e., the Fourier integral operators, possess matrix elements all of the same magnitude as in the previous case. In view of the fact that idempotent operators of the type $x\,(x_0)$, etc., are not really defined, we introduce idempotent operators $X(x, \Delta)$, defined as integral operators whose kernel equals 1 if $x \in \Delta$, and vanishes otherwise. We cover the space of numerical values of the x_s with a denumerable set of domains Δ without overlap. Similarly, we introduce idempotent operators $P(p, E)$, where the domains E cover the momentum space without overlap. The expression constructed in complete analogy to (3.1) will then not equal a multiple of the unit

matrix because of the coarseness of the cell structures established in x space and in p space. However, we may establish a sensible limit if we improve the fineness of both cell structures and if we multiply the expression (3.1) on the left by a factor corresponding to the effective n, eventually becoming infinite, so that the right side can actually tend to the identity operator I (whose trace diverges).

We now return to the expression (2.4) and substitute for a certain number of factors centered on F a multiple of I, both in the numerator and the denominator. The constant of proportionality used is immaterial, as it drops out in any case, and we might use I directly. We then see, almost by inspection, that (2.4) reduces to (2.3), the pure prediction formula, and, likewise, that (2.6) reduces to (2.1). We conclude, then, that because of the asymptotic properties of expressions of type (3.2) the prediction formulas may be recovered from the time-symmetric formulas.

We may derive the corresponding "retrodiction" expression by time reversing the procedure that we have just presented. If we follow the initial selection of an ensemble in the time-symmetric theory by a set of coherence-destroying measurements, then the outcome of subsequent observations is related to the final selection as follows:

$$p\left(d_k, d_l, \cdots, d_s/a, b\right) = \mathrm{Tr}\left(D_k D_l \cdots D_s B D_s \cdots D_l\right) \tag{3.3}$$

If, in particular, we are concerned with the one observation preceding the final selection, then the probability of the outcome d is

$$p(d/b) = |\langle b \mid d\rangle|^2 \tag{3.4}$$

The coherence destroying properties of the procedure
summarized in Eqs. (3.1), (3.2), and of the corresponding asymptotic procedure outlined for the infinitedimensional Hilbert space may be demonstrated by straightforward computation. It would be of considerable interest if there were a broad range of procedures having the samc cffect. Generally, sequences of measurements will destroy coherence to a greater or lesser extent provided that they involve all directions of Hilbert space in noncommuting measurements. There are, of course, degrees of noncommutativity: The noncommutavity may involve varying numbers of directions in Hilbert space, and the eigendirections of consecutive operators may differ from each other by various angles. Formally, the extent to which coherence is destroyed by a given sequence may be evaluated in terms of the degree to which matrices of the general form (3.2) approximate a multiple of the unit matrix. That there is some approach to the unit matrix in a sequence of noncommuting measurements is assured by the results to be found in von Neumann. [3] If $D^{(\alpha)}$ is a set of idempotent operators belonging to the same measurement and with properties

$$D^{(\alpha)} D^{(\beta)} = \delta^{\alpha\beta} D^{(\alpha)}, \quad \sum_{\alpha} D^{(\alpha)} = I \tag{3.5}$$

and if M is an arbitrary density matrix, then

$$M' = \sum_{\alpha} D^{(\alpha)} M D^{(\alpha)} \tag{3.6}$$

is also a density matrix and approximates a multiple of the unit matrix I at least as well as M in the following respects: (a) If we define the entropy of M as usual by the expression

$$S = -k\,\mathrm{Tr}(M \ln M) \tag{3.7}$$

then

$$S' \geqslant S. \tag{3.8}$$

The equality holds only if the idempotent operators commute with M. (b) The range of eigenvalues of M' is not greater than the range of eigenvalues of M; that is to say, the upper limit of its eigenvalues is not larger and the lower limit not smaller. Both entropy and range of eigenvalue spectrum are yardsticks for the approach to λI.

Thus, it appears that we can destroy coherence more or less completely by a wide variety of sequences of measurements and thereby obtain the asymptotic prediction and retrodiction situations within the framework of the time-symmetric theory of measurements.

The existence of the retrodiction formula (3.3), (3.4) suggests that the customary assignment of a state vector to a system on the basis of the most recent preceding observation may be somewhat arbitrary. This assignment is based on the intuitive notion that the measurement is the "cause" and the quantum state the "effect," and that cause must precede effect in time. Also, perhaps, there is the notion that the quantum state of a system embodies the maximum of information available to us about the system at any time; ordinarily, we
can know the outcome of all observations in the past but not of those yet in the future.
But, as we have seen, under suitable circumstances the usual prediction formula (2.1) may be replaced by the retrodiction formula (3.4), which bases a probabilistic statement about the outcome of one measurement on the outcome of the measurement next following in time. If the measurement of A (whose eigenvalues are being denoted by d) is preceded by coherence destroying operations as we have assumed in deriving Eqs. (3.3) and (3.4), then we know essentially nothing about the outcome of observations preceding A; that is to say, all possible outcomes of such preceding observations are approximately equally likely. Hence, our probabilistic statement about the outcome of the measurement of A is based primarily on the event immediately following, and the information on which our statement is based ought to be incorporated in an appropriate assignment of quantum state. Thus, we are led into assigning the state $|b\rangle$ to the period of time preceding the observation of F yielding the eigenvalue b.

From a purely operational point of view, one might eschew the assignment of quantum states to physical systems altogether and instead rely entirely on probabilistic statements referring to carefully defined ensembles. However, as long as one does assign quantum states to physical systems, it appears defensible to do so either in reliance on the (complete) observation immediately preceding (as is customary) or on the one next following, depending on circumstances. This ambiguity indicates that the quantum state of a system, though undoubtedly containing some elements of "reality" independent of any observer, also has subjective aspects.

We shall conclude this section by pointing out that, in general, the dispersion of probabilities of the outcome of one particular observation will be minimized (i.e., the "negative entropy" associated with this dispersion will be maximized) if we use all information about the system's past and future. This statement is a direct consequence of the properties of the entropy function to be found, e.g., in Khinchin. [6] Hence, if both the initial and final state of a system are known, use of the prediction formulas (2.1) or (2.3) instcad of (2.1) will lead to a loss in precision of the probabilistic statement concerning the intermediate observation.

28.6.4 IV. Direct Prediction

By now we have established that the conventional prediction formulas can be recovercd from the timesymmetric expressions (2.4) by means of a model that consists of shielding events close at hand from the terminal selection on which (2.4) is based by the interposition of a series of "coherence destroying" experi-

[86] A. I. Khinchin, Mathematical Foundations of Information Theory, transl. by R. A. Silverman and M. D. Friedman (Dover Publications, Inc., New York, 1957).

ments. Each measurement constitutes an interference with the physical system which destroys in a limited and mathematically well-described manner its dynamic behavior as an isolated system.

Normally, the prediction formula (2.1) and its corollary (2.3) are not conceived of as depending on carefully managed follow-up maneuvers, but are assumed to be independent of the subsequent history of the system. That this prediction theory is indeed logically independent of the time-symmetric formula (2.4) may be deduced immediately from the circumstance that in our universe the prediction formula is considered to be universally valid, whereas the timereflected formula, the retrodiction formula, is not.

Consider an ensemble of similar physical systems of arbitrary provenance and select a sample on the strength of a single complete measurement. The conventional theory of measurement then furnishes us, with respect to this selected subensemble, with relative frequencies of outcomes of a subsequent measurement or of a subsequent serics of measurements, regardless of the events that may have preceded the initial selection procedure, as well as of those events that follow on the heels of the specified series of measurements, as long as no further selection is involved. The reverse theory would have to concern itself with the probability of the outcome of certain measurements on an ensemble of similar physical systems, the ensemble to be determined solely on the basis of a pure-state selection immediately following the specified series of measurements; the expression for the probabilities should contain no reference to any events following the terminal selection, nor to the manner in which physically similar systems were collected prior to the onset of the series of measurements. Clearly, in our universe no such "retrodiction theory" would be valid: Suppose we constructed a monochromatic and well-collimated beam of particles possessing nonzero spin, performed some observation referring to the spin distribution of the beam, and then followed up with a Stern-Gerlach experiment singling out those particles in the beam being in a very definite spin state. Suppose we ask for the percentage of particles, from among those passing the postselection test, that had specified outcomes in the antecedent experiment (which should refer to an observable not possessing the specified final state as an eigenstate); surely these probabilities would not be independent of the state of polarization of our beam prior to the performance of the first experiment.

We conclude, therefore, that in order to recover the conventional prediction statement from the timesymmetric formulas of Sec. II, we must adopt a postulate that is logically independent of the timesymmetric theory; the postulate that in our universe ensembles chosen on the basis of an initial complete measurement alone possess unambiguous and reproducible probability characteristics. Once we adopt this
postulate the conventional prediction formulas (2.1), (2.3) follow from the time-symmetric formula (2.4) and from the considerations of Sec. III. We found in that section that there are "coherence destroying" procedures that make the "prediction" expressions (2.6) independent of the particular postselection we choose to perform. But if there are methods by which we can make our probabilities independent of the manner of postselection and if, by our new postulate, there exist unambiguous probabilities even in the absence of any postselection, then these two sets of probabilities should be equal.

Logically, it is conceivable that the time reverse of our new postulate should also hold; this would mean that postselection alone results in an ensemble with well-defined and reproducible probability characteristics. Actually we know that in our universe this proposition is untrue. We are thus confronted with an indubitable asymmetry in time direction. It remains to discuss whether this asymmetry is a property of microphysics proper or whether it represents the intrusion of the macroscopic universe on the microscopic scene. Granting that this question does not lend itself to straightforward logical analysis, it appears to us that the construction of ensembles in the real physical universe is a macroscopic operation and that it depends on the realities of the universe as a whole. Let us return once more to our beam of particles endowed

with spin.

If we attempt to analyze the different manner in which past and future histories affect its present characteristics, we find that no matter how we gather our beam, its constituent particles have come from one or several "sources" (e.g., a laboratory device, a distant galaxy, etc.), which determine its properties; there simply is no way of avoiding preselection completely. On the other hand, beams are not collimated toward a "sink," unless we arrange it so in our laboratory. This asymmetry is directly associated with the fact that the origins of all kinds of radiations in the universe are spatially and temporally concentrated, and their
destinations are not. The nature of ensembles or beams actually occurring in nature is, in fact, macroscopic, not microscopic; it is determined by the saine cause as all macroscopic irreversibility, conceivably by the expansion of the universe. [1]

As for the microscopically determined aspects of quantum measurements, we believe that they can be fairly summarized by the statement that in timesymmetrically constructed ensembles the laws of probability are also time symmetric; further, that to the extent that retrodiction situations may be said to exist, they obey the same laws as the corresponding prediction situations.

28.7 V.6 Lyapounov Variable: Entropy and Measurement in Quantum Mechanics

ABSTRACT We discuss the question of the dynamical meaning of the second law of thermodynamics in the framework of quantum mechanics. Previous discussion of the problem in the framework of classical dynamics has shown that the second law can be given a dynamical meaning in terms of the existence of so-called Lyapounov variables-i.e., dynamical variables varying monotonically in time without becoming contradictory. It has been found that such variables can exist in an extended framework of classical dynamics, provided that the dynamical motion is suitably unstable. In this paper we begin to extend these results to quantum mechanics. It is found that no dynamical variable with the characteristic properties of nonequilibrium entropy can be defined in the standard formulation of quantum mechanics. However, if the Hamiltonian has certain well-defined spectral properties, such variables can be defined but only as a nonfactorizable superoperator. Necessary nonfactorizability of such entropy operators M has the consequence that they cannot preserve the class of pure states. Physicaliy, this means that the distinguishability beiween pure states and corresponding mixtures must be lost in the case of a quantal system for which the algebra of observables can be extended to include a new dynamical variable representing nonequilibrium entropy. We discuss how this result leads to a solution of the quantum measurement problem. It is also found that the question of existence of entropy of superoperators M is closely linked to the problem of defining an operator of time in quantum mechanics.

28.7.1 1. Introduction

No other question in theoretical physics seems to have caused as much controversial discussions over as long a period of time as the question of the dynamical meaning of irreversibility expressed in the second law of thermodynamics. With the advent of quantum mechanics and the discovery of the apparently irreversible exponential decay of unstable particles, this question has gained added theoretical importance. Irreversibility is now an essential feature of gross macroscopic phenomena such as the familiar transport processes and it also seems to be in-

[87] H. Margenau, Phil. Sci. 30, 1 (1963); Ann. Phys. (N. Y.) 23 469 (1963). Further references are to be found in these two papers

trinsic in such basic processes as the "wave packet reduction" caused by measurement and the decay of unstable particles.

The difficulties encountered by the traditional approach to the problem of the dynamical meaning of the second law are well known (1). In this paper we shall discuss this question in the framework of quantum dynamics from the alternative viewpoint that has emerged from our previous work (1-4). This discussion will lead to the conclusion that the second law can be interpreted as a dynamical principle in an extended framework of quantum dynamics without involving contradictions and that thus interpreted it implies the loss of distinguishability between pure states and mixtures for systems to which the second law applies.

As is well known, a fundamental distinction is made in

The publication costs of this article were defrayed in part by page charge payment. This article must therefore be hereby marked advertisement " in accordance with 18 U. S. C. $1734 solely to indicate this fact.

quantum mechanics between pure states (usually represented by unit vectors of a Hilbert space) and the mixtures represented by the so-called density operators. The pure states occupy a privileged position in the theory: the quantum superposition principle holds between the pure states; dynamical evolution, as described by the Schrödinger equation, transforms pure states into pure states and the observables of the theory correspond to self-adjoint operators that again map pure states into pure states. The basic laws of quantum mechanics can thus be formulated without ever invoking the notion of mixtures and their representation by density operators. The use of this notion is generally believed to reflect incompleteness of knowledge about the system and it is considered to be only a matter of practical convenience or approximation.

The fundamental distinction between the pure states and mixtures and the privileged position of the pure states are, however, not maintained in measurement processes. As von Neumann's by now "classical" analysis has shown, we have, in addition to the deterministic and reversible evolution of the pure states into pure states described by the Schrödinger equations, the peculiar evolution, called "the reduction of the wave packet," which occurs during measurement processes. This latter evolution is irreversible and typically transforms pure states into mixtures.

Obviously, one can not accept such a dualism of state-evolution as final, and various authors have attempted to overcome it. (We do not intend to survey these attempts here; an excellent account of the subject can be found in ref. 5.) Let us only emphasize here that it is the presumed distinguishability between the pure state (which the Schrödinger equation would predict for the object + apparatus system) and the mixture that arises from the wave packet reduction that is at the root of the conceptual problems posed by quantum theory of measurement. This dualism of state-evolution could be avoided if one could formulate a physical principle that implies the loss of distinguishability between the pure states and the corresponding mixtures in the case of sufficiently complex systems capable of serving as measuring and recording apparatus (6). The main finding of our paper is that the second law of thermodynamics, when suitably interpreted as a dynamical principle, is just the physical principle that leads to the desired loss of distinguishability between the pure states and mixtures.

Before we discuss further our conclusions, it will be useful to consider briefly the problem of irreversibility in classical dynamics. Obviously, the simplest dynamical interpretation of the second law would be to require the existence of a dynamical variable with the characteristic properties of en-tropy-in particular, the property of monotonic variation with time. However, Poincar (7) has pointed out that such a dy-

namical variable can not exist within the class of standard dynamical variables of classical

[8†] Also at the University of Texas at Austin, Center for Statistical Mechanics and Thermodynamics, Austin, TX 78712.

[F] Postal address: campus plaine ULB, Boulevard du Triomphe, 1050 Bruxelles, Belgique.

mechanics (i.e., the class of functions on phase space). This seemed to exclude the possibility of interpreting the second law as a dynamical principle.

Our recent work (2-4), however, shows that this difficulty can be bypassed in an extended framework of dynamics. Briefly, our approach links the existence of a dynamical variable having the properties of nonequilibrium entropy to the presence of instabilities of dynamical motion. For systems presenting sufficiently strong instabilities of motion the notion of phase space trajectories loses operational meaning, and dynamics has to be formulated in terms of the motion of distribution functions on phase space. The dynamical variable can correspond now to more general operators (acting on the distribution functions) than just the multiplication operators by phase functions. In this extended framework the second law may be interpreted as requiring the existence of operators M (called Lyapounov variables) such that

$$\langle \rho_t, M\rho_t \rangle \tag{1.1}$$

varies monotonously with time t as the distribution functions ρ_t evolve according to the Liouville's equation:

$$i\frac{\partial \rho_t}{\partial t} = L\rho_t \tag{1.2}$$

Naturally, not all dynamical systems allow the existence of Lyapounov variables M. As expected, it iums out ilat a suitable degree of dynamical instability (for instance, "mixing instability") is necessary for the existence of M (3). More importantly, it is found that there is a well-defined class of dynamical systems (so-calied $\bar{K}$-filows) for which the L yapounov variables exist. In this case one can define a (self-adjoint) operator T representing "internal time" of the system which is "canonically conjugate" to the generator L of dynamical evolution:

$$i[L, T] = I \tag{1.3}$$

and Lyapounov variables M then can be obtained as monotone positive operator functions of T. The Lyapounov variables M may, under suitable conditions, lead further to (nonunitary) invertible similarity transformations Λ defined as

$$\Lambda = M^{1/2} \tag{1.4}$$

which convert the original deterministic evolution described by the Liouville equation into the stochastic evolution of a Markov process satisfying an H theorem of the Boltzmann type. We have exhibited examples of this possibility (4).

One thus begins to see how the second law can be formulated as a dynamical principle in terms of the existence of Lyapounov variables and the important implications of the existence of such variables. In particular, one begins to see the close links among intrinsic irreversibility (expressed in terms of the existence of M), inherent randomness (expressed in terms of the existence of Λ which converts the dynamical evolution to the evolution of a stochastic process), and the instabilities of dynamical motion. In this paper we make a start to extend these results to quantum mechanics.

We show in Section 2 that, under fairly general conditions, no entropy operator or Lyapounov variable can be defined in the standard framework of quantum mechanics. This is a consequence of the fact that in the standard formulation the generator of the time evolution group is also the operator representing the energy observable and hence is required to be bounded from below. This result is the quantum analogue of Poincar's conclusion that entropy cannot be defined as a phase function in classical mechanics.

The limitation of Section 2 does not apply if the quantum mechanical Liouville equation is taken as the basic equation

of motion because the Liouvillian operator need not be semibounded. It is found (Section 3) that, if the Liouville operator L (or equivalently the Hamiltonian) has certain well-defined spectral properties, then Lyapounov variables exist as "super operators" (i.e., as operators acting on the space of density operators). They cannot exist, however, even as superoperator for all systems. In particular, they do not exist for quantum systems of finite number of particles enclosed in a finite volume. In this respect the situation in quantum mechanics differs fundamentally from that in classical mechanics. Lyapounov variables exist, for instance, for the classical system of a finite number of hard spheres enclosed in a finite box because this system is known to satisfy the K-flow condition.

As a side remark let us add that this disparity in behavior (with regard to irreversibility) of the classical and quantum systems argues against the plausibility of "hidden variable theories" of quantum mechanics. This point is further developed in a forthcoming publication (8).

The essential point about the entropy superoperators M is that they are necessarily "nonfactorizable" and they cannot preserve the class of pure states. These results are proved in Section 4. Physically this means that, for systems whose algebra of observables can be extended to include a new dynamical variable representing nonequilibrium entropy, the distinguishability between pure states and mixtures must be lost. This opens the way to reconciling the two types of evolution distinguished by von Neumann in his analysis of measurement processes. The measurement process involves always a dynamical system (namely, the measuring + recording apparatus) for which the requirement of the second law-in the existence of an entropy superoperator-is satisfied. But this implies that the distinction between pure states and mixture is lost in measurement processes.

Let us mention that in previous work (2,9) it has been emphasized that kinetic theory leading to description of irreversible phenomena can only be developed on the level of mixture and it involves nonfactorizable superoperators. We begin to see now the deeper justification for this.

28.7.2 2. Incompatibility between the Existence of Entropy Operator and the Semiboundness of Generator of Time-evolution

Let us start by showing that in order to define an observable with the characteristic property of nonequilibrium entropy it is necessary to go beyond the standard formulation of quantum mechanics in which the Hamiltonian operator H is the generator of dynamical evolution. Suppose that there exists an operator M in the Hilbert space of pure states that represents nonequilibrium entropy. The requirement that M increases monotonically with time then translates into the condition:

$$i[H, M] = D \geq 0 \tag{2.1}$$

The operator D can now be interpreted as the entropy production operator, and it seems natural io suppose that the measurements of M and D are mutually compatible. This implies

$$[M, D] = 0 \tag{|2.2|}$$

The basic reason why conditions 2.1 and 2.2 cannot be satisfied by an operator M (except in the trivial case $D = 0$) is that the Hamiltonian operator H plays a dual role in quantum mechanics: it is the generator of the time-evolution group and it also represents the energy of the system. Hence, it must be bounded from below: $H \geq 0$.

Before proceeding to show the incompatibility of conditions 2.1 and 2.2 (with $D \neq 0$) with the semiboundedness of the Hamiltonian, let us remark that the operators involved in conditions 2.1 and 2.2 are in general unbounded. To obtain reasurably meaningful results it is

thus necessary to make the formal commutation conditions 2.1 and 2.2 more precise by making appropriate assumptions about the domains of definition of the involved operators. We need not discuss this question in detail here. Let us only mention that the argument given below is rigorously valid if (i) M is bounded and self-adjoint, (ii) $MD_H \subseteq D_H$, where D_H denotes the domain of H, and (iii) condition 2.2 is interpreted to mean that the operator DM is an extension of $MD : MD \subset DM$. Naturally, these conditions are not necessary but only sufficient to establish the incompatibility of conditions 2.1 and 2.2 with the semiboundedness of $\boldsymbol{H}$.

For instance, this incompatibility follows also even for unbounded M provided that suitable assumptions are made on the domain of M. But we do not discuss such generalizations here because they do not bring any essentially new point.

Returning to the proof of incompatibility, let us consider the identity

$$\frac{d}{dt}\left\langle e^{-iMt}\psi, He^{-iMt}\psi\right\rangle = -i\left(e^{-iMt}\psi, \mid H, M\right] e^{-iMt}\psi\Big) \tag{2.3}$$

which can be easily verified to hold for all ψ in the domain $\mathscr{D}_H$ of H. To be more explicit, using the previously stated conditions on the domain of H and condition $\overline{2}.\overline{2}$, one can verify the following: (i) for all $\psi \in \mathscr{D}_H, e^{-iMt}\psi$ also belongs to $\mathscr{D}_H$; (ii) for $\psi \in D_H, \left\langle e^{-iMt}\psi, He^{-iMt}\psi\right\rangle$ is differentiable with respect to T with its derivative given by identity 2.3.

Because the bounded self-adjoint operator M commutes with the self-adjoint operator D, by assumption it follows that $e^{iMt}De^{-iMt} = D$. Thus, identity 2.3 reduces to the equality:

$$\frac{d}{dt}\left\langle e^{-iMt}\psi, He^{-iMt}\psi\right\rangle = -\langle\psi, D\psi\rangle. \tag{\{2.4\}}$$

Integration of both sides of equality 2.4 from 0 to $t \geq 0$ yields

$$\left(e^{-iMt}\psi, He^{-iMt}\psi\right\rangle - \langle\psi, H\psi\rangle = -t\langle\psi, D\psi\rangle$$

or,

$$\langle\psi, H\psi\rangle = t\langle\psi, D\psi\rangle + \left\langle e^{-iMt}\psi, He^{-iMt}\psi\right\rangle$$
$$\text{for } \psi \in D_H.$$

Because $H \geq 0$, we have for all $\psi \in D_H$ and all $t \geq 0$,

$$\langle\psi, \mathbf{H}\psi\rangle \geq t\langle\psi, D\psi\rangle \tag{2.5}$$

or $1/t\langle\psi, H\psi\rangle \geq \langle\psi, D\psi\rangle$ for all $\psi \in \mathscr{D}_H$ and all $t \geq 0$. Letting $t \to \infty$ we then obtain $\langle\psi, D\psi\rangle \leq 0$ for a dense set of vectors; or $D \leq 0$.

At this point we may use the assumption that $D \geq 0$ and reach the desired conclusion $D = 0$. However, it is important to note that this conclusion does not depend on the positivity of D but follows only from condition 2.2 and the semiboundedness of H. To see this, we now integrate equality 2.4 from $-t$ to 0 and obtain, as before, the inequality:

$$\langle\psi, H\psi\rangle \geq -t\langle\psi, D\psi\rangle \tag{2.6}$$

for all $\psi \in D_H$ and all $t \geq 0$.

The inequality 2.6 together with the previously reached conclusion that $D \leq 0$ now proves that $D \equiv 0$. This shows that, in order to be able to define a new dynamical variable M representing nonequilibrium entropy, it is necessary to go beyond the standard formulation of quantum mechanics. Although the property of monotonic increase of entropy (i.e., the condition $D \geq 0$) does not play any role in reaching this conclusion, we shall see that it plays an essential role in establishing the important conclusion that the existence of an entropy "superoperator" implies the loss of distinction between pure and mixed states.

From a purely mathematical point of view, the result just obtained generalizes a result of Putnam (10). In fact, Putnam has shown that condition 2.2 together with the assumption that H is bounded implies that $D = 0$. Here we have generalized this result to semibounded H. Moreover, this generalization is "maximal" in the sense that the theorem fails to hold if the condition of semiboundedness of H is dropped. As discussed below, this fact allows the possibility of constructing Lyapounov variables or entropy operators in the Liouvillian formulation of dynamics.

There is an interesting connection between the nonexistence of entropy operator M in $\mathscr{H}$ and the impossibility [noted by Pauli (11)] of defining an operator of time in the usual formulation of quantum mechanics. Such an operator of time would be, by definition, a self-adjoint operator T which is canonically conjugated to the generator $\boldsymbol{H}$ of the time-evolution group; or

$$[H, T] = iI \tag{2.7}$$

However, as shown in ref. 3, if such a T exists then one can obtain an entropy operator M satisfying conditions 2.1 and 2.2 by simply taking $\boldsymbol{M}$ to be a monotonic operator function of T : M = f(T). One thus obtains yet another proof of Pauli's remark that there can be no operator T in the standard formulation of quantum mechanics. Let us also mention that more recent attempts to define a more general concept of operator T that need not be self-adjoint or satisfy condition 2.7 still conflict with the fact that the generator of motion is the Hamiltonian operator and hence is bounded from below (cf. ref. 12).

The impossibility of defining the entropy operator M, the nonexistence of time operator in the standard formulation of quantum mechanics, and the problem of interpreting and justifying the time-energy uncertainty relationship are thus all linked. Their common origin is the fact that in the usual formulation of quantum mechanics the generator H of the timetranslation group is identical with the energy operator of the system. To be able to define the entropy operator M it is thus necessary to overcome this degeneracy. The simplest way of achieving this is to go to the so-called Liouvillian formulation of (quantum) dynamics. The basic object in this formulation is the group describing the time evolution of the density operators. Under dynamical evolution, an initial density operator ρ is transformed in time t to the density operator $e^{-iHt}\rho e^{iHt}$. Therefore the generator of the time-translation group is now the Liouvillian operator L defined by the equation:

$$L\rho = [H, \rho]. \tag{2.8}$$

In the following section we investigate the existence and properties of entropy operator M in the Liouvillian formulation of quantum dynamics.

28.7.3 3. The Entropy Superoperator

The important advantage gained in going to the Liouvillian formulation of quantum dynamics is that the generator I. of the time-translation group is no longer physically required to be bounded from below. In fact if the spectrum of H extends from 0 to $+\infty$ the spectrum of L is the entire real line. The possibility of defining M as a superoperator (i.e., an operator acting on the space spanned by density operators) satisfying the relationships

$$i[L, M] = D \geq 0 \tag{3.1}$$

and

$$|\ M, D] = 0 \tag{3.2}$$

is thus not excluded by the argument given in the preceding section.

Naturally, one does not expect M to exist, even as a superoperator, for all dynamical systems. Let us recall that in classical mechanics the existence of M is always associated with certain strong instability properties of dynamical motion, which is related to certain well-defined spectral properties of the Liouvillian.

One expects similar conclusions in quantum mechanics. Let us first note that an entropy superoperator (or, equivalently, a Lyapounov variable) cannot exist in either of the following cases: (i) the Hamiltonian H has purely discrete spectrum; and (ii) H has bounded spectrum.

The first of these statements follows from the fact that, if H has purely discrete spectrum, then so does L (considered as a self-adjoint operator acting on the Hilbert space of the Hilbert-Schmidt operators. On the other hand, it has been shown that, if a pair of self-adjoint operators M and L satisfy relationship 3.1, then the eigenvectors of L belong to the null space $D(3)$. Thus, if L has a purely discrete spectrum its eigenvectors will span the entire space and D will vanish identically. Similarly, the second statement follows from the fact that, if H is bounded, then so is L. The argument of the preceding sections for the earlier result of Putnam (10)] now shows that, for bounded L, condition 3.2 can not be satisfied unless $D = 0$.

The physical meaning of the statements just proved is that an entropy superoperator can not exist for quantum systems consisting of finite numbers of particles enclosed in a finite volume (because the Hamiltonian has a discrete spectrum in this case) or in theories relying on finite cutoff energy. In quantum mechanics, it is only in the limit of infinite systems that irreversibility expressed in the second law of thermodynamics may become manifest. This is in marked contrast to the situation in classical mechanics. As shown (3), entropy operators can be constructed in classical mechanics for a class of systems which includes, for instance, the system of a finite number of hard spheres enclosed within a finite box. This shows that conceptually the problem of irreversibility in quantum mechanics is more involved than in classical mechanics.

A sufficient condition for the existence of M as a superoperator is that the Hamiltonian H has an absolutely continuous spectrum extending from 0 to $+\infty$. To see this, it may be observed that this condition on H implies that the corresponding Liouvillian has an absolutely continuous spectrum of uniform (actually infinite) multiplicity extending over the entire real line (M. Courbage and B. Misra, unpublished). Under this condition there always exists a self-adjoint operator T which is "canonically conjugate" to L. In fact, in the spectral representation (or direct integral representation) that "diagonalizes" L to make it correspond to the multiplication operator by the real variable λ this operator T can be taken to be the differentiation operator $id/d\lambda$. As mentioned before, monotonically increasing operator functions of T then satisfy defining conditions 3.1 and 3.2 for M.

A consequence of this remark is that the system of a single free particle in infinite volume admits an entropy superoperator, because the Hamiltonian $H = P2/2m$ obviously has an absolutely continuous spectrum extending over the entire interval $[0, +\infty]$. But one does not expect any physical irreversibility for this system. The spurious "irreversibility" associated with the evolution of the free particle in infinite volume is just a reflection of the fact that initially localized wave packets spread out and get rarified with the particle, eventually "escaping to infinity."

Naturally, one would like to distinguish such spurious cases from more physical irreversibility by requiring M to satisfy supplementary physically motivated conditions. We shall not discuss this question in detail here. However, let us mention that we have studied (4) the requirement that the square root $M^{1/2}$ of the Lyapounov variables of classical systems, as well as the semigroup $\Lambda e^{-iLt}\Lambda^{-1}, (t \geq 0)$, preserve the positivity of distribution functions on phase space. The physical meaning of this is as follows. Dynamical evolutions admitting the existence of such Lyapounov variables are intrinsically random in the sense that a change of representation effected by this (invertible) transformation Λ converts the original dynamical

evolution into the evolution of the stochastic Markov process. In quantum mechanics, one may formulate a corresponding requirement on the entropy operator M or, more accurately, on the Lyapounov variable $M^{-1} = M'$. In other words, one would require of the Lyapounov variable M' that its square root Λ' as well as the semigroup $\Lambda' e^{-itL}\Lambda'^{-1}$ (for $t \geq 0$) map density operators (positive operator with trace 1) to density operators. The physical meaning of the existence of such a Lyapounov variable is the same as in classical mechanics: it means that the quantum Liouvillian evolution in question is equivalent, through an invertible similarity transformation, to the evolution of a quantum stochastic Markov process.

A detailed discussion of how the measurement process can be adequately described in terms of the quantum stochastic processes obtained, through similarity transformation, from the Liouvillian evolution of the object + apparatus system will be presented elsewhere. Here we shall only show that the supposed distinguishability between the pure states and mixtures and the privileged position of the pure states in the usual formulation of quantum mechanics-the two facts that are at the root of the conceptual difficulties posed by the phenomena of wave packet reduction-must necessarily be given up in the case of physical systems, for which entropy superoperators exist. To this end, let us show that the entropy superoperators are necessarily nonfactorizable.

28.7.4 4. Nonfactorizability of Entropy Superoperators

Nonfactorizability of an entropy superoperator means, by definition, that $M\rho$ cannot be written in the form

$$M\rho = A_1 \rho A_2 \tag{4.1}$$

where A_1 and A_2 are two ordinary Hilbert space operators acting on the same Hilbert space on which ρ acts. We shall show that if a positive and hermiticity-preserving superoperator M satisfies conditions 3.1 and 3.2 and is factorizable (i.e., satisfies Eq. 4.1), then $D = 0$. Let us recall that the positivity- and her-miticity-preserving conditions on superoperator M mean, respectively, that

$$\mathrm{Tr}\,(\rho^* M\rho) \geq 0 \tag{4.2}$$

and

$$\rho = \rho^* \text{ implies } M\rho = (M\rho)^*$$

These are natural requirements to impose on the entropy superoperator M. They lead to the simplification that, if a factorizable superoperator M satisfies them, then $M\rho$ can be written in the form

$$M\rho = A\rho A \tag{\{4.3\}}$$

where A is a positive operator. It will thus suffice to show that conditions 3.1, 3.2, and 4.3 together imply that $D = 0$.

Now it follows from the positivity of D (condition 3.1) and the assumed form 4.3 for M that

$$i[H, A] \equiv B \geq 0. \tag{4.4}$$

To see this, let us compute the action of D on density operators of the form

$$\rho_\phi = |\phi\rangle\langle\phi|$$

with ϕ in the domain D_H of H. Using definition 2.8 of L and form 4.3 for M, one easily verifies that

$$D_{l_\phi} = i|LM - ML| \mid \phi > < \phi \mid$$
$$= |B\phi >< A\phi| + |A\phi >< B\phi| \tag{4.5}$$

Positivity of D then implies that

$$\mathrm{Tr}\,(\rho_\psi D \rho_\phi) = g(\phi, B\phi\rangle\langle\phi, A\phi\rangle \geq 0$$

Because $A \geq 0$ it follows that $B \geq 0$.
In the same way, computing $\mid D, M] \mid \phi > \langle\psi|$ and setting it equal to 0 (condition 3.2), one finds that

$$\left|[|H, A|, A]\phi > \left\langle A^2\psi\right| = \right| A^2\phi\rangle \langle[|\ H, A], A]\psi \mid \tag{4.6}$$

for all ϕ, ψ in the dense set $\mathscr{D}_H$. But this means

$$[(\boldsymbol{H}, \boldsymbol{A}), \boldsymbol{A}]_\phi = \boldsymbol{C}\boldsymbol{A}^2\phi$$

with

$$C = \langle[|H, A|, A]\psi, \psi\rangle / \left\langle A^2\psi, \psi\right\rangle$$

a real number independent of ϕ. Thus

$$[|\ \mathbf{H}, \mathbf{A}], \mathbf{A}] = C\mathbf{A}^2$$

with C a real number; or

$$i|B, A| = -CA^2 \tag{4.7}$$

Since $B \geq 0$ (relationship 3.4) and $-CA^2$ obviously commutes with A, the argument of Section 2 applies with B taking the role of H, A that of M, and $-CA^2$ that of D. Thus, we conclude that $-CA^2 = 0$. Now, there are two cases: (i) if $C \neq 0$, we conclude that $A^2 = 0$ and hence $A = 0$ with the result that M given by form 4.3 and, a fortiori, D vanish; (ii) if $C = 0$, then $B = i \mid H,\ A \mid$ and A commutes and again the argument of Section 2 applies, leading to the conclusion that $B = 0$. This then implies (relationship 4.5) that $D = 0$. Let us remark that, unlike the argument of Section 2, the proof of the nonfactorizability of the entropy operator makes essential use of the positivity, or rather definiteness in sign, of entropy production operator D.

The nonfactorizability of M has the important consequence that M can not preserve the purity of states. In fact, if M were to map pure states $|\phi\rangle\langle\phi|$ into operators of the same form it would follow that M would also map positive operator to positive operators. Such a purity- and positivity-preserving map M is, however, one of the following three forms (13): (i) M is factorizable; (ii) $M\rho = A'\rho^* A'^*$ with A' an antilinear operation of $H; (iii) M\rho = \mathrm{Tr}(\rho B).|\psi >< \psi|$ when B is a fixed positive operator and ψ is a fixed vector. But the entropy superoperator cannot be any of these forms. Case i is already ruled out. To rule out case ii, let us consider the operator M^2 which, as it can be verified easily, is factorizable. On the other hand, as the entropy superoperator M satisfies conditions 3.1 and 3.2, M^2 satisfies $i\,|L, M^2| \equiv D' \equiv 2DM = 2M^{1/2}DM^{1/2} \geq 0$ and $|M^2, D'| = 0$. Thus, M^2 is also an entropy superoperator and hence it can not be factorizable. Finally, this entropy superoperator can not be of the form iii because in this case M, being an operator of rank l, will have a purely discrete spectrum. This, however, contradicts the easily verified fact that entropy superoperators can not have a purely discrete spectrum.

28.7.5 5. Concluding Remarks

The preceding considerations lead up to the following conclusions. For an infinite quantal system, there exists the possibility of enlarging the algebra of observables to include an operator M representing nonequilibrium entropy. The operator M can be defined, however, only as a nonfactorizable superoperator. The inclusion of a (necessarily nonfactorizable) entropy operator among the observables thus entails that the pure states lose their privileged position in theory and that the pure and mixed states be treated on equal basis. Physically, this means that, for systems having entropy as an observable, the distinction between the pure and mixed states must cease to be operationally meaningful and there would be limitations on the possibility of realizing coherent superposition of quantum states.

Evidently this conclusion, which is reached here as a logical consequence of our theory of entropy operator, should be further elucidated by an analysis of the physical reason for the loss of the distinction between pure and mixed states.

The corresponding situation for classical systems has been discussed elsewhere (1, 3, 4). In those papers, the existence of an entropy superoperator implies that the phase space trajectories cease to be physically observable. The physical reason for this is linked to the instability of dynamical motion, which is a necessary condition for the existence of an entropy superoperator or a Lyapounov variable.

One would expect a suitable quantum analogue of the instability mechanism to operate for quantal systems (admitting the existence of Lyapounov variables) which is responsible for the loss of physical distinction between pure states and mixtures.

A detailed formulation of the instability mechanism in quantum mechanics is work for the future. It remains, nevertheless, a remarkable fact that, when interpreted as a dynamical principle in terms of the existence of Lyapounov variables or entropy operator M, the second law of thermodynamics implies the loss of distinction between pure states and mixtures. This provides the way to a resolution of the duality of state evolution considered in the "orthodox" theory of measurement by von Neumann.

Finally, the approach to the measurement problem which emerges from this paper is in accord with the often repeated observation by Bohr that any correct account of a measurement process must take into consideration two important facts: irreversibility of measurement processes and the classical nature of measuring apparatus. Our approach links these two features. We show that irreversibility (expressed by the existence of entropy superoperator M for the measuring apparatus) implies the classical nature of apparatus in that the distinction between pure and mixed states is lost.

1. Prigogine, I (1979) Order and Fluctuations in Equilibrium and Nonequilibrium Statistical Mechanics, 17th International Solvay Conference in Physics, Brussels, $20-24$ November 1978, in press.

2. Prigogine, I., George, C., Henin, F. & Rosenfeld, L. (1973) Chem. Scr. 4, 5-32.

3. Misra, B. (1978) Proc. Natl. Acad. Sci. USA 75, 1627-1631

4. Misra, B., Prigogine, I. & Courbage, M. (1979) Proc. Natl. Acad. Sci. USA 76, 3607-3611.

5. d'Espagnat, B. (1976) Conceptual Foundations of Quantum Mechanics (Benjamin, Menlo Park, CA), 2nd Ed

6. Wigner, E. P. (1963) Am. J. Phys. 31, 615.

7. Poincar, H. (1889) C. R. Hebd. Seances Acad. Sci. 108, 550553.

8. George, C. & Prigogine, I. (1979) Physica, in press.

9. George, C., Prigogine, I. & Rosenfeld L. (1972) K. Dan. Vidensk. Selsk. Mat-fys. Meddel 38, 1-44.

10. Putnam, C. R. (1967) Communication Properties of Hilbert Space Operators (Springer, New York), Theorem 1.6.3., p. 12.

11. Pauli, W. (1958) in Encyclopedia of Physics, ed. Flgge, S. (Springer, Berlin), Vol. 5.

12. Misra, B. & Sudarshan, E. C. C. (1977) J. Math. Phys. 18, 756-763 (see especially p. 762).

13. Davies, E. B. (1976) Ouantum Theory of Open Systems (Academic, New York), Theorem 3.1, p. 21.

28.8 Teleporting An Unknown Quantum State Via Dual Classical and Einstein-podolsky-rosen Channels by Bennett, Brassard, Crépeau, Jozsa, Peres, Wootters

Abstract

An unknown quantum state $|\phi\rangle$ can be disassembled into, then later reconstructed from, purely classical information and purely nonclassical EPR correlations. To do so the sender, "Alice," and the receiver, "Bob," must prearrange the sharing of an EPRcorrelated pair of particles. Alice makes a joint measurement on her EPR particle and the unknown quantum system, and sends Bob the classical result of this measurement. Knowing this, Bob can convert the state of his EPR particle into an exact replica of the unknown state $|\phi\rangle$ which Alice destroyed.

The existence of long range correlations between Einstein-Podolsky-Rosen (EPR) [1] pairs of particles raises the question of their use for information transfer. Einstein himself used the word "telepathically" in this context [2]. It is known that instantaneous information transfer is definitely impossible [3]. Here, we show that EPR correlations can nevertheless assist in the "teleportation" of an intact quantum state from one place to another, by a sender who knows neither the state to be teleported nor the location of the intended receiver.

Suppose one observer, whom we shall call "Alice," has been given a quantum system such as a photon or spin- $\frac{1}{2}$ particle, prepared in a state $|\phi\rangle$ unknown to her, and she wishes to communicate to another observer, "Bob," sufficient information about the quantum system for him to make an accurate copy of it. Knowing the state vector $|\phi\rangle$ itself would be sufficient information, but in general there is no way to learn it. Only if Alice knows beforehand that $|\phi\rangle$ belongs to a given orthonormal set can she make a measurement whose result will allow her to make an accurate copy of $|\phi\rangle$. Conversely, if the possibilities for $|\phi\rangle$ include two or more non-orthogonal states, then no measurement will yield sufficient information to prepare a perfectly accurate copy.

A trivial way for Alice to provide Bob with all the information in $|\phi\rangle$ would be to send the particle itself. If she wants to avoid transferring the original particle, she can make it interact unitarily with another system, or "ancilla," initially in a known state $|a_0\rangle$, in such a way that after the interaction the original particle is left in a standard state $|\phi_0\rangle$ and the ancilla is in an unknown state $|a\rangle$ containing complete information about $|\phi\rangle$. If Alice now sends Bob the ancilla (perhaps technically easier than sending the original particle), Bob can reverse her actions to prepare a replica of her original state $|\phi\rangle$. This "spin-exchange measurement" [4] illustrates an essential feature of quantum information: it can be swapped from one system to another, but it

cannot be duplicated or "cloned" [5]. In this regard it is quite unlike classical information, which can be duplicated at will. The most tangible manifestation of the non-classicality of quantum information is the violation of Bell's inequalities [6] observed [7] in experiments on EPR states. Other manifestations include the possibility of quantum cryptography [8], quantum parallel computation [9], and the superiority of interactive measurements for extracting information from a pair of identically prepared particles [10].

The spin-exchange method of sending full information to Bob still lumps classical and nonclassical information together in a single transmission. Below, we show how Alice can divide the full information encoded in $|\phi\rangle$ into two parts, one purely classical and the other purely nonclassical, and send them to Bob through two different channels. Having received these two transmissions, Bob can construct an accurate replica of $|\phi\rangle$. Of course Alice's original $|\phi\rangle$ is destroyed in the process, as it must be to obey the no-cloning theorem. We call the process we are about to describe "teleportation," a term from science fiction meaning to make a person or object disappear while an exact replica appears somewhere else. It must be emphasized that our teleportation, unlike some science fiction versions, defies no physical laws. In particular it cannot take place instantaneously or over a space-like interval, because it requires,
among other things, sending a classical message from Alice to Bob. The net result of teleportation is completely prosaic: the removal of $|\phi\rangle$ from Alice's hands and its appearance in Bob's hands a suitable time later. The only remarkable feature is that in the interim, the information in $|\phi\rangle$ has been cleanly separated into classical and nonclassical parts. First we shall show how to teleport the quantum state $|\phi\rangle$ of a spin- $\frac{1}{2}$ particle. Later we discuss teleportation of more complicated states.

The nonclassical part is transmitted first. To do so, two spin- $\frac{1}{2}$ particles are prepared in an EPR singlet state

$$\left|\Psi_{23}^{(-)}\right\rangle = \sqrt{\frac{1}{2}}\left(|\uparrow_2\rangle\,|\downarrow_3\rangle - |\downarrow_2\rangle\,|\uparrow_3\rangle\right) \tag{1}$$

The subscripts 2 and 3 label the particles in this EPR pair. Alice's original particle, whose unknown state $|\phi\rangle$ she seeks to teleport to Bob, will be designated by a subscript 1 when necessary. These three particles may be of different kinds, e.g. one or more may be photons, the polarization degree of freedom having the same algebra as a spin.

One EPR particle (particle 2) is given to Alice, while the other (particle 3) is given to Bob. Although this establishes the possibility of nonclassical correlations between Alice and Bob, the EPR pair at this stage contains no information about $|\phi\rangle$. Indeed the entire system, comprising Alice's unknown particle 1 and the EPR pair, is in a pure product state, $|\phi_1\rangle\left|\Psi_{23}^{(-)}\right\rangle$, involving neither classical correlation nor quantum entanglement between the unknown particle and the EPR pair. Therefore no measurement on either member of the EPR pair, or both together, can yield any information about $|\phi\rangle$. An entanglement between these two subsystems is brought about in the next step.

To couple the first particle with the EPR pair, Alice performs a complete measurement of the von Neumann type on the joint system consisting of particle 1 and particle 2 (her EPR particle). This measurement is performed in the Bell operator basis [11] consisting of $\left|\Psi_{12}^{(-)}\right\rangle$and

$$\left|\Psi_{12}^{(+)}\right\rangle = \sqrt{\frac{1}{2}}\left(|\uparrow_1\rangle\,|\downarrow_2\rangle + |\downarrow_1\rangle\,|\uparrow_2\rangle\right) \quad \text{and} \quad \left|\Phi_{12}^{(\pm)}\right\rangle = \sqrt{\frac{1}{2}}\left(|\uparrow_1\rangle\,|\uparrow_2\rangle \pm |\downarrow_1\rangle\,|\downarrow_2\rangle\right). \tag{2}$$

Note that these four states are a complete orthonormal basis for particles 1 and 2.
It is convenient to write the unknown state of the first particle as

$$|\phi_1\rangle = a\,|\uparrow_1\rangle + b\,|\downarrow_1\rangle \tag{3}$$

with $|a|^2 + |b|^2 = 1$. The complete state of the three particles before Alice's measurement is thus

$$|\Psi_{123}\rangle = \frac{a}{\sqrt{2}}\left(|\uparrow_1\rangle\,|\uparrow_2\rangle\,|\downarrow_3\rangle - |\uparrow_1\rangle\,|\downarrow_2\rangle\,|\uparrow_3\rangle\right) + \frac{b}{\sqrt{2}}\left(|\downarrow_1\rangle\,|\uparrow_2\rangle\,|\downarrow_3\rangle - |\downarrow_1\rangle\,|\downarrow_2\rangle\,|\uparrow_3\rangle\right). \tag{4}$$

In this equation, each direct product $|_1\rangle\,|_2\rangle$ can be expressed in terms of the Bell operator basis vectors $\left|\Phi_{12}^{(\pm)}\right\rangle$and $\left|\Psi_{12}^{(\pm)}\right\rangle$, and we obtain

$$\begin{aligned}|\Psi_{123}\rangle = \tfrac{1}{2}\Big[&\left|\Psi_{12}^{(-)}\right\rangle\left(-a\,|\uparrow_3\rangle - b\,|\downarrow_3\rangle\right) + \left|\Psi_{12}^{(+)}\right\rangle\left(-a\,|\uparrow_3\rangle + b\,|\downarrow_3\rangle\right) + \\ &\left|\Phi_{12}^{(-)}\right\rangle\left(a\,|\downarrow_3\rangle + b\,|\uparrow_3\rangle\right) + \left|\Phi_{12}^{(+)}\right\rangle\left(a\,|\downarrow_3\rangle - b\,|\uparrow_3\rangle\right)\Big].\end{aligned} \tag{5}$$

It follows that, regardless of the unknown state $|\phi_1\rangle$, the four measurement outcomes are equally likely, each occurring with probability 1/4. Furthermore, after Alice's measurement, Bob's particle 3 will have been projected into one of the four pure states superposed in Eq. (5), according to the measurement outcome. These are, respectively,

$$-\,|\phi_3\rangle \equiv -\begin{pmatrix}a\\ b\end{pmatrix}, \quad \begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}|\phi_3\rangle\,, \quad \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}|\phi_3\rangle\,, \quad \text{and} \quad \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}|\phi_3\rangle\,. \tag{6}$$

Each of these possible resultant states for Bob's EPR particle is related in a simple way to the original state $|\phi\rangle$ which Alice sought to teleport. In the case of the first (singlet) outcome, Bob's state is the same except for an irrelevant phase factor, so Bob need do nothing further to produce a replica of Alice's spin. In the three other cases, Bob must apply one of the unitary operators in Eq. (6), corresponding respectively to 180 degree rotations around the z, x, and y axes, in order to convert his EPR particle into a replica of Alice's original state $|\phi\rangle$. (If $|\phi\rangle$ represents a photon polarization state, a suitable combination of half-wave plates will perform these unitary operations.) Thus an accurate teleportation can be achieved in all cases by having Alice tell Bob the classical outcome of her measurement, after which Bob applies the required rotation to transform the state of his particle into a replica of $|\phi\rangle$. Alice, on the other hand, is left with particles 1 and 2 in one of the states $\left|\Psi_{12}^{(\pm)}\right\rangle$or $\left|\Phi_{12}^{(\pm)}\right\rangle$, without any trace of the original state $|\phi\rangle$.

Unlike the quantum correlation of Bob's EPR particle 3 to Alice's particle 2, the result of Alice's measurement is purely classical information, which can be transmitted, copied, and stored at will in any suitable physical medium. In particular, this information need not be destroyed or canceled to bring the teleportation process to a successful conclusion: the teleportation of $|\phi\rangle$ from Alice to Bob has the side effect of producing two bits of random classical information, uncorrelated to $|\phi\rangle$, which are left behind at the end of the process.

Since teleportation is a linear operation applied to the quantum state $|\phi\rangle$, it will work not only with pure states, but also with mixed or entangled states. For example, let Alice's original particle 1 be itself part of an EPR singlet with another particle, labelled 0 , which may be far away from both Alice and Bob. Then, after teleportation, particles 0 and 3 would be left in a singlet state, even though they had originally belonged to separate EPR pairs.

All of what we have said above can be generalized to systems having $N > 2$ orthogonal states. In place of an EPR spin pair in the singlet state, Alice would use a pair of N-state particles in a completely entangled state. For definiteness let us
write this entangled state as $\sum_j |j\rangle \otimes |j\rangle/\sqrt{N}$, where $j = 0, 1, \ldots, N-1$ labels the N elements of an orthonormal basis for each of the N-state systems. As before, Alice performs a joint measurement on particles 1 and 2 . One such measurement that has the desired effect is the one whose eigenstates are $|\psi_{nm}\rangle$, defined by

$$|\psi_{nm}\rangle = \sum_j e^{2\pi ijn/N}|j\rangle \otimes |(j+m) \bmod N\rangle/\sqrt{N} \tag{7}$$

Once Bob learns from Alice that she has obtained the result nm, he performs on his previously entangled particle (particle 3) the unitary transformation

$$U_{nm} = \sum_k e^{2\pi ikn/N}|k\rangle\langle(k+m) \bmod N|. \tag{8}$$

This transformation brings Bob's particle to the original state of Alice's particle 1, and the teleportation is complete.

The classical message plays an essential role in teleportation. To see why, suppose that Bob is impatient, and tries to complete the teleportation by guessing Alice's classical message before it arrives. Then Alice's expected $|\phi\rangle$ will be reconstructed (in the spin- $\frac{1}{2}$ case) as a random mixture of the four states of Eq. (6). For any $|\phi\rangle$, this is a maximally mixed state, giving no information about the input state $|\phi\rangle$. It could not be otherwise, because any correlation between the input and the guessed output could be used to send a superluminal signal.

One may still inquire whether accurate teleportation of a two-state particle requires a full two bits of classical information. Could it be done, for example, using only two or three distinct classical messages instead of four, or four messages of unequal probability? Later we show that a full two bits of classical channel capacity are necessary. Accurate teleportation using a classical channel of any lesser capacity would allow Bob to send superluminal messages through the teleported particle, by guessing the classical message before it arrived (cf Fig. 2).

Conversely one may enquire whether other states besides an EPR singlet can be used as the nonclassical channel of the teleportation process. Clearly any direct product state of particles 2 and 3 is useless, because for such states manipulation of particle 2 has no effect on what can be predicted about particle 3 . Consider now a nonfactorable state $|\Upsilon_{23}\rangle$. It can readily be seen that after Alice's measurement, Bob's particle 3 will be related to $|\phi_1\rangle$ by four fixed unitary operations if and only if $|\Upsilon_{23}\rangle$ has the form

$$\sqrt{\frac{1}{2}}\left(|u_2\rangle\,|p_3\rangle + |v_2\rangle\,|q_3\rangle\right) \tag{9}$$

where $\{|u\rangle, |v\rangle\}$ and $\{|p\rangle, |q\rangle\}$ are any two pairs of orthonormal states. These are maximally entangled states [11], having maximally random marginal statistics for measurements on either particle separately. States which are less entangled reduce the fidelity of teleportation, and/or the range of states $|\phi\rangle$ that can be accurately teleported. The states in Eq. (9) are also precisely those obtainable from the EPR singlet by a local one-particle unitary operation [12]. Their use for the nonclassical
channel is entirely equivalent to that of the singlet (1). Maximal entanglement is necessary and sufficient for faithful teleportation.

Although it is currently infeasible to store separated EPR particles for more than a brief time, if it becomes feasible to do so, quantum teleportation could be quite useful. Alice and Bob would only need a stockpile of EPR pairs (whose reliability can be tested by violations of Bell's inequality [7]) and a channel capable of carrying robust classical messages. Alice could then teleport quantum states to Bob over arbitrarily great distances, without worrying about the effects of attenuation and noise on, say, a single photon sent through a long optical fiber. As an application of teleportation, consider the problem investigated by Peres and Wootters [10], in which Bob already has another copy of $|\phi\rangle$. If he acquires Alice's copy, he can measure both together, thereby determining the state $|\phi\rangle$ more accurately than can be done by making a separate measurement on each one. Finally, teleportation has the advantage of still being possible in situations where Alice and Bob, after sharing their EPR pairs, have wandered about

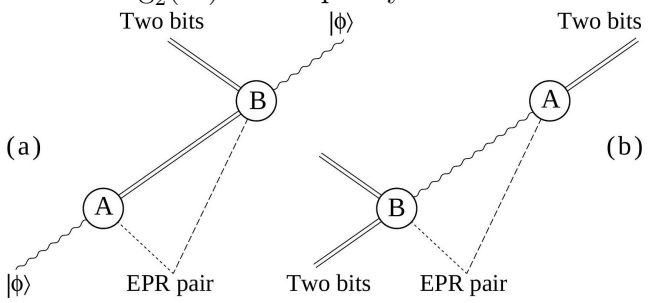
independently and no longer know each others' locations. Alice cannot reliably send Bob the original quantum particle, or a spin-exchanged version of it, if she does not know where he is; but she can still teleport the quantum state to him, by broadcasting the classical information to all places where he might be.

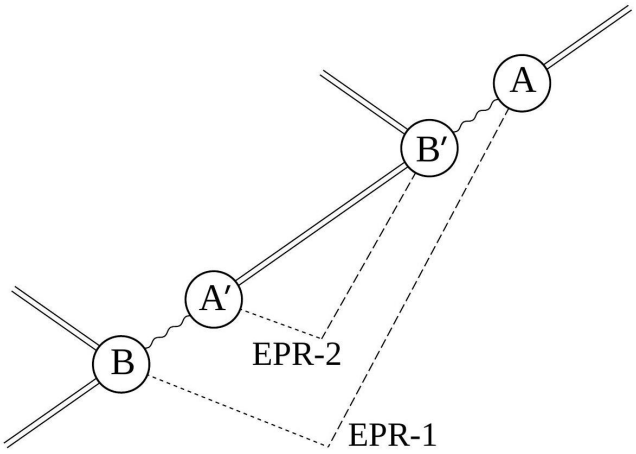
Teleportation resembles another recent scheme for using EPR correlations to help transmit useful information. In "4-way coding" [12] modulation of one member of an EPR pair serves to reliably encode a 2 -bit message in the joint state of the complete pair. Teleportation and 4 -way coding can be seen as variations on the same underlying process, illustrated by the spacetime diagrams in Fig. 1. Note that closed loops are involved for both processes. Trying to draw similar "Feynman diagrams" with tree structure, rather than loops, would lead to physically impossible processes.

On the other hand, more complicated closed-loop diagrams are possible, such as Fig. 2, obtained by substituting Fig. 1a into the wavy line of Fig. 1b. This represents a 4-way coding scheme in which the modulated EPR particle is teleported instead of being transmitted directly. Two incoming classical bits on the lower left are reproduced reliably on the upper right, with the assistance of two shared EPR pairs and two other classical bits, uncorrelated with the external bits, in an internal channel from A' to B'. This diagram is of interest because it can be used to show that a full two bits of classical channel capacity are necessary for accurate teleportation of a two-state particle (cf caption).

FIG. 1. Spacetime diagrams for (a) quantum teleportation, and (b) 4-way coding [12]. As usual, time increases from bottom to top. The solid lines represent a classical pair of bits, the dashed lines an EPR pair of particles (which may be of different types), and the wavy line a quantum particle in an unknown state $|\phi\rangle$. Alice (A) performs a quantum measurement, and Bob (B) a unitary operation.

FIG. 2. Spacetime diagram of more complex 4 -way coding scheme in which the modulated EPR particle (wavy line) is teleported rather than being transmitted directly. This diagram can be used to prove that a classical channel of 2 bits capacity is necessary for teleportation. To do so, assume on the contrary that the teleportation from A' to B' uses an internal classical channel of capacity $C < 2$ bits, but is still able to transmit the wavy particle's state accurately from A' to B', and therefore still transmit the external two bit message accurately from B to A. The assumed lower capacity $C < 2$ of the internal channel means that if B' were to guess the internal classical message superluminally instead of waiting for it to arrive, his probability 2^{-C} of guessing correctly would exceed $1/4$, resulting in a probability greater than $1/4$ for successful superluminal transmission of the external two-bit message from B to A. This in turn entails the existence of two distinct external two-bit messages, r and s, such that $P(r \mid s)$, the probability of superluminally receiving r if s was sent, is less than $1/4$, while $P(r \mid r)$, the probability of superluminally receiving r if r was sent, is greater than $1/4$. By redundant coding, even this statistical difference between r and s could be used to send reliable superluminal messages; therefore reliable teleportation of a 2 -state particle cannot be achieved with a classical channel of less than 2 bits capacity. By the same argument, reliable teleportation of an N-state particle requires a classical channel of $2\log_2(N)$ bits capacity





References

[1] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. 47, 777 (1935); D. Bohm, Quantum Theory (Prentice Hall, Englewood Cliffs, NJ, USA 1951).
[2] A. Einstein, in Albert Einstein, Philosopher-Scientist, ed. by P. A. Schilpp (Library of Living Philosophers, Evanston, 1949) p. 85.
[3] A. Shimony, in Proc. International Symposium on Foundations of Quantum Theory (Phys. Soc. Japan, 1984).
[4] J. L. Park, Found. Phys. 1, 23 (1970).
[5] W. K. Wootters and W. H. Zurek, Nature 299, 802 (1982).
[6] J. S. Bell, Physics 1, 195 (1964); J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. 23, 880 (1969).
[7] A. Aspect, J. Dalibard, and G. Roger, Phys. Rev. Lett. 49, 1804 (1982); Y. H. Shih and C. O. Alley, Phys. Rev. Lett. 61, 2921 (1988).
[8] S. Wiesner, Sigact News 15:1, 78 (1983); C. H. Bennett and G. Brassard, Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, December 1984, pp. 175-179; A. K. Ekert, Phys. Rev. Lett., 67, 661 (1991); C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. 68, 557-559 (1992); C. H. Bennett, Phys. Rev. Lett. 68, 3121 (1992); A. K. Ekert, J. G. Rarity, P. R. Tapster, and G. M. Palma, Phys. Rev. Lett., 69, 1293 (1992); C. H. Bennett, G. Brassard, C. Crépeau and M.-H. Skubiszewska, Advances in Cryptology—Crypto '91 Proceedings, Aug. 1991, pp. 351-366; G. Brassard, G. and C. Crépeau, Advances in Cryptology—Crypto '90 Proceedings, Aug. 1990, pp. 49-61.
[9] D. Deutsch Proc. Roy. Soc. Lond. A 400, 97 (1985); D. Deutsch and R. Jozsa, Proc. Roy. Soc. Lond. A 439, 553-558 (1992); A. Berthiaume and G. Brassard, Proc. 7th Annual IEEE Conf. on Structure in Complexity Theory, Boston, June 1992, pp. 132-137; "Oracle quantum computing," Proc. Workshop on Physics and Computation, PhysComp 92, IEEE Press, Dallas (in press).
[10] A. Peres and W. K. Wootters, Phys. Rev. Lett. 66, 1119 (1991).
[11] S. L. Braunstein, A. Mann, and M. Revzen, Phys. Rev. Lett. 68, 3259 (1992).
[12] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. 69, 2881 (1992).

28.9 V. 7 Can We Undo Quantum Measurements? by Peres

Abstract

The Schrödinger equation cannot convert a pure state into a mixture (just as Newton's equations cannot display irreversibility). However, to observe phase relationships between macroscopically distinguishable states, one has to measure very peculiar operators. An

example, constructed explicitly, shows that the classical analog of such an operator cannot be measured, because to do so would violate classical irreversibility. This result justifies von Neumann's measurement theory, without any hypothesis on the role of the observer.

28.9.1 Theory

The measurement process in quantum physics was analyzed long ago by von Neumann [1] who showed that it could formally be described as the transformation of a pure state $\Psi = \sum c_n \phi_n$ into a mixture $\rho = \sum |c_n|^2 P_n$. Here, the ϕ_n are eigenstates of the dynamical variable being measured, and the P_n are the corresponding projection operators.

This irreversible transformation, commonly called the "collapse of the wave packet," cannot follow from the Schrödinger equation, since the latter generates a unitary mapping of the Hilbert space of states. In fact, the coupling of the eigenstates of the measured system to those of the measuring apparatus is a perfectly reversible process [2–4] as long as we are willing to measure correlations between the two. For these reasons, von Neumann's theory has been considered unsatisfactory, or at least incomplete.

There have been several attempts [5–7] to prove von Neumann's conjecture by supplementing quantum theory with superselection rules forbidding the measurement of operators of a certain type (those which connect macroscopically different states of the apparatus). The purpose of this paper is to show that systems with many degrees of freedom are indeed subject to such superselection rules. A general proof of this assertion would be very difficult, but the following model is typical enough to convey belief in the result.

Consider a macroscopic apparatus designed to measure the z component of the spin of an electron. This apparatus has a pointer (center-ofmass coordinate q, conjugate momentum p) initially localized around $q = 0$. The pointer is to move through a macroscopic distance L to the right or the left depending on whether $s_z = \frac{1}{2}$ or $-\frac{1}{2}$. This can be achieved by the coupling $H = 2V(t)s_z p$, where $V(t)$ is a large velocity, so large indeed that we can neglect all the other terms in the Hamiltonian during the brief duration of the coupling. [a]

Before the measurement, the state of the electron is $\binom{\alpha}{\alpha}$ and that of the apparatus is $\Psi(q, q_2, q_3, \ldots, q_N)$ where $q_2, q_3, \ldots, q_N$ are the other, "irrelevant," degrees of freedom. Naturally, N is a very large number, say 10^{23}. (It would be more realistic to assume a density matrix instead of the pure state ψ, but this refinement is not needed at the present stage.)

After completion of the coupling, the combined state is

$$\binom{\alpha}{0} e^{-iL_p}\psi + \binom{0}{\beta} e^{iL_p}\psi, \tag{1}$$

where $L = \int V dt$. Since ψ is peaked around $q = 0$, $e^{\pm iLp}\psi$ is peaked around $q = \mp L$. Thus, the sign of q is correlated to that of s_z and

$$\langle s_z \rangle = \left\langle \frac{1}{2}\,\mathrm{sign}(q) \right\rangle = \frac{1}{2}\left(|\alpha|^2 - |\beta|^2\right). \tag{2}$$

We have performed what von Neumann calls a measurement. (As we shall soon see, a better word would be "premeasurement.")

The question is whether this process is reversible and, in particular, whether the relative phase α/β is still observable. At the present stage, it is, as can be seen by measuring the expectation values of the operators,

$$A_1 = s_x \cos 2Lp + s_y \sin 2Lp \tag{3a}$$

and

$$A_2 = s_x \sin 2Lp - s_y \cos 2Lp. \tag{3b}$$

[To measure A_1 and A_2 we divide the electrons in two identical but disjoint ensembles. After each electron passage through the apparatus, we first measure p (modulo π/L) then the component of $\overrightarrow{\mathbf{S}}$ in the direction of $\tan^{-1}(2Lp)$ or $\cot^{-1}(-2Lp)$. Note that the eigenvalues of A_1 and A_2 are $\pm\frac{1}{2}$.]

These operators can conveniently be combined as

$$A = A_1 + iA_2 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} e^{2iLp}. \tag{4}$$

A straightforward calculation yields $\langle A \rangle = \alpha\beta^*$
which, together with Eq. (2), gives α and β separately, up to a common phase.

However, if we wait some time, the state (1) will evolve into

$$e^{-itH}\left[\begin{pmatrix}\alpha\\0\end{pmatrix}e^{-iL_p}\psi + \begin{pmatrix}0\\\beta\end{pmatrix}e^{iL_p}\psi\right] \tag{5}$$

where H is the Hamiltonian of the electron and apparatus. Assuming for simplicity that the two spin states have the same energy, we obtain

$$\langle A \rangle = \alpha\beta^* \int \left(e^{-itH}e^{iLp_\psi}\psi\right)^* e^{2iLp}e^{-itH}e^{-iLp_\psi}\psi d^N q \tag{6}$$

But $e^{iLp}e^{-ttH}e^{-iLp}$ is simply $e^{-itH(a+L)}$ (i.e., H with the q coordinate shifted by L) and (6) can be written as

$$\langle A \rangle = \alpha\beta^* \left\langle e^{itH^{(q-L)}}e^{-itH(q+L)}\right\rangle \tag{7}$$

The coefficient of $\alpha\beta^*$ would still be one if H did not depend on q, but there is no reason to expect that. As the pointer moves with respect to some fixed scale on the apparatus, its energy may vary somewhat from place to place and the coefficient of $\alpha\beta^*$ may be less than one in absolute value. For small t we get

$$\left|\left\langle e^{itH(q-L)}e^{-itH(q+L)}\right\rangle\right|^2 = 1 - t^2\delta H^2 + \cdots \tag{8a}$$

where
$\delta H^2 = \langle[H(q-L) - H(q+L) - \langle H(q-L) - H(q+L)\rangle]^2\rangle$.

Moreover, if the other degrees of freedom of the apparatus are in a mixed state, this coefficient will quickly fall to zero, [9] because of the randomness of the phases. The time needed to erase $\langle A \rangle$ is of the order of $1/\delta H$. It is therefore inversely proportional to the strength of the coupling of the macroscopic degree of freedom q, used for the measurement, with the other degrees of freedom of the apparatus. In the present model, this time could be of the order of the size of the pointer divided by the speed of sound (a few microseconds).

This neat distinction between the reversible premeasurement-Eq. (1)-and the ensuing irreversible process is admittedly unrealistic in most instances. In practice, a macroscopic apparatus has almost always an amplification mechanism based on a metastable initial state [10] and irreversibility appears at the very outset of the process. However, the amplification requirement is not essential and it obscures the true nature of the irreversibility of quantum measurements, which is explained below. (The reversal of an idealized premeasurement is illustrated in Fig. 1.)

The above discussion of Eq. (7)-or some similar argument [10,11]-is usually considered as a proof that the relative phase of the two branches of Eq. (5) is "lost" after some finite time.

However, such arguments are not convincing, because Eq. (5) represents a pure state (what else could it be?) and this can be shown by measuring the expectation value of another operator, namely,

$$A' = e^{-itH} A e^{itH}. \tag{9}$$

Indeed, we trivially have $\langle A' \rangle = \alpha\beta^*$, since the $e^{\pm itH}$ factors in A' cancel those of the wave functions.

However, the operator A' has very peculiar properties. (It is not of course the Heisenberg picture of A, the latter being $e^{itH} A e^{-itH}$. In fact, we are always working in the Schrödinger picture.) This A' operator is explicitly time dependent and is also a constant of the motion.

To verify that it is a constant of the motion, it is enough to observe that its matrix elements between any two Schrödinger states are constant, or simply to go to the Heisenberg picture, where A'_H looks like A_S, without any time dependence.

Now, the se explicitly time-dependent constants of the motion are very familiar in classical mechanics. For example, for a free particle, $q - tp/m$ is such a constant. Its meaning simply is the initial value of q. For an harmonic oscillator, such a constant would be $\tan^{-1}(m\omega q/p) - \omega t$, the meaning of which is the initial value of the phase. In general, for a system with N degrees of freedom, there are $2N$ constants of the motion, a few of which may be explicitly time independent (the total energy, momentum, etc.), but almost all

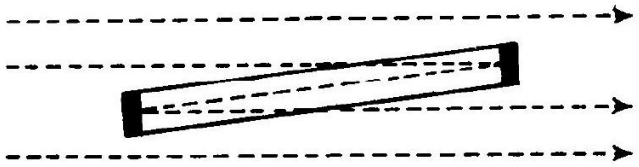


FIG. 1. Idealized premeasurement, using the recoil of a rigid double mirror. If a particle is reflected from the first mirror, a correlation is established between the momentum of the particle and that of the instrument (this is the premeasurement). That correlation is then reversibly destroyed when the particle is reflected from the second mirror. (Note that if we wish to complete the measurement and to observe the recoll of the double mirror between the two reflections, the latter must be prepared with $\Delta\phi \ll h/\lambda$. If this device is part of a double-slit experiment, it allows to determine through which slit the particle passed only at the expense of destroying the interference pattern, because $\Delta q \gg \lambda$. But if we forego observing the recoil, the interference pattern is restored because the same Δq is added and subtracted at both reflections.)

of which include the time explicitly. Their physical meaning is to give the $2N$ initial positions and momenta as explicit functions of the positions and momenta at some future time t. The structure of these constants of the motion is of course hopelessly complicated for large N and finite t. It leaves us no choice but to replace Newtonian mechanics by statistical mechanics. It is our inability to make use of these constants of the motion which is the cause of irreversibility. In the present case, we must measure, instead of A given by Eq. (4),

$$A' = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} e^{2iLp'}$$

where $p' = e^{-itH} p e^{itH}$ is the value of p immediately after the premeasurement, expressed as a function of p and $2N-1$ other variables at a later time t. In classical physics, we would say that this is so complicated that only a "Maxwell demon" can measure all these variables and then compute p' (assuming H is known). In quantum physics, the task is even more difficult

because the $2N$ variables do not commute. Therefore, the Maxwell demon must contrive a single measurement [12] for p', which is an incredibly complicated function of $2N$ noncommuting variables and of t.
In other words, we see that not every selfadjoint operator corresponds to an observable, simply because not every classical dynamical variable is observable. It is the inobservability of these operators which makes pure states appear as mixtures and causes the irreversibility of quantum measurements.

In conclusion, let us summarize the assumptions used in the derivation of this result. First, we note that the macroscopic degree of freedom used for the measurement-here, the center of mass of the pointer-is not completely isolated from the other degrees of freedom of the apparatus. [13] (We could, of course, have treated these other degrees of freedom as an external reservoir, but then our result would have been trivial. It is essential that our system be a closed one.)

The second assumption is the impossibility of measuring the classical analog of the operator p'. (There is also a tacit assumption that if a classical measurement is impossible, the same is true for the corresponding quantum measurement.) Here, it may be objected that as long as the number of degrees of freedom is finite, it is not impossible to measure p', only very difficult. In principle, a measurement of p' should always be possible at the cost of a great increase of entropy of the rest of the world. [14] From this point of view, as long as we are able to pay the price, [15] we definitely can undo quantum measurements, [4] except in the
unattainable mathematical limit of an infinite apparatus. [16] However, if we admit that a finite system may appear irreversible (if the time needed for a Poincar recurrence is longer than the Universe lifetime), the present paper shows how the irreversibility of quantum measurements is rooted in the familiar classical ir reversibility.

I am very grateful to J. A. Wheeler for the warm hospitality of the University of Texas and to E. C. G. Sudarshan for many stimulating discussions. The final version of this paper has benefited from comments by J. S. Bell (CERN) and A. Ron (Technion). This work was supported in part by the Center for Theoretical Physics, The University of Texas at Austin, Austin, Texas 78712, and also by NSF Grant No. PHY78-26592.

28.9.2 Appendix: a More Realistic Model

The simple model discussed above involves an explicitly time-dependent coupling $V(t)$, supposedly switched on and off by an external agent. This may give the impression that we are dealing with an open (i.e., incompletely described) system, for which the transformation of a pure state into a mixture would be trivial.

In a real-life Stern-Gerlach experiment, this time dependence is of course due to the translational degree of freedom of the electron, which was arbitrarily ignored in our model. A more realistic description of what happens follows.

We write the complete Hamiltonian as

$$H = H_a + H_e + 2V\,spu\,(x_2 - x)\,u\,(x - x_1)\,, \tag{A1}$$

where H_a refers to the apparatus, H_e to the free electron (mass m, momentum k, position x), V is a coupling constant, u is the unit step function, and x_1 and x_2 are the entrance and exit points of the electron as it passes through the apparatus. The pointer is assumed massive enough so that its velocity p/M is negligible when the electron is outside the apparatus. When it is inside, the pointer velocity is $\pm V$.

The measurement process can be described as a scattering of the electron and the apparatus. Before the "collision," the electron has momentum k. When it reaches the apparatus, it meets an energy barrier of height $\pm Vp$ and thickness $x_2 - x_1$. Inside the barrier, its momentum is $k' =$

$(k^2 \pm 2mVp)^{1/2} \simeq k \pm mVp/k$, where we have as sumed that $k^2 \gg 2mVp$, so that most electrons are transmitted (a reflected electron would mean an unsuccessful experiment). The outgoing electron still has momentum k, but has been subject to a phase shift $(k' - k)(x_2 - x_1) = \pm\tau Vp$ where $\tau = m(x_2 - x_1)/k$ is the classical time of passage through the apparatus. We now identify $L = \tau V$ and the
inal state of the combined system is

$$e^{ikx}\left[\begin{pmatrix}\alpha\\0\end{pmatrix}e^{-iLp}\psi + \begin{pmatrix}0\\\beta\end{pmatrix}e^{iLp}\psi\right], \tag{A2}$$

whence the discussion proceeds as before.
However, several remarks are in order. First, we have treated p as a constant during the collision, i.e., we assumed that $\dot{p} = \partial H_a/\partial q = 0$. This is of course incompatible with a nontrivial δH [see Eq. (8b)]. However, we can make the change in p arbitrarily small by increasing V and k (keeping their ratio constant, so that L remains unchanged). This does not affect $\dot{\phi}$, but makes τ arbitrarily small. The condition is easily seen to be $\tau \ll 1/\delta H$, i.e., the premeasurement must be very brief, compared to the time required to make the measurement irreversible.

To avoid a possible misunder standing, it must be emphasized that δH is much smaller than the energy uncertainty $\Delta H = ((H^2\rangle - \langle H\rangle^2)^{1/2}$. Indeed there must be many different energy eigenstates involved to make the measurement possible. [17,18] In particular, the incoming electron must have $\Delta H \gg \overline{OH}$ because the two branches of the outgoing electron will not interfere if $\delta H > \Delta H$ (that is, we would need an operator much more complicated than A to display their interference [19]).

The above remark is closely related to overall energy conservation. We have assumed hitherto that the outgoing electron had the same energy as the incoming one. This cannot, of course, be rigorously exact if $H(q - L) \neq H(q + L)$. A more correct treatment follows.

First, assume that initially the apparatus is in an eigenstate of energy E_0 and that the electron too is monochromatic with energy $K = k^2/2m$. Then obviously there is no irreversibility since the operator e^{-itH} in Eq. (A2) becomes a phase factor $\exp[-it(E_0 + K)]$ and $\langle A\rangle$ is constant. The energy picked up or released by the electron exactly compensates the energy difference in the final state of the apparatus. It is thus important to understand why $i\langle\hat{A}\rangle$ | may decrease if we have a superposition (or mixture), rather than an energy eigenstate.
Even if $|E_0\rangle$ is an eigenstate of H_c, the states $e^{\pm iL}|E_0\rangle$ usually are not. We can write

$$e^{*\{L\rho}|E_0\rangle = \int c_\pm(E_0, E, K)|E\rangle dE,$$

where the coefficients $c_\pm$depend also on K, because $L = m|x_2 - x_1|/k$. By virtue of energy conservation, the scattering process can therefore be written as

$$|E_0, K\rangle - \int c_t(E_0, E, K)|E, K + E_0 - E\rangle\, dE$$

where the $\pm$ subscripts refer to $s_g = \pm\frac{1}{2}$.
Now let the electron be initially in a superposition $\int g(K)|K\rangle dK$ (the apparatus may still be initially in an energy eigenstate [10]). The outgoing states become

$$\int g(K)c_\pm(E_0, E, K)|E, K + E_0 - E\rangle\, dEdK$$

In order to compute $\langle A\rangle$, we first note that

$$\langle E', K' + E_0 - E'|\, e^{2iLp}\,|E, K + E_0 - E\rangle \\ = \langle E'|\, e^{2iLp_1}|E\rangle\hat{o}(K' - E' - K + E),$$

so that

$$\langle A\rangle = \alpha\beta^* \int g\,(K')\,g^*\,(K')\,c_*\,(E_0,E,K)\,c_*^*\,(E_0,E',K') \times \langle E'|\,e^{2iLp}|E\rangle\delta\,(K'-E'-K+E)\,dEdE'dKdK'$$

We now make two essential physical assumptions.) One is that $\Delta K \ll K$ (otherwise, L is illdefined) so that in $c_{\pm}$we can replace K by its aver age value K_0. The second one is that $\delta H \ll \Delta K$, i.e., $c_t\,(E_0,E,K_0)$ is very small unless $|E-E_0| \ll \Delta K$ (as explained above, $|K_{\text{out}} - K_{\text{in}}|$ must be much smaller than ΔK to allow the two "branches" of the electron to interfere). We can therefore replace $g^*\,(K+E'-E)$ by $g*(K)$. Integration over K and K' gives

$$\langle A\rangle = \alpha\beta^* \int c_*\,(E_0,E,K_0)\,c_-^*\,(E_0,E',K_0) \times \langle E'|\,e^{2iLp}|E\rangle dEdE'$$

We see that the electron energy no longer appears in the formula (except as an average). The result looks as if the final state of the apparatus were $\int c_\star\,(E_0,E,K_0)\,|E\rangle dE$. Therefore, the energy shift of the electron cannot prevent $\langle A\rangle$ from having a nontrivial time dependence, due to the factor $e^{-i(E-E')t}$ in $\langle E'|\,e^{2iL}|E\rangle$.

dent coupling is discussed in the Appendix.

[9] It is not necessary that (A) be "rigorously" zero because it is an average value, not an eigenvalue. The eigenvalues are $\pm\frac{1}{2}$ and the probable error on $\langle A\rangle$ after n measurements is $\sim 1/\sqrt{n}$. Now n cannot exceed e^{2000}, say, because of cosmological limitations. Therefore, after 1000 lifetimes $\langle A\rangle$ is indistinguishable from zero as a matter of principle, not only as an approximation. ° A. Daneri, A. Loinger, and G. M. Prosperi, Nucl.

Phys. 33, 297 (1962), Numo paras metastable. This is but, as shown in the present paper and in particular in the Appendix, this assumption is not necessary.

[11] K.Hepp, Helv.Phys.Acta 15, 237 (1072),

[12] For example, it is not the same thing to measure $s_x s_y$ (eigenvalues sil/v/2) on to measure s_x and s_y separately and sum the results.

[13] A mactosopic superconducing current is not accepi able as a measuring instrument, unless it is coupled to some monitoring device with numerous degrees oi freedom.

[14] Here again, we may encounter cosmological limita-

tions [A. Peres and N. Rosen, Phys. Rev. 135, B1486 (1964). The assume that the Universe is inite, there may be generated in it. It is then plausible that if N is large, irreversibility sets in after a finite time t. However, I do not wish to enter deeper into this subject: The nurpose of this paper was not to explain classical irreversibility, but only te clarify its relationship to the quantum measurement problem.

This is the only place where the human observer has periments a fuller discussion, see A. Peres, Found. Phys (to be published). [16]. Whitten-Wolfe and

[8] *On sabbatical leave from Technion-Israel Institute of Technolngy, Haifa.

[1] J. von Neumann, Mathematical Foundations of Quantum Mechanics (Princeton University Press, Princeton, 1955).

[2] P. A. Moldauer, Phys. Rev. D 5, 1078 (1972).

[3] A. Peres, Am. J. Phys. 42, 886 (1974).

[84] J. S. Bell, Helv. Phys. Acta 48, 93 (1975).

[5] H. Wakita, Prog. Theor. Phys-23, 32 (1960).

[6] A. Komar, Phys. Rev. 133, B542 (1964).

[7] E. C. G. Sudarshan, Pramana 6, 117 (1976); T. N. Sherry and E. C. G. Sudarshan, Phys. Rev. D 18, 4580 (1978); 20, 857 (1979).

[8] A more realistic model with no explicitly time-depen-

B. W. Emch, Helv. Phys. Acta 11 E P. Wigner
18. P. Wigner, Z. Phys. 133, 101 (1952).
(1960); M. M. Yanase, ibid. Phys. nev. 120, 622 (1960); M. M. Yanase, ibid. 123, 666 (1961). we have $\Delta H \simeq kT$ part of it is in thermal equilibrium, » 1. This does not hamper the measurement as $\tau\delta H \ll 1$.

29 VI Accuracy of Measurements: Quantum Limitations

29.1 VI.1 The Unmeasurability of the Spin of a Free Electron

Commentary of Casimir (1967)

Bohr gave much thought to the spin of the electron and to Dirac's theory. I never felt quite at ease about his argument that the spin cannot be observed by classical means although he always succeeded in showing the fallacies in any proposed experimental setup.

Commentary of Rosenfeld (1971b)

Bohr as a lecturer is a different matter It is much glossed, but very little written about. Perhaps the only one who has put his vicw of it iil print so far is Larmor: in a speech (later published)* at the Maxwell celebrations in Cambridge in 1931, he commented upon Maxwell's reputation of being a poor lecturer' and roundly added: "So perhaps with our friend Bohr: he might want to instruct us about the correlations of too many things at once . . . ." I was sitting near Bohr when the speech was delivered; as this judgment was expressed, Bohr whispered to me: "Imagine, he thinks I am a poor lecturer!" Bohr's lectures, composed with tremendous labour, were indeed masterpieces of allusive evocation of a subtle dialectic; the trouble was that the audience was usually unprepared to catch subtle allusions to conceptions and arguments which were anyhow unfamiliar and hard to grasp.
*Jumes Clerk Maxwell: A Commemoration Volume 1831-1931, p. 78, Cambridge University Press, Cambridge (1931).

I am not sure whether Bohr's introductory talk at the conference was really worse than the average; perhaps he had not prepared it so thoroughly, since the idea was to have quite informal discussions: no programme had been set up in advance-Bohr took in turn each of the participants aside and asked him what topic he wished to bring up. At any rate, here is the impression this talk has left in my memory, as I described it (with some hindsight) in 1945: "He had begun with a few gencral considerations calculated, no doubt, to convey to the audience that peculiar sensation of having the ground suddenly removed from under their feet, which is so effective in promoting receptiveness for complementary thinking. This preiiminary result being readily achieved, he had eagerly hastencd to his main subject and stunned us all (except Pauli) with the non-observability of the electron spin. I spent the afternoon with Heitler pondering on the scanty fragments of the hidden wisdom which we had been able to jot down in our notebooks."

It was comforting to hear from Klein, when I told him some time ago of our failure to understand what Bohr meant by the impossibility of measuring the spin of the electron, that he had had the the same difficulty when Bohr first discussed the matter with him in the autumn of 1928. Guided by the general correspondence idea, Bohr argued that such a purely quantal concept as the electron spin, vanishing from the theory
in the classical limit, could not possibly be brought in direct relation with classical quantities like anguiar momentum or magnetic moment. It was not immediately clear to Klein, however, how this correspondence argument could be reconciled with the Stern-Gerlach effect, which clearly exhibited a contribution to the magnetic moment of an atom from an electron bound in

a ^2S state; but what Bohr demonstrated was precisely that with a free electron a Stern-Gerlach experiment could not succeed, because the effect of the Lorentz force would inevitably blur any Stern-Gerlach pattern.

- IN. F. Miou, Proc. Roy. Soc. Ai24, 440 (1929).

This is the point he ineffectually tried to make in his talk. Fortunately, Mott, during his stay at the Institute, had been engaged in the problem of electron polarization, and in the paper* in which he brilliantly showed how this property could in principle be ascertained by a double scattering experiment, he gave a very clear account of the whole situation. He finished writing this paper shortly after the conference (it was sent off by Bohr on the 25th of April) and we were thus soon able to appreciate at leisure the full force of Bohr's famous argument.

29.2 VI.1 Magnetic Moment of the Electron by Miott, Massey

(this article is not searched in the internet)

2. Magnetic moment of the electron

We have discussed so far only the magnetic moment of the atom. We shall not review here the evidence, derived from the anomalous Zeeman effect, from the gyromagnetic effect, etc., that the electron has a fourth degree of freedom, a magnetic moment - $\epsilon\hbar, 2mc$, and a mechanical moment $\frac{1}{2}h$. We shall content ourselves with remarking that according to the Schrödinger theory the ground state of the hydrogen atom is not degenerate, and therefore, in order to account for the splitting in a magnetic field revealed by the Stern-Gerlach experiment, it is necessary to assume that the electron has a fourth degree of freedom.

The first evidence that electrons have a magnetic moment was derived from their behaviour when bound in stationary states in atoms. For the study of collision problems it is necessary to inquire what meaning can be attached to the magnetic moment of a free electron. In the first place, just as in the case of the atom, it is impossible to determine the moment by means of a magnetometer experiment. This can be shown by the following argument, due to Bohr. † Let us suppose that the position of the electron is known with an accuracy Δr and that we wish to determine the magnetic moment at a point distant r from it. It will not le possible to deduce from our measurement anything about the magnetic moment of the electron unless

$$\Delta r \ll r. \tag{5}$$

The field H that we wish to observe will be of order of magnitude

$$H \sim M/r^3.$$

If, however, the electron is motion with velocity v, there will be a magnetic field due to its motion, of amount $\epsilon v/cr^2$; since we do not know v exactly we cannot allow for this field exactly. From our measurements, therefore, of the magnetic field, it will not be possible to find out anything about the magnetic moment of the electron, unless

$$M/r^3 \gg \epsilon\Delta v/cr^2,$$

where Δv is the uncertainty in our knowledge of v. Since by the

† Cf. Mott, Proc. Roy. Soc. A, 124 (1929), 440.

Originally published as section 2, chapter IX of The Theory of Atomic Collisions by N. F. Mott and H.S.W. Massey, pp. 214-19 of the third edition, Clarendon Press, Oxford (1965).
uncertainty principle $\Delta r \Delta v > h/m$, this leads to

$$\Delta r \gg r$$

which contradicts the inequality (5). We conclude therefore that it is not possible to measure the magnetic moment of an electron in this manner.

We shall now show that it is impossible, by means of a Stern-Gerlach experiment, to determine the magnetic moment of a free electron, or to prepare a beam of electrons with the magnetic moments all pointing in the same direction. The argument is also due to Bohr.

In Fig. 35 a beam of electrons is supposed to travel parallel to the z-axis (i.e. perpendicular to the plane of the paper). The pole pieces of the magnet are shown, as are also the lines of force. The purpose of the experiment is to observe a splitting in the y-direction. The force on an electron tending to split the beam will be

$$\pm M \frac{\partial H_y}{\partial y}. \tag{6}$$

Now all electrons will experience a force due to their motion through the field. Those moving in the plane Oyz will experience a force in the direction Ox. This force is perpendicular to the direction of the splitting, and its only effect will be to displace the beams to the right or to the left. However, electrons which do not move in the plane Oyz will experience a force in the direction Oy, because the lines of force in an inhomogeneous magnetic field cannot be straight, and there must to a component H_x of H along Ox. This force will have magnitude

$$\epsilon v H_r / c. \tag{7}$$

We can compare (7) with the force (6) tending to produce the splitting. H_x at a point distant Δx from the plane Oyz will be equal to $(\partial H_x/\partial x)\,\Delta x$, and since $\operatorname{div} H$ vanishes, this is equal to $-(\partial H_y/\partial y)\,\Delta x$. The quantities (6) and (7) therefore stand in the ratio

$$\frac{\epsilon h}{4\pi m c}\frac{\partial H_y}{\partial y} : \frac{\epsilon v}{c}\frac{\partial H_y}{\partial y}\Delta x.$$

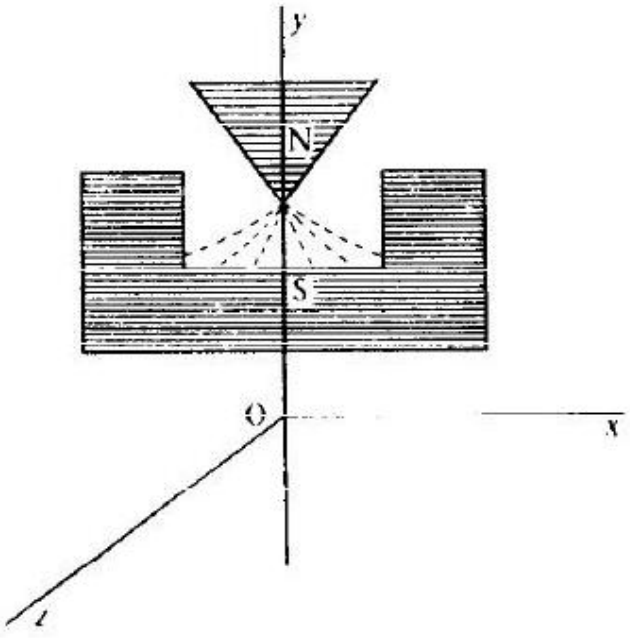
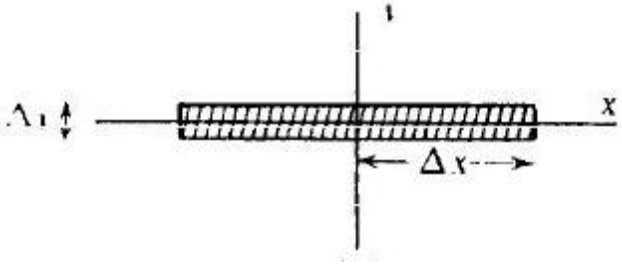


FIG. 35



(a)

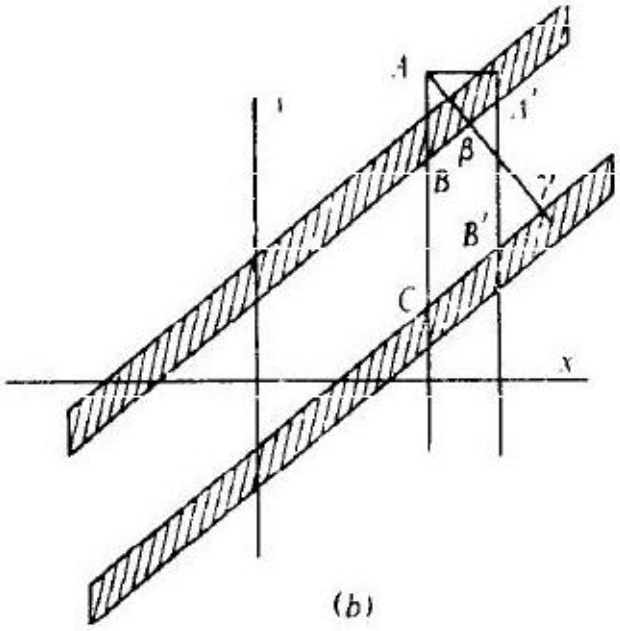


Fig. 36

Dividing through by common factors this becomes

$$1 : 4\pi\Delta x/\lambda, \tag{7.1}$$

where λ is the wavelength h/mv of the waves that represent the electrons. Suppose now that $\perp \Delta x$ is the distance from the plane O_{yz} of the two extremities of the beam. Since Δx must be greater than λ, it is clear that the two extremities of the beam will be deflected in opposite directions through angles greater than the angle of splitting, which we hope to observe.

To see now that it is impossible to observe any splitting, let us consider the trace that the beam would make on a photographic plate. Suppose that it were possible to use finer beams than is allowed by the uncertainty principle, so that the thickness Δy of the beam in the y-direction would be infinitely small. Before passing through the magnetic field, the cross-section of the heam would be as in Fig. 36 (a). Afterwards, it would be as in Fig. 36 (b), which shows the trace produced on a photographic plate. The tilting of the traces is produced by the Lorentz forces discussed above. If $ABC, A'B'$ are two lines parailel to Oy and distant λ apart, then by (7.1) we see that the tilting is so great that $AB > BC$. If $A\beta\gamma$ is drawn perpendicular to the traces, it follows that $A\beta > \beta\gamma$. But $A\beta < \lambda$, and hence $\beta\gamma$, the distance between the traces, is less than λ. Thus the maximum separation that can be produced is λ. But actually

we cannot obtain a trace of breadth comparable with λ. Therefore it is impossible to observe any splitting.

From these arguments we must conclude that it is meaningless to assign to the free electron a magnetic moment. It is a property of the electron that when it is bound in an S state in an atom, the atom has a magnetic moment. When we consider the relativistic treatment of the electron due to Dirac, we shall see that this magnetic moment is not in general equal to $-\epsilon\hbar/2mc$, unless the velocities of the electron within the atom are small compared with that of light (§ 3.3). A single
electron bound in its lowest state in the field of a nucleus of charge $Z\epsilon$ gives, according to Dirac's theory, a magnetic moment †

$$-\frac{1}{3}\left[1+2\sqrt{\left(1-\gamma^2\right)}\right]\epsilon\hbar/2mc \quad \left(\gamma = Z\epsilon^2/\hbar c\right) \tag{8}$$

The statement that a free electron has four degrees of freedom is on a different footing, for it is hardly conceivable that an electron in an atom should have four degrees of freedom, and a free electron three. It is interesting to inquire, therefore, whether there is any conceivable experiment by which this fourth degree of freedom can be detected. We wish to know whether it is possible to prepare a beam of electrons that is in some sense 'polarized', and whether it would be possible to detect this polarization.

Although it is now well known that polarization in this sense can be detected (see §§ 4.5, 4.6) it is instructive to consider the following experiment. ‡ A beam of atoms is prepared, by means of a SternGerlach experiment, with their axes all pointing in the same direction, say along the z-axis. Electrons are ejected from these atoms by illuminating them with ultra-violet light. The beam of electrons obtained may be said to be polarized, for the following reasons: Assuming for the moment that the electron behaves like a small magnet, let us ask whether forces sufficient to eject the electron would be sufficient to alter appreciably the direction of the magnetic moment. The following purely classical considerations of the order of magnitude of the forces involved show that they are not, and so we may consider that the magnetic moments in the beam of ejected electrons all point in the same direction.§

If an electric field of intensity E acts on an electron for time t, the kinetic energy acquired is $\frac{1}{2}\left(E_\epsilon\right)^2 t^2/m$. The energy that must be given to an electron to remove it from an atom is of order of magnitude $m\epsilon^4/h^2$. Thus to remove an electron from an atom the product of E and t must be of order of magnitude $Et \sim \epsilon m/h$. The average velocity of an electron in an atom is ϵ^2/h. The average couple acting on the electron magnet, due to its motion through the electric field E, will be of order

$$E\frac{\epsilon\bar{h}}{mc}\frac{\epsilon^2}{h}\frac{1}{c}$$

† This formula is due to Breit, Nature, 122 (1928), 649. Cf. § 3.3 of this chapter. ‡ This method of preparing a polarized beam of electrons was first suggested by Fues and Hellmann, Phys. Zeits. 31 (1930), 465.
§ There is, of course, a small probability that the direction of the spin-axis is reversed, and the following discussions show this to be of order of magnitude $(1/137)^2$. There is no known method by means of which a completely polarized beam can be produced.

which is equal to $E\epsilon^3/mc^2$. To change the orientation of the electron by an angle comparable with π, this couple must produce a change of angular momentum comparable with h. The time T necessary for this to occur is given by

$$T\frac{E\epsilon^3}{mc^2} \sim h$$

which gives

$$ET \sim hmc^2/\epsilon^3.$$

We deduce that

$$\frac{ET}{Et} \sim \left(\frac{hc}{\epsilon^2}\right)^2$$

Thus

$$T \gg t$$

It would, however, be meaningless to speak of a polarized beam, unless the fact that the beam is polarized could be detected in some way. This could be done if the beam were passed through a gas of ionized atoms, so that some of the electrons were captured. If the neutral atoms formed were shown by means of a Stern-Gerlach experiment to be polarized, then we should have a method of detecting the polarization. The argument used above about the order of magnitude of the forces involved indicates that this should be the case; a proper proof can, however, be given on the hasis of Dirac's theory of the electron.

An account of more practical methods of preparing and of detecting a polarized beam is given in §§ 4.2 and 4.6.

We see, then, that the spin of a free electron may be described by the same wave function $\chi_l(s)$ that was used before to describe the magnetic moment of an atom. The function

$$|\chi_l(s)|^2 \quad (s = \pm 1)$$

gives the probability that, if the electron is prepared with its magnetic moment in the direction 1, then, if the electron be captured by an atom, and if that atom be passed into an inhomogeneous magnetic field, the energy of that atom will be either $\pm MH$. It is necessary to give to the square of the amplitude of the wave function this rather complicated interpretation, because it is not possible to measure the energy of an electron in a magnetic field, unless the electron is captured in an atom. It is further to be noted that, by the statement that an electron is prepared with its magnetic moment in a given direction, it is meant that the electron has been knocked off an atom that has been so prepared.

As in the case of the bound electron, an electron is completely described by a wave function $\psi(\mathbf{r}, s)$.

If the forces acting on the electron are so small that the direction of the spin remains constant throughout the experiment considered. then a before this function may be spit up into the product

$$\text{(ri) } \chi^{(s)}.$$

where $\dot{J}(r)$ is a whation of schardinger * equation. The form of sor. 1 when this is not the case can be found from Dirac, theory.

29.3 VI.2 Measurement of Quantum Mechanical Operators by Araki, Yanase

The limitation on the measurement of an operator imposed by the presence of a conservation law is studied. It is shown that an operator which does not commute with a conserved (additive)

quantity cannot be measured exactly (in the sense of von Neumann). It is also shown for a simple case that an approximate measurement of such an operator is possible to any desired accuracy.

29.3.1 1. Introduction

I T was pointed out by Wigner [1] that the presence of a menservation law puts a limitation on the measurement of an operator which does not commute with the conserved quantity. The limitation is such that the measurement of such an operator is only approximately possible. An approximate measurement ca be done by measuring apparatus which is large enough in the sense that the apparatus should be a superposition of sufficiently many states with different quantum numbers of the conserved quantity. He has proved these statements for a simple case where the x component of the spin of a spin one-half particle is measured, the z component of the angular momentum being the conserved quantity. The aim of this paper is to present a proof of the above statement for the general case.
In Sec. 2, we will prove that an exact measurement of an operator M which does not commute with a conscrved operator L_1 is impossible. In Scc. 3, we will prove that an approximate measurement of the operator M is possible if L_1 has discrete eigenvalues and is bounded in the Hilbert space of the measured object.

29.3.2 2. Impossibility of an Exact Measurement of an Operator Which Does Not Commute with a Conserved Quantity with a Conserved Quantity

Suppose we measure a self-adjoint operator M for a system represented by a Hilbert space $\mathfrak{Y}_1$. Assume that M has discrete eigenvalues μ and corresponding eigenvectors $\boldsymbol{\phi}_{\mu\rho}$ which are orthonormal and complete in $\mathfrak{G}_1$,

$$M\phi_{\mu\rho} = \mu\phi_{\mu\rho}, \tag{2.1}$$
$$(\phi_{\mu\rho}, \phi_{\mu'\rho'}) = \delta_{\mu\mu'}\delta_{\rho\rho'}. \tag{2.2}$$

The measuring apparatus is represented by a Hilbert space $\mathfrak{S}_2$. Then a state of the combined system of the measured object and the measuring apparatus is represented by a unit vector in $\mathfrak{S}_1 \otimes \mathfrak{S}_2$.

According to von Neumann, [2] the measurement of the

*Present address: Department of Nuclear Engineering, Kyoto University, Kyoto, Japan.
† On leave of absence from Sophia University, Tokyo, Japan. [1] E. P. Wigner, Z. Physik 131, 101 (1952).
chanik (Verlag Julius Springer, Berlin, 1932; English ed.: Princeton University Press, Princeton, 1955). 1932 ; English ed.: Princeton University Press, Princeton, 1955).
operator M in a state ϕ is accomplished by choosing an apparatus in a state ξ (fixed normalized state independent of ϕ) in $\mathfrak{W}_2$ such that the combined system, if it is in the state $\dot{\phi}_{\mu\rho}\widehat{\otimes}\xi$ before the measurement, goes over after a finite time t into

$$U(l)\,(\phi_{\mu\rho} \otimes \xi) = \sum_{\rho'} \phi_{\mu\rho'} \otimes \mathbf{X}_{\mu\rho\rho'}, \tag{2.3}$$

where $U(t)$ is a unitary operator describing the timedevelopment of the combined system. In order to be able to distinguish the different measured values of the operator M in terms of states of measuring apparatus after the measurement, we require

$$(\mathrm{X}_{\mu\rho\rho''}, \mathrm{X}_{\mu'\rho'\rho'''}) = 0, \quad \text{if} \quad \mu \neq \mu'. \tag{2.4}$$

We note that, because we are not measuring the degeneracy parameter ρ, we have to allow the possibility that the measuring object remains in any linear combination of $\phi_{\mu\rho'}$, with fixed μ but with arbitrary ρ.[3]

We now assume the existence of a universal conservation law for a self-adjoint operator L which is additive in the sense that

$$L = L_1 \otimes 1 + 1 \otimes L_2, \tag{2.5}$$

where L_1 and L_2 are self-adjoint operators in $\mathfrak{W}_1$ and $\mathfrak{W}_2$, respectively. Actually this additivity will be used only before and after the measurement, when the two systems are separated. By universal, we mean that, whatever measuring apparatus we take, $U(t)$ commutes with L,

$$[U(t), L] = 0. \tag{2.6}$$

Our claim is that (2.3) is impossible unless

$$[L_1, M] = 0. \tag{2.7}$$

[3] For any state of the measured object, we can write $U(t)(\phi \otimes \xi) = \Sigma_{\mu\rho} \phi_{\mu\rho} \otimes \mathrm{X}_{\mu\rho}(\phi)$, where $\mathrm{X}_{\mu\rho}(\phi)$ depends on ϕ. The Eqs. (2.3) and (2.4) give the most general form of the above equation satisfying (1) the distinguishability of the measured result,

$$(\mathrm{X}_{\mu\rho}(\phi), \mathrm{X}_{\mu'\rho'}(\phi)) = 0, \quad \text{if} \quad \mu \neq \mu',$$

and (2) the requirement that the probability of an eigenvalue μ in the state ϕ, as measured by the state of the measuring apparatus
after the measurement, should give the conventionally postulated value,
$\Sigma_\rho ||\mathrm{X}_{\mu\rho}(\phi)||^2 = \Sigma_\rho \left|(\phi_{\mu\rho}, \phi)\right|^2$.

For the proof, we first note that, becausc of the unitarity of $U(t)$ and the conservation law (2.6), we have

$$\begin{aligned}
&(\phi_{\mu'\rho'} \otimes \xi, L\,(\phi_{\mu\rho} \otimes \xi)) \\
&\quad = (U(t)\,(\phi_{\mu'\rho'} \otimes \xi)\,, U(t) L\,(\phi_{\mu\rho} \otimes \xi)) \\
&\quad = (U(t)\,(\phi_{\mu'\rho'} \otimes \xi)\,, L U(t)\,(\phi_{\mu\rho} \otimes \xi)) \\
&\quad = \left(\sum_{\rho'''} \phi_{\mu'\rho'''} \otimes \mathrm{X}_{\mu'\rho'\rho'''}, L \sum_{\rho''} \phi_{\mu\rho''} \otimes \mathrm{X}_{\mu\rho\rho''} \right).
\end{aligned} \tag{2.8a}$$

Hence, as the necessary condition for the conservation law for the operator L, we can write

$$\begin{aligned}
&(\phi_{\mu'\rho'} \otimes \xi, L\,(\phi_{\mu\rho} \otimes \xi)) \\
&\quad = \left(\sum_{\rho'''} \phi_{\mu'\rho'''} \otimes \mathrm{X}_{\mu'\rho'\rho'''}, L \sum_{\rho''} \phi_{\mu\rho''} \otimes \mathrm{X}_{\mu\rho\rho''} \right).
\end{aligned} \tag{2.8b}$$

Using the additivity of L, (2.5), we obtain

$$
\begin{aligned}
&(\phi_{\mu'\rho'} \otimes \xi, L\,(\phi_{\mu\rho} \otimes \xi)) \\
&\quad - (\phi_{\mu'\rho'}, L_1\phi_{\mu\rho})\,(\xi,\xi) \mid (\phi_{\mu'\rho'}, \phi_{\mu\rho})\,(\xi, L_2\xi) \\
&\quad = \sum_{\rho''\rho'''} [(\phi_{\mu'\rho'''}, L_1\phi_{\mu\rho''})\,(\mathbf{X}_{\mu'\rho'\rho'''}, \mathrm{X}_{\mu\rho\rho''}) \\
&\quad + (\phi_{\mu'\rho'''}, \phi_{\mu\rho''})\,(\mathrm{X}_{\mu'\rho'\rho'''}, L_2\mathrm{X}_{\mu\rho\rho''})]\,. \qquad (2.8c)
\end{aligned}
$$

Because of the orthogonalities, (2.2) and (2.4), we finally obtain

$$
(\phi_{\mu'\rho'}, L_1\phi_{\mu\rho}) = 0, \quad \text{if} \quad \mu \neq \mu', \qquad (2.9a)
$$

or

$$
(\phi_{\mu'\rho'}, L_1\phi_{\mu\rho}) = \delta_{\mu\mu'}\,(\phi_{\mu'\rho'}, L_1\phi_{\mu'\rho})\,. \qquad (2.9b)
$$

We are now ready to prove that L_1 commutes with M. For this purpose we decompose M into projection operators

$$
M = \sum_{\mu} \mu P_\mu; \quad P_\mu\phi_{\mu'\rho'} = \delta_{\mu\mu'}\phi_{\mu'\rho'}. \qquad (2.10)
$$

To prove the commutativity of L_1 and M, (2.7), it is sufficient to prove the commutativity of L_1 and P_μ,

$$
P_\mu L_1 - L_1 P_\mu = 0. \qquad (2.11)
$$

From the self-adjoint nature of P_μ, (2.9b) and (2.10), we see that

$$
\begin{aligned}
&(\phi_{\mu'\rho'}, P_\mu L_1\phi_{\mu''\rho''}) = \delta_{\mu\mu'}\delta_{\mu'\mu''}\,(\phi_{\mu'\rho'}, L_1\phi_{\mu''\rho''})\,, \\
&\left(\phi_{\mu'\rho'}, L_1 P_{\mu\psi_{\mu''\rho''}}\right) = \delta_{\mu\mu''}\delta_{\mu'\mu''}\,(\phi_{\mu'\rho'}, L_1\psi_{\mu''\rho''})\,,
\end{aligned}
$$

which manifestly demonstrate (2.11). Thus we have succeeded in proving that (2.3)-(2.6) imply (2.7). [4]

Although we have assumed in the above proof that M has a discrete spectrum, the conclusion holds for any self-adjoint operator M. Namely, suppose

$$
M = \int \mu dP(\mu)
$$

---

[84] If L_2 is unbounded, the above proof does not exclude the possibility that one can measure M, even if M does not commute with L_1, by a measuring apparatus (ξ or $\mathbf{X}_{\mu\rho\rho'}$) in a state which is outside the domain of L, because (2.8) would then be meaningless.
However, even if L_2 is unbounded, as long as L_1 is bounded, we can modify the above argument in the following way. We introduce unitary operators

$$
V(S) = \exp(iLS); \quad V_j(S) = \exp\,(iL_jS)\,, \quad j = 1, 2. \qquad \text{(i)}
$$

Because of the additivity, (2.5),

$$
V(S) = V_1(S) \otimes V_2(S). \qquad \text{(ii)}
$$

Then, by the conservation law (2.6), we have
($\phi_{\mu'\rho'} \otimes \xi, V(S)\,(\phi_{\mu\rho} \otimes \xi)$)

$$
= (\Sigma_{\rho'''}\phi_{\mu'\rho'''} \otimes \mathbf{X}_{\mu'\rho'\rho'''}, V(S)\,(\Sigma_{\rho''}\phi_{\mu\rho''} \otimes \mathbf{X}_{\mu\rho\rho''}))\,. \qquad \text{(iii)}
$$

is a spectral decomposition of M. If M can be measured exactly, $P(\mu)$ for each μ can obviously be measured exactly. Since the projection operator $P(\mu)$ has a discrete eigenvalue 1 or 0 , the above proof tells us that $P(\mu)$ for each μ commutes with L_1, which in turn implies (2.7).

29.3.3 3. Possibility of an Approximate Measurement

In this section we will discuss the problem of whether the operator M, which does not commute with the conserved operator L_1 of the preceding section, can be measured approximately. We will prove that this is possible if L has a discrete spectrum and L_1 has only a finite number of eigenvalues.

We may assume that the eigenvalues of L_1 are [5]$0, \pm 1, \pm 2, \cdots \pm l$. We decompose L 's into projection operators

$$L = \sum_{\lambda} \lambda P(\lambda) \tag{3.1a}$$

$$L_i = \sum_{\lambda} \lambda P_i(\lambda), \quad i = 1, 2 \tag{3.1b}$$

The additivity, (2.5), implies

$$P(\lambda) = \sum_{|\lambda'| \leq l} P_1(\lambda') P_2(\lambda - \lambda') . \tag{3.2}$$

As a first step of our proof, we state the following Lemma which will be proved at the end of this section.

Lemma. Given two sets of vectors ${\Psi_a}^i$ and ${\Psi_\alpha}^f$ in a Hilbert space $\mathfrak{S} = \mathfrak{W}_1 \otimes \mathfrak{W}_2$ satisfying

$$\left({\Psi_n}^i, P(\lambda) {\Psi_\beta}^i\right) = \left({\Psi_n}^f, P(\lambda) {\Psi_\beta}^f\right), \tag{3.3}$$

for every λ, then there exists a Hilbert space $\mathfrak{W}_2'$ con-

By the orthogonality, (2.2),

$$\begin{aligned} &(\phi_{\mu'\rho'} \otimes \xi, \ V_2(S)(\phi_{\mu\rho} \otimes \xi)) \\ &\quad = (\Sigma_{\rho'''} \phi_{\mu'\rho'''} \otimes \mathrm{X}_{\mu'\rho'\rho'''}, V_2(S)(\Sigma_{\rho''} \phi_{\mu\rho''} \otimes \mathrm{X}_{\mu\rho\rho'})) \\ &\quad = 0 \quad (\text{ for } \mu \neq z'\mu') \end{aligned}$$

Combining the two equations above and using the additivity, (ii), we obtain for $\mu \neq \mu'$,

$$(\phi_{\mu'\rho'} \otimes \xi, F(S)(\phi_{\mu\rho} \otimes \xi)) \left(\sum_{\rho'''} \phi_{\mu'\rho'''} \otimes \mathrm{X}_{\mu'\rho'\rho'''}, F(S) \left(\sum_{\rho''} \phi_{\mu\rho''} \otimes \mathrm{X}_{\mu\rho\rho''} \right) \right),$$

$$F(S) = (1/iS)[V_1(S) - 1] \otimes V_2(S). \tag{vi}$$

Since $F(S) \to L_1$, as $S \to 0$, we obtain

$$(\phi_{\mu'\rho'} \otimes \xi, L_1(\phi_\mu \otimes \xi))$$

$$= \left(\Sigma_{\rho''', \phi_{\mu'\rho''}, \left(\otimes \mathbf{X}_{\mu'\rho'\rho'''}, L_1\left(\Sigma_{\rho''} \phi_{\mu\rho''} \otimes \mathbf{X}_{\mu\rho\rho''}\right)\right).} \right). \tag{vii}$$

Because of the orthogonality, (2.4), we finally obtain (2.9a) from which we conclude (2.11) as before.

[5] The proof holds without this specification but notations become complicated, especially in dividing various regions of values of λ.

taining $\mathfrak{W}_2$ and a unitary operator U on $\mathfrak{S}' = \mathfrak{W}_1 \otimes \mathfrak{W}_2{}'$ such that (1) a self-adjoint operator $L_2{}'$ (representing the conserved quantity in $\mathfrak{S}_2{}'$) is defined on $\mathfrak{W}_2{}'$ coinciding with L_2 on $\mathfrak{W}_2$, (2) U commutes with the conserved quantity L' on $\mathfrak{S}', L' = L_1 \otimes 1 + 1 \otimes L_2{}'$, and

$$(3)\ \Psi_a{}^f = U\Psi_a{}^i \tag{3.4}$$

If the set of the indices α is finite, $\mathfrak{S}_2{}'$ can be taken to be $\mathfrak{H}_2$.

This Lemma is used in the following way. We will construct states $\xi, \mathrm{X}_{\mu\rho}, \psi$, and $\eta_{\mu\rho}$ satisfying

$$(\mathrm{X}_{\mu\rho}, \mathrm{X}_{\mu'\rho'}) = 0, \quad \text{if } \mu \neq \mu', \tag{3.5}$$

$$(\mathrm{X}_{\mu\rho}, \eta_{\mu'\rho'}) = 0, \quad \text{for any } \mu, \rho, \mu', \rho', \tag{3.6}$$

$$\left\|\psi \otimes \eta_{\mu_\rho}\right\|^2 < \epsilon,$$

$$(\eta_{\mu\rho}, \eta_{\mu'\rho'}) = 0, \quad \text{for } (\mu, \rho) \neq (\mu', \rho') \tag{3.7}$$

in such a way that the two sets of vectors

$\Psi_\alpha{}^i = \phi_{\mu\rho} \otimes \xi, \quad \Psi_\alpha{}^j = \phi_{\mu\rho} \otimes \mathrm{X}_{\mu\rho} + \psi \otimes \eta_{\mu\rho}, \quad \alpha = (\mu, \rho),$

fulfill (3.3). If we succeed in constructing such states, then by the Lemma, there exists a unitary operator U in $\mathfrak{W}'$ which conserves L' and for which (3.4) holds. This implies, for any normalized state ϕ in $\mathfrak{S}_1$,

$$U(\phi \otimes \xi) = \sum_{\mu\rho} (\phi_{\mu\rho}, \phi)\, (\phi_{\mu\rho} \otimes \mathrm{X}_{\mu\rho}) + \eta(\phi) \tag{3.9}$$

$$\eta(\phi) = \sum_{\mu\rho} (\phi_{\mu\rho}, \phi)\, (\psi \otimes \eta_{\mu\rho}) \tag{3.10}$$

and, due to (3.7),

$$\|\eta(\phi)\|^2 < \epsilon \tag{3.11}$$

Thus if we choose the setup of a measurement in such a way that the Hilbert space of the measuring instrument is $\mathfrak{W}_2{}'$, the initial state of the instrument is ξ, and the time development of the combined system of the measured object and the measuring apparatus in a certain time interval t is described by $U(l) = U$, then we can measure the operator M in terms of the states $\mathrm{X}_{\mu\rho}$ of the measuring apparatus after the measurement within the inaccuracy representing by $\eta(\phi)$. This inaccuracy can be made as small as one desires by making ϵ small chough. Because we are only concerned with the effect of the conservation law of L, we have assumed in the above argument that, if U is a unitary operator commuting with the conserved quantity, then there always exists an experimental setup whose time development in a certain time period is described by U. There may be many other conditions on U in addition to that it commutes with L. Hence, our argument does not assure that a system exists whose Hamiltonian leads to U.

We now give an explicit construction of states $\xi, \mathrm{X}_{\mu\rho}$, ψ and $\eta_{\mu\rho}$. For this purpose we denote by $\mathfrak{S}_{2\lambda}$ the subspace of $\mathfrak{S}_2$ which is spanned by eigenvectors of L_2

with an eigenvalue λ.ψ is taken to be a normalized eigenstate of L_1 with the eigenvalue 0 ,

$$I_1\psi = 0, \quad (\psi,\psi) = 1. \tag{3.12}$$

$\xi, \mathrm{X}_{\mu\rho}$, and $\eta_{\mu\rho}$ are given by

$$\xi = \sum \lambda\xi_\lambda \quad X_{\mu p} = \sum \lambda X_{\mu p\lambda}; \quad \eta_{\mu p} = \sum \lambda\eta_{\mu p\lambda}, \tag{3.13}$$

where $\xi_\lambda, \mathrm{X}_{\mu\rho\lambda}$, and $\eta_{\mu\rho\lambda}$ are vectors in $\mathfrak{S}_{2\lambda}$ to be specified below.
ξ_λ is any state in $\mathfrak{W}_{2\lambda}$ with the norm given by

$$\begin{aligned} (\xi_\lambda,\xi_\lambda) &= 0, && \text{for } |\lambda| > N \\ &= (2N+1)^{-1}, && \text{for } |\lambda| \le N \end{aligned} \tag{3.14a}$$

N is any integer satisfying

$$N > 2l/\epsilon^{-\frac{1}{2}}. \tag{3.15}$$

The $\mathrm{X}_{\mu\rho\lambda}$ are any states in $\mathfrak{S}_{2\lambda}$, orthogonal to each other and with the norm given by

$$(\mathrm{X}_{\mu\rho\lambda}, \mathrm{X}_{\mu'\rho'\lambda}) = 0, \quad \text{for} \quad |\lambda| > N - 2l \tag{3.8}$$

$$= (2N+1)^{-1}\delta_{\mu\mu'}\delta_{\rho\rho'}, \tag{3.16a}$$

$$\text{for} \quad |\lambda| \le N - 2l \tag{3.10b}$$

The orthogonal complement of the set $\{\mathrm{X}_{\mu\rho\lambda} \mid \mu,\rho \text{ varying}\}$ in $\mathfrak{W}_{2\lambda}$ will be denoted by ${\mathfrak{S}_{2\lambda}}^{\eta}$.
$\eta_{\mu\rho\lambda}$ are taken from ${\mathfrak{S}_{2\lambda}}^{\eta}$ and defined in the following way
(I) Fur $|\lambda| > N + l$ or $|\lambda| \le N - 3l$,

$$\eta_{\mu\rho\lambda} = 0 \tag{3.17a}$$

(II) For $N + l \ge |\lambda| > N - l$, [6]
$(\eta_{\mu\rho\lambda}, \eta_{\mu'\rho'\lambda})$

$$= (2N+1)^{-1} \sum_{\substack{|\lambda'|\le l \\ |\lambda-\lambda'|\le N}} \left(\phi_{\mu_\rho}, P_1(\lambda')\,\phi_{\mu'\rho'}\right) \tag{3.17b}$$

(III) For $N - l \ge |\lambda| > N - 3l, \eta_{\mu\rho\lambda}$ are any states in $\mathfrak{W}_{2\lambda^\pi}$ orthogonal to each other and with the norm given by

$$(\eta_{\mu\rho\lambda}, \eta_{\mu'\rho'\lambda}) = (2N+1)^{-1}(\phi_{\mu\rho}, Q_\lambda\phi_{\mu\rho})\,\delta_{\mu\mu'}\delta_{\rho\rho'} \tag{3.17c}$$

where Q_λ is a projection operator given by

$$Q_\lambda = \sum_{\substack{|\lambda'|\le l \\ |\lambda-\lambda'|>N-2l}} P_1(\lambda') \tag{3.18}$$

Note that $(\phi_{\mu\rho}, Q_\lambda\phi_{\mu\rho})$ is non-negative (between 0 and 1).
We now show that $\xi, \mathrm{X}_{\mu\rho}, \psi$, and $\eta_{\mu\rho}$ thus constructed have the desired properties. ξ is normalized due to (3.14). (3.5) and (3.6) are trivially satisfied by our
[6] This means that $\eta_{\mu\rho\lambda}$ is defined by

$$\eta_{\mu\rho\lambda} = (2N+1)^{-\frac{1}{2}} \sum_{\substack{|\lambda'|\le l \\ |\lambda-\lambda'|\le N}} P_1^{(\lambda)}(\lambda')\,\phi_{\mu\rho}^{(\lambda)}$$

where we have made an isometric linear mapping of $\mathfrak{W}_1$ into $\mathfrak{W}_{2\lambda^n}$ and $\phi_{\mu\rho}$ and $P_1(\lambda')$ thus mapped are called ${\phi_{\mu\rho}}^{(\lambda)}$ and ${P_1}^{(\lambda)}(\lambda')$.
choice. To prove (3.3), we rewrite (3.5) using (3.2):

$$\begin{aligned}
&\sum_{|\lambda'|\le l} \left(\phi_{\mu\rho}, P_1(\lambda')\,\phi_{\mu'\rho'}\right)\left(\xi, P_2(\lambda-\lambda')\,\xi\right) \\
&= \sum_{|\lambda'|\le l} \left(\phi_{\mu\rho}, P_1(\lambda')\,\phi_{\mu'\rho'}\right)\left(\mathrm{X}_{\mu\rho}, P_2(\lambda-\lambda')\,\mathrm{X}_{\mu'\rho'}\right) \\
&\quad + \left(\eta_{\mu\rho}, P_2(\lambda)\eta_{\mu'\rho'}\right) \qquad (3.19)
\end{aligned}$$

where we have also used (3.12). By (3.13), this is equivalent to

$$\begin{aligned}
&\sum_{|\lambda'|\le l} \left(\phi_{\mu\rho}, P_1(\lambda')\,\phi_{\mu'\rho'}\right) \\
&\quad \times \left[\|\xi_{\lambda-\lambda'}\|^2 - \left(\mathrm{X}_{\mu\rho,\lambda-\lambda'}, \mathrm{X}_{\mu'\rho',\lambda-\lambda'}\right)\right] \\
&\quad = \left(\eta_{\mu\rho\lambda}, \eta_{\mu'\rho'\lambda}\right). \qquad (3.20)
\end{aligned}$$

We divide the range of λ into 4 parts and prove (3.20) separately for λ in each of these 4 regions.
(I) If $|\lambda| > N + l$, then $|\lambda - \lambda'| > N$ and (3.20) is trivially satisfied because all terms vanish.
(II) If $N + l \ge |\lambda| > N - l$, then $|\lambda - \lambda'| > N - 2l$, and hence the term containing X still vanishes. Due to (3.14b), the left-hand side of (3.20) becomes

$$\sum_{|\lambda'|\le l} \left(\phi_{\mu\rho}, P_1(\lambda')\,\phi_{\mu'\rho'}\right)\|\xi_{\lambda-\lambda'}\|^2 \sum_{\substack{|\lambda'|\le l \\ |\lambda-\lambda'|\le N}} \left(\phi_{\mu\rho}, P_1(\lambda')\,\phi_{\mu'\rho'}\right),$$

which is equal to the right-hand side of (3.20) calculated by (3.17b).
(III) If $N - l \ge |\lambda| > N - 3l$, then $|\lambda - \lambda'| \le N$ and hence $\|\xi_{\lambda-\lambda'}\|^2$ is always $(2N+1)^{-1}$. By the orthogonality, (2.2), the definition (3.16b) and the equation

$$\sum_{|\lambda'|\le l} P_1(\lambda) = 1, \qquad (3.21)$$

the left-hand side of (3.20) becomes

$$\begin{aligned}
&\sum_{|\lambda'|\le l} \left(\dot{\varphi}_{\mu\rho}, P_1(\lambda')\,\dot{\phi}_{\mu'\rho'}\right)\left[(2N+1)^1 - \left(\mathbf{X}_{\mu\rho,\lambda-\lambda'}, \mathbf{X}_{\mu'\rho',\lambda-\lambda'}\right)\right] \\
&= (2N+1)^{-1}\delta_{\mu\mu'}\delta_{\rho\rho'} \sum_{|\lambda'|\le l} \left(\phi_{\mu\rho}, P_1(\lambda')\,\phi_{\mu\rho}\right) \\
&\qquad \times \left[1 - (2N+1)\left(\mathbf{X}_{\mu\rho,\lambda-\lambda'}, \mathbf{X}_{\mu'\rho',\lambda-\lambda'}\right)\right]. \qquad (3.22)
\end{aligned}$$

Because of (3.16b), the inside of the square bracket of (3.22) vanishes for $|\lambda - \lambda'| \le N - 2l$ and is unity for $|\lambda - \lambda'| > N - 2l$. Thus, due to (3.17c) and (3.18), (3.22) is equal to the right-hand side of (3.20).
(IV) If $N - 3l \ge |\lambda|$, then $|\lambda - \lambda'| \le N - 2l$ and the left-hand side of (3.20) becomes

$$\sum_{|\lambda'|\le l} \left(\phi_{\mu\rho}, P_1(\lambda)\phi_{\mu'\rho'}\right)\left(1 - \delta_{\mu\mu'}\delta_{\rho\rho'}\right).$$

Because of (3.21) and the orthogonality, (2.2), this expression vanishes and hence is equal to the right-hand side of (3.20) which also vanishes due to (3.17a). This completes the proof of (3.4).

Finally, we will prove (3.7). Since ψ is normalized, $\|\psi \otimes \eta_{\mu\rho}\|$ is equal to $\|\eta_{\mu\rho}\|$. By (3.13), we have

$$(\eta_{\mu\rho'}\eta_{\mu'\rho'}) = \sum \lambda \, (\eta_{\mu\mu'}, \eta_{\mu'\rho'}\lambda)$$

By (3.20), we get
$\sum_\lambda \left(\eta_{\mu\rho\lambda,\eta_{\mu\rho'}\lambda'}\right)$

$$= \sum_{\substack{\lambda\lambda' \\ |\lambda'|\leq l}} (\phi_{\mu\rho}, P_1(\lambda')\,\phi_{\mu'\rho'}) \left[\|\xi\lambda - \lambda'\|^2 - \|\mathrm{X}_{\mu\rho,\lambda-\lambda'}\|^2 \delta_{\mu\mu}\delta_{\rho\rho'}\right]$$

$$= \sum_{\substack{\lambda\lambda' \\ |\lambda'|\leq l}} (\phi_{\mu\rho}, P_1(\lambda')\,\phi_{\mu'\rho'}) \left[\|\xi\lambda\|^2 - \|\mathrm{X}_{\mu\rho,\lambda}\|^2 \delta_{\mu\mu'}\delta_{\rho\rho'}\right].$$

By (3.21) and (2.2),

$$\sum_{|\lambda'|\leq l} (\phi_{\mu\rho}, P_1(\lambda')\,\phi_{\mu'\rho'}) = \hat{\partial}_{\mu\mu'\rho\rho'}$$

By (3.14) and (3.16)

$$\sum_\lambda \left[\|\xi_\lambda\|^2 - \|\mathrm{X}_{\mu\rho\lambda}\|^2\right] = 4l(2N+1)^{-1}.$$

Combining these, and using (3.15), we obtain

$$\left\|\psi \otimes \eta_{\lambda_\rho}\right\|^2 = \frac{4l}{2N+1} < \epsilon$$
$$(\eta_{\mu\rho}, \eta_{\mu'\rho'}) = 0, \quad \text{for } (\mu,\rho) \neq (\mu',\rho')$$

In the above construction, $\mathfrak{S}_{2\lambda}$ for $|\lambda| \leq N - 3l$ should have at least the dimension of $\mathfrak{S}_1$. We need higher dimension for $\mathfrak{S}_{2\lambda}$ with $N - 3l < |\lambda| \leq N$.[7]

Finally we will give a proof of our Lemma. For this purpose, we denote the subspace of $\mathfrak{S}$ spanned by eigenvectors of L with eigenvalue λ by $\mathfrak{S}_\lambda$, the subspace spanned by $P(\lambda)\Psi_a{}^i$ with varying α by $\mathfrak{S}_\lambda{}^i$, the subspace spanned by $P(\lambda)\Psi_\alpha{}^f$ with varying α by $\mathfrak{S}_\lambda{}^f$, the orthogonal complement of $\mathfrak{S}_\lambda{}^i$ in $\mathfrak{S}_\lambda$ by $\mathfrak{S}_\lambda{}^i{}_\perp$, and the orthogonal complement of $\mathfrak{S}_\lambda{}^j$ in $\mathfrak{S}_\lambda$ by $\mathfrak{S}_\lambda{}^j{}_\perp$. Obviously

$$\mathfrak{S} = \oplus_\lambda \left(\mathfrak{S}_\lambda{}^i \oplus \mathfrak{S}_\lambda{}^i{}_1\right) = \oplus_\lambda \left(\mathfrak{W}_\lambda{}^j \oplus \mathfrak{W}_\lambda{}^i{}_1\right). \tag{3.23}$$

We will first show that

$$U_\lambda \left(\sum_\alpha C_\alpha P(\lambda)\Psi_\alpha^i\right) = \sum_\alpha C_\alpha P(\lambda)\Psi'_\alpha, \tag{3.24}$$

defines a unitary mapping U_λ of $\mathfrak{S}_\lambda{}^i$ onto $\mathfrak{S}_\lambda{}^f$, where $\{C_\alpha\}$ is a set of arbitrary complex numbers. To see this, we note that, due to (3.3), $\sum_\alpha C_\alpha P(\lambda)\Psi_\alpha{}^i$ and

[87] In the above construction, the measuring apparatus is a superposition of eigenstates of L_2 with different eigenvalues λ varying over the range of the order $1/\epsilon$. However, if one counts the number of equations to be satisfied, one finds a possibility of constructing a similar measuring apparatus which is a superposition of eigenstates of L_2 with eigenvalues, near a certain large value of the order $1/\epsilon$, but varying only over the range

$\sum_\alpha C_\alpha P(\lambda)\Psi_\alpha{}'$ converge, diverge, or vanish simultaneously. Hence, U_λ is a one-to-one mapping of $\mathfrak{S}_\lambda{}^i$ onto $\mathfrak{W}_\lambda{}^j$. Since this mapping is linear and, due to (3.3), isometric, U_λ is a unitary mapping of $\mathfrak{W}_\lambda{}^i$ onto $\mathfrak{W}_\lambda{}^j$ as was to be proved. This also proves that the dimensions of $\mathfrak{S}_\lambda{}^i$ and $\mathfrak{S}_\lambda{}^j$ are the same.

If this dimension is finite, the dimensions of $\mathfrak{S}_\lambda{}^i{}_1$ and $\mathfrak{W}_{\lambda\perp}$ are the same. Then there always exists a unitary mapping $U_{\lambda\perp}$ of $\mathfrak{W}_\lambda{}^i{}_\perp$ onto $\mathfrak{W}_\lambda{}^f{}_\perp$. Now we define an operator U in $\mathfrak{S}$.

$$U = \oplus_\lambda \left(U_\lambda \oplus U_{\lambda 1}\right) \tag{3.25}$$

Because of the unitarity of U_λ and $U_{\lambda\perp}$ and the decomposition, (3.23), U is obviously unitary. For any $\Psi \in \mathfrak{H}$,

$$U\Psi = \sum_\lambda \left(U_\lambda \Psi_\lambda{}^i + U_{\lambda\perp}\Psi_\lambda{}^i{}_\perp\right), \tag{3.26}$$

where

$$\Psi = \sum_\lambda \left(\Psi_\lambda{}^i + \Psi_\lambda{}^i{}_\perp\right), \Psi_\lambda{}^i \in \mathfrak{W}_\lambda{}^i, \Psi_\lambda{}^i{}_\epsilon \in \mathfrak{S}_\lambda{}^i{}_\perp, \tag{3.27}$$

is a unique decomposition of Ψ according to the first equation of (3.23). Since the subspace $\mathfrak{W}_\lambda$ of $\mathfrak{W}$ spanned by eigenvectors of $L = L_1 \otimes 1 + 1 \otimes L_2$ with the eigenvalue λ is mapped onto itself by $U, I/$ commutes with L. This completes the proof for the case where the dimension of $\mathfrak{S}_\lambda{}^i$ and $\mathfrak{W}_\lambda{}^j$ is finite.

If this dimension is infinite, then the dimensions of $\mathfrak{W}_\lambda{}^i{}_\lambda$ and $\mathfrak{W}_\lambda{}^j{}_\perp$ can be different. In such a case we introduce a new Hilbert space $\mathfrak{S}_2{}^r$ (on which the conserved quantity $L_2{}^r$ is defined) in such a way that the dimension of $\mathfrak{W}_\Lambda{}^r$ is at least the number of indices α where $\mathfrak{S}_\lambda{}^r$ is the subspace of $\mathfrak{S}^r \equiv \mathfrak{Y}_1 \otimes \mathfrak{S}_2{}^r$ spanned by the eigenstates of $L^r = L_1 \otimes 1 + 1 \otimes L_2{}^r$ with eigenvalues λ. Then since the dimension of $\mathfrak{S}_\lambda{}^i$ and $\mathfrak{S}_\lambda{}^f$ does not
exceed the cardinal number of the set of the indices α, $\mathfrak{W}_\lambda{}^{ir} \equiv \mathfrak{S}_\lambda{}^i{}_1 \oplus \mathfrak{W}_\lambda{}^r$ and $\mathfrak{S}_\lambda{}^{fr} \equiv \mathfrak{W}_\lambda{}^f{}_1 \oplus \mathfrak{S}_\lambda{}^r$ have the same dimension. Hence, there always exists a unitary mapping $U_{\lambda\perp}$ of $\mathfrak{S}_\lambda{}^{ir}$ onto $\mathfrak{S}_\lambda{}^{jr}$.

We are now in the position to construct the Hilbert space $\mathfrak{W}_2{}'$ and the unitary operator U for this case. $\mathfrak{W}_2{}'$ is taken to be $\mathfrak{W}_2 \oplus \mathfrak{W}_2{}^r$. $L_2{}'$ on $\mathfrak{W}_2{}'$ is taken to be $L_2 \oplus L_2{}^r$. $\mathfrak{W}'$ can be decomposed as

$$\mathfrak{Y}' = \oplus_\lambda \left(\mathfrak{W}_\lambda{}^i \oplus \mathfrak{S}_\lambda{}^{ir}\right) = \oplus_\lambda \left(\mathfrak{W}_\lambda{}' \oplus \mathfrak{W}_\lambda{}'^r\right). \tag{3.28}$$

U is defined as unitary mapping

$$U = \oplus_\lambda \left(U_\lambda \oplus U_{\lambda 1}\right) \tag{3.29}$$

Instead of (3.26), (3.27), we have, for any $\Psi \in \mathfrak{F}'$

$$U\Psi = \sum_\lambda \left(U_\lambda \Psi_\lambda{}^i + U_\lambda \Psi_\lambda{}^{ir}\right) \tag{3.30}$$

$$\Psi = \sum_\lambda \left(\Psi_\lambda{}^i + \Psi_\lambda{}^{ir}\right), \Psi_\lambda{}^i \in \mathfrak{W}_\lambda{}^i, \Psi_\lambda{}^{ir} \in \mathfrak{S}_\lambda{}^{ir}. \tag{3.31}$$

---

of the order of the dimension of $\mathfrak{W}_1$, provided that the latter is finite. Here we will not pursue the problem of such minimization, but we will only note that, if we do minimize the number of eigenvalues of L_2 to be used in the measuring apparatus, then $\mathrm{X}_{\mu\rho}$ will be nearly strictly determined and if that is the case, there is a fair chance that $\mathrm{X}_{\mu\rho}$ cannot be made macroscopically distinguishable any better than $\phi_{\mu p}$.

Then by the same argument as in the previous case, we can show the unitarity of U, and commutativity with I', where I' is defined as $I' \equiv L_1 \otimes 1 + 1 \otimes L_2'$.

We note that in our application of the Lemma, the number of the indices α is the same as the dimension of $\mathfrak{S}_1$.

29.4 VI.3 Optimal Measuring Apparatus by Yanse

Abstract

An upper limit for the accuracy of the measurement of a simple quantity which does not commute with a conserved quantity is obtained in terms of the "size" of the apparatus. The "size" of the apparatus is defined as the mean square value $\hbar^2 M^2$ of the conserved quantity for the apparatus which is, in the example chosen, the z component of the angular momentum. The measured quantity is the projection of a spin in a perpendicular direction. It is found that the probability of an unsuccessful measurement is at least $1/8M^2$.

29.4.1 1. Introduction

II' was shown recently that a quantum mechanical operator which does not commute with the operator of a conserved quantity can be measured only approximately. There is a finite probability that the measurement is unsuccessful, but this probability can be very small if the measuring apparatus contains a large amount of the conserved quantity. [1] It was shown, in particular, that if the product of the probability of an unsuccessful measurement and of the maximum value of the conserved quantity which is present in the measuring apparatus exceeds a certain value, no contradiction with the conservation law occurs. The objective of the present article is to find the "best" measuring apparatus for a given "size." The conserved quantity will not have an upper limit in the initial state of this; rather, we specify the mean-square value of the conserved quantity and ask for the minimum probability for an unsuccessful measurement, consistent with the prescribed mean square of the conserved quantity and, of course, the validity of the conservation law.

We require that the operator of the conserved quantity for the apparatus commute with the operator, by which the final state of the apparatus is measured. This condition is necessary because otherwise-as a

consequence of the result of our previous work-we cannot ascertain the result of the measurement exactly.

The condition to be obtained will be only a necessary one. In other words, for the given mean square of the conserved quantity, the probability of a malfunctioning of the apparatus cannot be smaller than the value to be calculated. Whether an apparatus with the specified properties is actually possible will not be decided. All that can be claimed is that the existence of such · an apparatus is not in conflict with the conservation law considered.

The quantity to be measured and the conservation law to be considered will be the same as in the first publication on this subject: The quantity is the component of the spin of a particle in a given direction; the conserved quantity, the angular momentum about a direction perpendicular to the aforementioned direction. It will be shown in Sec. 2 that the minimum probability for the malfunctioning of the apparatus is inversely proportional to the mean square of the conserved quantity, and the proportionality constant will be determined. Section 3 will contain a discussion of the results.

8

- On leave of absence from Sophia University, Tokyo, Japan. [1] E. P. Wigner, Z. Physik 133, 101 (1952); H. Araki and M. M. Yanase, Phys. Rev. 120, 622 (1960).

29.4.2 2. Minimization of the Malfunctioning Probability

We measure the x component of the spin of a particle with spin $\frac{1}{2}$; the z component of the spin of this particle is the additive conserved quantity. To make the computation simpler, we choose the eigenvalues of the z component as 0 and 1 and denote the corresponding eigenstates ψ_0 and ψ_1, respectively. Then eigenstates of the x component are $2^{-\frac{1}{2}}(\psi_0+\psi_1)$ and $2^{-\frac{1}{2}}(\psi_0-\psi_1)$. The state of the measuring apparatus before the measurement will be denoted by ξ. The measurement will result in a unitary transformation U in the Hilbert space of the combined system of the object and the measuring apparatus:

$U\left[2^{-\frac{1}{2}}(\psi_0+\psi_1)\xi\right] = 2^{-\frac{1}{2}}(\psi_0+\psi_1)X + 2^{-\frac{1}{2}}(\psi_0-\psi_1)\eta,$

$U\left[2^{-\frac{1}{2}}(\psi_0-\psi_1)\xi\right] = 2^{-\frac{1}{2}}(\psi_0-\psi_1)X' + 2^{-\frac{1}{2}}(\psi_0+\psi_1)\eta',$

where X, X', η, η' are the states of the measuring apparatus after the measurement.

From (2.1) and (2.2) we have

$$U(\psi_0\xi) = \psi_0 u + \psi_1 v, \tag{2.3}$$

$$U(\psi_1\xi) = \psi_0 w + \psi_1 z, \tag{2.4}$$

where

$$\begin{aligned} u &= \frac{1}{2}(X + X' + \eta + \eta'), \\ v &= \frac{1}{2}(X - X' - \eta + \eta'), \\ w &= \frac{1}{2}(X - X' + \eta - \eta'), \\ z &= \frac{1}{2}(X + X' - \eta - \eta'). \end{aligned} \tag{2.4a}$$

It follows from the conservation law for the z component of the angular momentum that

$$U(\psi_0\xi_\mu) = \psi_0 u_\mu + \psi_1 v_{\mu-1}, \tag{2.5}$$

$$U(\psi_1\xi_{\mu-1}) = \psi_0 w_\mu + \psi_1 z_{\mu-1}, \tag{2.6}$$

where we decomposed $\xi, u, v, w, z,$ into $\xi = \sum \xi_\mu$, $u = \sum u_\mu, v = \sum v_\mu, w = \sum w_\mu, z = \sum z_\mu$, the index μ being the eigenvalues of the z component of the angular momentum of the apparatus, and the ξ_μ, u_μ, etc., corresponding eigenstates. We normalize

$$(\xi, \xi) = 1 \tag{2.7}$$

After the measurement, the apparatus is separated from the object, and subject to the second measurement to distinguish the states corresponding to the states of the measured object. For this second measurement we require the following conditions. First, the two states X and X' should be the two orthogonal eigenstates of the operator N of the second measurement, i.e.,

$$(X, X') = 0. \tag{2.8}$$

Secondly, N should commute with the operator L_2 of the conserved quantity for the apparatus, otherwise we cannot measure N exactly, [1] i.e.,

$$[\Lambda', L_z] = 0. \tag{2.9}$$

This leads to the relation

$$(X_\mu, X_\mu{}') = 0, \tag{2.10}$$

the X_μ being eigenfunctions of both N' and L_z. Because of (2.4a) this can be written also as

$$(u_\mu + z_\mu, u_\mu + z_\mu) = (v_\mu + w_\mu, v_\mu + w_\mu)\,. \tag{2.10a}$$

In an ideal measurement, both η and η' would be zero. It is not possible to accomplish this, but we shall try to find the minimum ϵ of the probability that the measurement was unsuccessful, i.e., the minimum of

$$\begin{aligned}\epsilon &= (\eta, \eta) + (\eta', \eta') \\ &= \frac{1}{2}\left[(u-z)^2 + (v-w)^2\right] \\ &= \frac{1}{2}\left[\left(\sum u_\mu - \sum z_\mu\right)^2 + \left(\sum v_\mu - \sum w_\mu\right)^2\right],\end{aligned} \tag{2.11}$$

consistent with a definite "size" of the measuring apparatus, to be defined below. The conservation law, together with (2.5), (2.6), (2.7), and the unitary nature of U gives

$$\begin{aligned}(\xi_\mu, \xi_\mu) &= (u_\mu, u_\mu) + (v_{\mu-1}, v_{\mu-1}) \\ &= (w_{\mu+1}, w_{\mu+1}) + (z_\mu, z_\mu)\end{aligned} \tag{2.12}$$

$$\begin{aligned}1 &= (u,u) + (v,v) = \sum (u_\mu, u_\mu) + \sum (v_\mu, v_\mu) \\ &= (w,w) + (z,z) = \sum (w_\mu, w_\mu) + \sum (z_\mu, z_\mu)\end{aligned} \tag{2.13}$$

and

$$(u_\mu, w_\mu) + (v_{\mu-1}, z_{\mu-1}) = 0 \tag{2.14}$$

We define the "size" of the measuring apparatus as the mean square of the additive conserved quantity which we denote by M^2

$$\left(\xi, {L_z}^2 \xi\right) = \sum \mu^2 {\xi_\mu}^2 = M^2 \tag{2.15}$$

The problem is $_1$ therefore, to obtain the smallest value of ϵ consistent with Eqs. (2.12) to (2.15), the $\xi_\mu, u_\mu, v_\mu, w_\mu, z_\mu$, being otherwise arbitrary eigenstates of L_2 to the eigenvalue μ. The ξ_μ can be eliminated from (2.13) by means of (2.10) and one obtains

$$\sum \mu^2 \left(u_\mu^2 + v_{\mu-1}^2\right) = \sum \mu^2 \left(w_{\mu-1}^2 + z_\mu^2\right) = M^2. \tag{2.16}$$

We note that (2.14) can be always satisfied because no equation depends on the angles between the u_μ and w_μ, or the v_μ and $\tilde{z}_\mu$, except (2.14). It is easy to see that, in order to obtain the smallest possible ϵ at given $\|u_\mu\|, \|v_\mu\|, \|w_\mu\|, \|z_\mu\|$, the Hilbert vectors u_μ and z_μ must be parallel for all μ and the same applies for the vectors v_μ and w_μ.

To solve the preceding equations, we note that, because of (2.10a) and (2.12),

$$u_\mu + z_\mu = v_\mu + w_\mu, \tag{2.17}$$
$$u_\mu - z_\mu = \left({w_{\mu+1}}^2 - {v_{\mu-1}}^2\right) / \left(v_\mu + w_\mu\right), \tag{2.18}$$

where the u_μ, z_μ are now the lengths of the corresponding vectors (which are parallel), and the same epplies to v_μ and z_μ.

We introduce new variables s_μ, t_μ such that

$$w_\mu + v_\mu = s_\mu, \tag{2.19}$$
$$w_\mu - v_\mu = t_\mu. \tag{2.20}$$

If ϵ is small, M is large and the s_μ, t_μ can be considered to be continuous functions of μ. It can be verificd from
the solutions to be obtained that

$$\begin{aligned} s_\mu &= O\left(M^{-\frac{1}{2}}\right), \quad \partial s_\mu/\partial\mu = \dot{s}_\mu = O\left(M^{-\frac{1}{2}}\right), \quad \text{etc.;} \\ t_\mu &= O\left(M^{-\frac{1}{2}}\right), \quad \partial t_\mu/\partial\mu = \dot{t}_\mu = O\left(M^{-\frac{1}{2}}\right), \quad \text{etc.} \end{aligned} \tag{2.22}$$

Using these estimates, we obtain from (2.18), (2.19), (2.20)

$$u_\mu - z_\mu = \dot{\S}_\mu + i_\mu + O\left(M^{-7/2}\right). \tag{2.23}$$

whereas (2.11) becomes

$$\begin{aligned} \epsilon &= \frac{1}{2}\left\{\sum\left[\dot{s}_\mu + \iota_\mu + O\left(M^{-7/2}\right)\right]^2 + \sum {\iota_\mu}^2\right\} \\ &= \frac{1}{2}\sum\left[{\dot{s}_\mu}^2 + 2{\iota_\mu}^2 + 2\dot{s}_\mu\iota_\mu + O\left(M^{-5}\right)\right]. \end{aligned} \tag{2.24}$$

The s and t are still subject to the conditions (2.13) and (2.14) which now read
5

$$\frac{1}{2}\sum\left[s_\mu^2 + O\left(M^{-3}\right)\right] = 1, \tag{2.25}$$
$$\frac{1}{2}\sum\mu^2\left[s_\mu^2 + O\left(M^{-3}\right)\right] = M^2. \tag{2.26}$$

Since the t do not occur in these equations, the derivative of (2.24) with respect to t_μ will be zero at the mini mum for ϵ :

$$2l_\mu = -\dot{s}_\mu + O\left(M^{-7/2}\right). \tag{2.27}$$

Hence ϵ becomes

$$\epsilon = \sum\left[\frac{1}{4}{\dot{s}_\mu}^2 + O\left(M^{-5}\right)\right]. \tag{2.28}$$

Using $-\lambda$ and $2m^2$ as the Lagrange multipliers for (2.25) and (2.26), we obtain the Euler equation for s_μ

$$-\ddot{\varepsilon}_\mu + \left(4m^2\mu^2 - 2\lambda\right)s_\mu = 0, \tag{2.29}$$

where terms of lower order of magnitude have been omitted. The solution of (2.29) is

$$s_\mu = c \exp\left(-m\mu^2\right); \quad c^2 = 2(m/\pi)^{\frac{1}{2}}. \tag{2.30}$$

This already satisfies the normalization condition (2.25). The condition (2.26) gives

$$M^2 = 1/4m, \tag{2.31}$$

and this gives, finally, for the probability (2.28) of an unsuccessful measurement

$$\epsilon = 1/8M^2, \tag{2.32}$$

for a given M. Tracing through the omitted low-order terms, one finds that (2.32) is accurate up to terms of the order $1/M^3$.

29.4.3 3. Conclusions and Discussions

(1) The relation (2.32) tells us that the probability of an unsuccessful measurement is $1/8M^2$, if one uses the "best possible" apparatus with given M^2. Therefore,
neglecting terms of the order $1/M^2$, the inequality

$$\epsilon > 1/8M^2 \tag{3.1}$$

holds. In other words, with given M^2, we cannot make the probability of unsuccessful measurement smaller than $\hbar^2/8M^2$ (in dimensionless units). This limitation of the measurement is not the consequence of an uncertainty relation for the simultaneous measurement of two noncommuting operators, but the consequence of the existence of the additive conserved quantity whose operator does not commute with the single operator to be measured.
(2) We required the condition $(X_\mu, X_\mu') = 0, (2.10)$, so that the conservation law does not interfere with the possibility of distinguishing X and X'. However, if we loosen this condition and require only $(X, X') - 0$, we obtain the same value for ϵ except for terms of order $1/M^3$ or lower. However, in this case the second measurement (which distinguishes X and X') can be carried out only approximately, and the total probability for an unsuccessful measurement becomes larger.
(3) The theory of measurement, as described by von Neumann, [2] contains no limitation for the size of the measuring apparatus. As we have seen, there always are such limitations unless the operator to be measured commutes with all the operators of additive conserved quantities. [3] Recently the macroscopic character of the measuring apparatus has been studied in detail by several auihors, [1] but no quantitative conditions have been established before.

[2] J. von Neumann, Mrathematical Foundation of Quantum Mechanics (Princeton University Press, Princeton, New Jersey, 1955).

[3] See reference 1 . We will discuss this problem, "exactly measurable operators," in another article.

[4] G. Ludwig, Die Grundlagen der Quantenmechanik (SpringerVerlag. Berlin, 1954), Chap. V; H. S. Green, Nuovo cimento 9, 880 (1958); P. K. Feyerabend, Observation and Interpretation, edited by S. Koerner (Butterworth's Scientific Publications, L.t.d., Lodon, 1957), p. 121, II. Wakia, Progr. Theorei. Mys. (Kyoto) 23, 32 (1960); H. Margenau (to be published); S. Watanabe, Revs. Modern Phys. 27, 179 (1055).

29.5 VI.4 Time in the Quantum Theory and the Uncertainty Relation for Time and Energy by Aharonov, Bohm

Abstract

Because time does not appear in Schrödinger's equation as an operator but only as a parameter, the timeenergy uncertainty relation must be formulated in a special way. This problem has in fact been studied by many authors and we give a summary of their treatments. We then criticize the main conclusion of these treatments; viz., that in a measurement of energy carricd out in a time interval, Δt, there must he a minimum uncertainty in the transfer of energy to the observed system, given by $\Delta(E' - E) \geqslant h/\Delta t$. We show that this conclusion is erroneous in two respects. First, it is not consistent with the general principles of the quantum theory, which require that all uncertainty relations be expressible in terms of the mathematical formalism, i.e., by means of operators, wave functions, etc. Secondly, the examples of measurement processes that were used to derive the above uncertainty relation are not general enough. We then develop a systematic presentation of our own point of view, with regard to the role of time in the quantum theory, and give a concrete example of a measurement process not satisfying the above uncertainty relation.

29.5.1 1. Historical Summary of the State of the Problem of Time Measremenent Inv the Quantum Theory

AS is well known, the uncertainty relations in quantum mechanics can be regarded in two closely related ways. First of all, they are a direct mathematical consequence of the replacement of classical numbers by operators, and of adding the basic principle that the statistical distributions of the corresponding observables can be obtained by means of the usual formulas from the wave function and its probability interpretation. [1] Secondly, however, it can be shown by analyses such as that of the Heisenberg microscope experiment that they are also limitations on the possible accuracy of measurements. [2]

These considerations apply to observables such as x, p, and H. With regard to the measurement of time, however, a further problem appears, because time enters into Schrödinger's equation, not as an operator (i.e., and "observable") but rather, as a parameter, which is a " c " number that has a well defined value. Nevertheless, the uncertainty principle, $\Delta E \Delta t \geqslant h$, is generally accepted as valid, even though it is not deduced directly from commutation relations in the way described above.

The justification of the time-energy uncertainty relationship has been attempted in several ways. (We shall restrict ourselves here entirely to a discussion of the nonrelativistic case, since the theory of relativity has no essential relationship to the measurement problems that we are going to treat in this paper.)

First, one can begin with the wave function

$$\psi(x,t) = \sum_E C_E \psi_E(\mathbf{x}) e^{-iEl/\hbar} \tag{1}$$

- Now at Brandeis University, Waltham, Massachusetts.

[1] The uncertainty relations are obtained in this way using Schwarz's inequality with the expressions for

$$\left\langle (A - \bar{A})^2 \right\rangle_{\text{av}} \left\langle (B - \bar{B})^2 \right\rangle_{\text{av}} = (\Delta A)^2 (\Delta B)^2.$$

See, for example, D. Bohm, Quantum Theory (Prentice-Hall, Inc., Englewood Cliffs, New Jersey, 1951), p.p. 205-206.

[2] W. Heisenberg, The Physical Principles of the Quantum Theory (Dover Publications, New York, 1930), Chap. 2.

where $\psi_E(x)$ is the eigenfunction of the Hamiltonian H of the system belonging to the eigenvalue

E, and C_E is an arbitrary coefficient. If we consider a wave packet of width ΔE in energy space (i.e., ΔE is the range in which $|C_E|$ is appreciable), it immediately follows from the properties of Fourier analysis that $(\Delta E)r \geqslant h$, where τ is the time during which the wave packet does not change significantly (r may be regarded as the mean life of the state in question [3]).

The above is a discussion in terms of the Schrödinger representation. Mandelstamm and Tamm [4] have formulated what is, in essence, the same point of view but it is expressed in the Heisenberg representation. They consider a dynamical variable A, which is a function of the time (e.g., the location of the needle on a clock dial or the position of a free particle in motion) and which can therefore be used to indicate time. If ΔA is the uncertainty in A, then the uncertainty in time is

$$\Delta t = \Delta A / \left| \langle \dot{A} \rangle_{\text{av}} \right| ,$$

provided that A does not change significantly during the time, Δt, and that $\Delta \dot{A} / \left| \langle \dot{A} \rangle_{\text{av}} \right|$ is negligible. From the relation

$$\Delta .4 \Delta H \geqslant |\langle (.1, H) \rangle_{\text{av}}| = \hbar \, |\langle A \rangle_{\text{av}}| ,$$

we obtain

$$\Delta .1 \Delta I I'_j \langle \dot{\Lambda} \rangle_{\text{av}} = \Delta I \Delta I I \geqslant h. \tag{2}$$

Since H represents the Hamiltonian of the isolated system, ΔH is also equal to ΔE, the uncertainty in energy of that syntem.

It should be noted that the method proposed by Mandelstamm and Tamm can actually lead to a determination of time, only when the system is not in a stationary state; i.e., only when the wave function takes the form of a packet, consisting of a linear superposition of stationary states. In other words, the ΔH appearing in equation (2) is determined by the range of energies in the wave packet. In this way, the relation of the Mandelstamm and Tamm treatment to the Schrödinger representation is made clear.

The above is then a discussion of the relation $\Delta E \Delta l \geqslant h$ insofar as this has been obtained from the mathematical formalism of the quantum theory (i.e., the wave function, operators, and probability interpretation). Naturally, as is necessary in the case of observables such as x and p, this uncertainty relation must also be analyzed in terms of the interaction of the measuring apparatus with the observed system. Landau and Peierls, [5,6] for example, do this by considering a special example, in which the momentum of a free particle is measured by means of a collision with a heavy test particle (also free). To simplify the problem they consider a case in which the measuring particle is a perfectly reflecting mirror, and discuss only the movement in one dimension (perpendicular to the mirror). They then apply the laws of conservation of energy and monenium, which are

$$p' + P' - (p + P) = 0 \tag{3a}$$

$$E' + \epsilon' - (E + \epsilon) = 0 \tag{3b}$$

where lower case letters refer to the observed particle, capitals to the test particle, unprimed quantities to values before collision, and primed quantities to values after collision. Because $E = P^2/2M, \epsilon = p^2/2m$, one can solve for the momentum of the observed particle before and after collision, in terms of the corresponding momenta of the test particle.

[83] V. Fock and N. Krylov, J. Phys. (U.S.S.R.) 11, 112 (1947), present a more detailed account of the lifetime of a state.

[4] I. Mandelstamm and I. Tamm, J. Phys. (U.S.S.R.) 9, 249 (1945).

In order to define the time of measurement, Landau and Peierls [5] (and also Landau and Lifshitz) [6] consider the case of a time-dependent interaction between the particle and the mirror, which lasts for some known period of time, Δt. This period Δt, which is the uncertainty in the time of measurement, then implies (e.g., according to perturbation theory) an uncertainty in the energy of the combined system consisting of observed particle and mirror, of magnitude $h/\Delta l$, resulting from the time-dependent interaction. Instead of Eq. (3b) for the exact conservation of energy, we must therefore write

$$|\epsilon' + E' - (\epsilon + E)| \geqslant h/\Delta l. \tag{3c}$$

Evidently the momentum of the test particle before and after collision can be measured with arbitrary accuracy, so that $\Delta P = \Delta P' = 0$. As a result, we obtain from Eq. (3a), $\Delta p = \Delta p'$; and from (3r), we have

$$\Delta\,(\epsilon' - \epsilon) \geqslant h/\Delta l \tag{4}$$

Since $\epsilon = p^2/2m$, we can also write the above result as

$$(v' - v)\,\Delta p \geqslant h'_{/}\Delta l. \tag{5}$$

(Note that although Δp itself may be very small, there

is still a minimum uncertainty in energy transfer, because the change of velocity will then become very large, if Δt is finite.)

Landau and Peierls therefore conclude that there is an uncertainty relation between the energy transferred to the system and the time at which the energy is measured. This means that the energy of the observed system cannot be measured in a short time, without changing it in an unpredictable and uncontrollable way. In other words, energy measurements carried out in short periods of time are not reproducible.

Fock and Krylov [3] criticize the derivation of the above results, but come to essentially the same conclusion. In effect, they do not accept the definition of the time of measurement by means of a time-dependent potential of interaction between the two particles. This is because in a real collision, there is no such time-dependent potential. Rather, the time of collision is determined by the movement of the particles themselves, in such a way that one of them serves as a clock. Let us suppose that it is the test particle which fulfills this function. This particle defines the time, l, as that at which it passes a definite point, X, by the equation, $t = X/V$. The time, as defined in this way, has an uncertainty $\Delta t = \Delta X/V$ (provided, as will actually be the case in our example, that $\Delta V/V \ll 1$).

In order to define the time of collision, we must have some information about the initial location of the observed particle, as well as that of the test particle. For simplicity, let us suppose that the initial velocity of the test particle is so much higher than that of the observed particle that the latter can be regarded as essentially at rest until the collision. The mean initial position x of the observed particle will be taken to be at the origin, while the uncertainty in this position is represented by Δx. Evidently we must choose $\Delta x < \Delta X$, if the location of the test particle is to serve as a definition of the time of collision. Therefore

$$\Delta t = \Delta X/V \geqslant \hbar/(\Delta P)V = \hbar/\Delta E$$

(This is just the well-known uncertainty relation between the energy of the test particle and the time that is defined by the movement of its coordinate.)

[85] L. Landau and R. Peierls, Z. Physik 69, 56 (1931).

[6] See also L. Landau and E. Lifschitz, Quantum Mechanics (Pergamon Press, New York, 1958), pp. 150-153.

Fock and Krylov then point out that in this case, the laws of conservation of energy and momentum are both satisfied exactly, so that Eqs. (3a) and (3b) can be used directly, while the approximate form ($3c$) for the conservation of energy is not to be applied here (since perturbation theory no longer has any relevance to the problem.) From (3a), we oblain

$$\Delta\left(p-p'\right)=\Delta\left(P-P'\right)$$

If V is chosen large enough, we can for a given $\Delta t>\hbar/V\Delta P$ make ΔP and $\Delta P'$ arbitrarily small, and, as a result, we can likewise make $\Delta\left(p-p'\right)$ as small as
we please. From Eq. (3b), it then follows that

$$\Delta\left(\epsilon'-\epsilon\right)=\frac{\left(p'-p\right)}{m}\frac{\Delta\left(p'+p\right)}{2}=\left(v'-\vartheta\right)\Delta p=\Delta\left(\epsilon'-\epsilon\right)\geqslant\frac{\hbar}{\Delta l},$$

where we have used the result that $\Delta\left(p'-p\right)$ is negligible. The above is exactly the same Eq. (5) as that obtained by Landau and Peierls, but the uncertainty in energy transfer to the observed system is now deduced on the basis of the fact that the (time-dependent) position of one of the particles is used to define the time of collision.

Fock and Krylov then go on to criticize the approach of Mandelstamm and Tamm, suggesting that it is incomplete. They assert that by means of the wave function and the operators of the observed system, one can discuss only the statistical features of any measurement. In order to discuss an individual measurement process, they refer to what they call "Bohr's uncertainty relation," $\Delta\left(\epsilon'-\epsilon\right)\Delta t>h$, where ϵ and ϵ' are the actual values of the energy of an individual observed system before and after measurement.

To clarify this distinction between the statistical uncertainty relations discussed by Mandelstamm and Tamm, and the Bohr relation, they point out that, for example, in observation of a state with lifetime τ (as described by its wave function), one can make measurements in times much shorter than τ. Therefore, it is necessary to distinguish between the time intervals defined by the wave function of the observed system, and the time interval representing the actual duration of an individual measurement. The time interval defined by the wave function has in measurements generally only a statistical significance.

Even if one treated the measurement process by means of a many-body Schrödinger equation, including the apparatus coordinates, the same distinction would arise. For it would the necessary to observe the combined system by means of additional apparatus; and here too, there will be a "Bohr uncertainty principle" for the individual observation and a statistical uncertainty principle following from the wave function, which applies to an ensemble of cases. To treat the apparatus by quantum theory is, in effect, to push back the well known "cut" between classical and quantum sides another stage. While it is always permissible and sometimes convenient to do this, it cannot change the content of the theory.

Let us now sum up the problem. Mandelstamm and Tamm propose a mathematical operator uncertainty relation between energy and time, as determined by the wave function. Fock and Krylov regard such a treatment as incomplete, because it applies only statistically to a large number of measurements, and because within it one cannot even consider the question of the interval of time needed to carry out an individual measurement. To complete the treatment, they call attention to the "Bohr uncertainty relation" (discussed also by Landau
and Peierls, [5] as well as by Landau and Lifshitz [6]) which applies to individual measurements, and which refers to the relation between the error in the measurement of energy and the duration of the measurement process. While criticizing some of the methods of Landau and Peierls, they agree with the essential conclusion that energy cannot be measured in arbitrarily short periods of time, without introducing uncertainties, according to the relation $\Delta\left(\epsilon'-\epsilon\right)\geqslant h/\Delta t$.

29.5.2 2. Criticism of Commonly Accepted Interpretations of the Time-energy Uncertainty Relation

The main conclusion of Landau and Peierls, [5] Landau and Lifschitz, [6] and Fock and Krylov [3] (given in Sec. 1), viz., that energy cannot be measured in a short time without introducing an uncertainty in its value, represents a very widely accepted interpretation of the time-energy uncertainty relation. This conclusion is, as we shall show, erroneous, the error being based in part on an inadequate formulation of Bohr's point of view concerning measurement, and in part on the use of an illustrative example of a measurement process, that was not sufficiently typical of the general case of such a measurement. (In fact, in Sec. 4 we shall give a counterexample, in which the energy of a particle is measured to arbitrary accuracy in as short a time as we please).

With regard to Bohr's point of view concerning measurements, it is important to stress here his continual insistence that the minimum ambiguities in the results of any individual measurement process (in the sense of what Fock and Krylov called the "Bohr uncertainty relations") are always exactly the same as the minimum ambiguities in the possibility of definition in the mathematical theory of the observables that are being measured. [7] (These latter ambiguities are, of course, the "statistical" uncertainty relations referred to by Fock and Krylov.)

The ambiguities in the results of individual measurements are regarded as originating in the indivisible quantum connections of the object under investigation to the apparatus (and indeed to the whole universe), which give rise to a minimum ambiguity in the degree to which well-defined classical properties (e.g., position and momentum) can be assigned to the object as a result of any such measurement. [8] In addition, however, the result of each measurement defines a "quantum state" of the observed system, specified by its wave function. This wave function is, of course, not a representation of an individual system, but it implies, in general, only a set of statistical predictions concerning the results of possible measurements. Nevertheless, if these predictions were such that the minimum ambiguity in the definition of the results of an individual measurement were less than the minimum statistical

fluctuation implied by the mathematical theory, then there would be a contradiction. Vice versa, if they were such that the minimum ambiguity in the result of an individual measurement were greater than the minimum statistical fluctuation as described above, then this would lead to an arbitrary restriction, not related in any general way to the mathematical formalism, a restriction that evidently has no place in a coherent over-all framework of theory. Moreover, one could, in general, expect that with sufficient effort, it would be possible to find an example of an individual measurement process with the same minimum ambiguity as that implied by the formalism; and if such a process is found, then the supposedly greater minimum ambiguity in the results of an individual measurement will be contradicted. For these reasons, it is necessary to consider the statistical and individual uncertainty relations as two equally essential sides of what is basically the same limitation on the precise definability and measurability of the state of any system. In other words, as Bohr [9] has stressed, there can be no limitation on individual measurements that cannot also be obtained from the mathematical formalism and the statistical interpretation.

There is no question that all the above considerations apply for common examples of the uncertainty principle (e.g., x and p). However, as we pointed out in Sec. 1, time enters into Schrödinger's equation only as a parameter, so that there is no straightforward way to apply these ideas to the time-energy uncertainty relation. Of course, we can, with Mandelstamm and Tamm, obtain an uncertainty relation between the lifetime of a state of the observed system and its energy. But let us recall here that (as pointed out by Fock and Krylov), the operators of the

[87] N. Bohr, Die Naturwissenschaften, 251 (1928).

[8] W. Heisenberg, Physics and Philosophy (Allen and Unwin, London, 1959), Chap). 3.

observed system have no connection whatsoever with the duration of the measurement process (which is evidently determined, in general, by the apparatus). Keeping this fact in mind, let us now raise the question of whether there can be a genuine uncertainty relation between the energy transferred to the observed system and the time at which the measurement took place (as has been suggested by Landau and Peierls, Fock and Krylov, and other authors).

In accordance with Bohr's point of view on the subject, as we have described it above, we are led to point out that one cannot safely regard any given uncertainty relations as representing a real limitation on the accuracy of all possible measurements of the quantities under discussion unless the relationship has been shown to follow from the mathematical formalism. On the other hand, all of the authors referred to above seem to be satisfied to establish the time-energy uncertainty relations as applying to individual measurements by what Fock and Krylov called "illustrative examples." Such a point of view would imply, of course, that the uncertainty relations applying to individual measurements could in principle, have a basis that is independent of the satistical relations obtainable from the mathematical formalism. As we have already pointed out, however, such a procedure is arbitrary and therefore subject to the continual danger of being contradicted by the development of new examples of measurement processes, which reduce the ambiguity down to the minimum allowed by the formalism. (For, as is quite evident, there is no way to be sure that conclusions obtained from an illustrative example have universal validity).

It follows from the above discussion that to complete the treatment of the time-energy uncertainty relation, it is necessary to develop a method of showing how the time of measurement and the energy transferred in this measurement are to be expressed in terms of suitable operators. The method that we shall use in this paper starts from our discussion of the example first treated by Landau and Peierls, and then by Fock and Krylov; viz., the one in which the energy of a free particle is measured by collision with another particle. As we saw in Sec. 1, in such an interaction, the time of collision is determined physically by the state of some system which serves as a clock. In the example of Fook and Krylov, it is determined by the position of the test particle (which was taken to be free). Now, for any system, one can define a Hermitian operator representing such a time. In the case of a free particle, this is

$$t_c = \frac{y}{z'_y} = \frac{1}{2} M \left(\begin{array}{cc} 1 & \\ y^- & + \frac{1}{p_n} \\ p_y & \end{array} \right) \tag{7}$$

where y and p_y are respectively position and momentum of the particle in question. [10]

The commutation relations between the above operator and the Hamiltonian, H_c, of the "clock" in question are (as can easily be verificd for the case of a free particle, for which $H_c = {p_y}^2/2,$ K),

$$[H_c, t_c] = i\hbar. \tag{8}$$

This procedure is evidently very similar to that of Mandelstamm and Tamm. However, they discussed only the operators of the observed system, and obtained an uncertainty relation (2) between the energy of this system and the "inner" time as defined by dynamical variables in this system (e.g., the lifetime of a state). On the other hand, we are applying the relations (8) to the energy, E_c, of the "clock" in the apparatus, and to the time, l_l, of measurement as determined by this clock.

Since the time of measurement can be represented by an operator, t_c, belonging only to the observing apparatus, it follows that this time must commule with every operator of the ubserved system and, in pu-licular, with its IIamillonian. There is therefore no reason inherent

[89] N. Bohr (private communication).

in the principles of the quantum theory why the energy of a system cannot be measured in as short a time as we

please. (Recall, however, that in accordance with the treatment of Mandelstamm and Tamm, any such a measurement of the energy of the observed system to an accuracy ΔE must leave the "inner" time undefined to $\Delta t \geqslant \hbar/\Delta E$).

In view of the above discussion, it is evident that the usual treatment of the energy-time uncertainty relation (e.g., as discussed by Fock and Krylov) must be in some way erroneous. Since the particular illustrative example chosen by all the authors cited here (which is, in fact, the one usually given) has in fact been treated correctly, it follows that the mistake must be that this example is not sufficiently typical of the general case. And, indeed, as we shall see in Sec. 4, one can suggest more general methods of measurement of energy, which do not lead to the above limitation. In this way, we confirm our conclusion, based on general considerations regarding the principles of the quantum theory, that it is always possible to obtain true limitations on the measurability of any observable from the mathematical formalism, and that any other limitations that are added to these are arbitrary restrictions, which can eventually be contradicted, if further examples of measurement processes are sought. [11]

Finally, it is instructive to point out that problems similar to those connected with the time-energy uncertainty relations arise in the more familiar example of the position momentum relationship, $\Delta p_x \Delta x \geqslant \hbar$. To bring out the analogy, we can ask ourselves whether the momentum of a particle can be measured to arbitrary accuracy by means of an apparatus, which is localized in space. (Here, p_x takes the place of E, while the region of space in which the apparatus is located takes the place of the duration, Δt, of the measurement.) At first sight, it may seem that if the apparatus is localized in a very small region of size ΔX, the momentum of a particle cannot be measured to an accuracy greater than $\Delta p_x = h/\Delta X$. This, however, is not the case, because, what is defined here is the coordinate, X, of the apparatus, and not that of the measured particle, x. Since p_x commutes with X, there is no inherent limitation on how accurately it can be moasured, if X is defined.

To illustrate such a possibility, consider the measurement of the momentum of a photon, by measuring its energy and using the relation $p = E/c$. (This is analogous to the measurement of energy of a particle by measuring its momentum and using the relation $E = p^2/2M$.) We can do this by means of an atom which is very highly localized, provided that this atom has a sharp level, excited above the ground state by the amount $E = pc$. If the photon has the appropriate energy, it will be absorbed and eventually reemitted (being delayed and perhaps scattered). It is observable whether this happens or not. If it does happen, then this provides a measurement of the energy, and through this, of the

momentum. It is evident that the uncertainty in this momentum has no essential relation to the size of the atom, but only to the lifetime of the excited state. The momentum has therefore been measured by an apparatus, which is as localized in space as we please. (Of course, the position of the photon after the measurement is over is indeterminate, just as happens with "inner" time variables in the analogous case of time measurement.)

29.5.3 3. Treatment of Time of Measurement in Terms of the Mathematical Formalism of the Quantum Theory

We saw in Sec. 1 that (as pointed out by Fock and Krylov [3]) there is a need to make a careful distinction between the time at which a measurement takes place and the time as

[810] There is a singularity for $p_y = 0$, but it is easily shown that this will be unimportant if p_y is large enough, as will be the case in our applications.

[811] This conclusion, the validity of which is fairly evident, will be obtained again in Sec. 3 from a more detailed discussion of the mathematical formalism.

defined by the wave function and operators of the observed system (e.g., the lifetime of an excited state). In Sec. 2, we showed how such a distinction can be represented within the mathematical formalism of the quantum theory by considering as operators certain variables that have hitherto usually been associated with the observing apparatus; viz., those variables determining the time at which interaction between the apparatus and the observed system takes place. This implies, of course, that the wave function must now be extended, so as to depend on these latter variables, It is equivalent to placing the "cut" between observing apparatus and observed system at a different point.

It is well known that while there is a certain kind of arbitrariness in the location of this cut, it is not completely arbitrary. For example, in the treatment of the energy levels of a hydrogen atom, one can, in a certain approximation, regard the nucleus as a classical particle in a well-defined position. If, however, the treatment aims at being accurate enough to take the reduced mass into account, both electron and nucleus must be treated quantum-mechanically, and the cut is introduced instead between the atom as a whole and its environment. The place of the cut therefore depends, in general, on how accurate a treatment is required for the problem under discussion. Of course, it follows that once a given place of the cut is justified, then it can always be moved further toward the classical side without changing the results significantly.

If we are interested only in discussing what Fock and Krylov called the "Bohr uncertainty relation" (the one referring to an individual measurement of energy and time), then we are justified in placing the physical variables that determine the time of the measurement on the classical side of the cut. For, as is quite evident, in this aspect of the uncertainty relations, these variables are by definition regarded as classical, in the sense that their uncertainty represents only an inherent ambiguity in the possibility of defining the state of an individual system. We have seen in Sec. 2, however, that according to the Bohr point of view, every uncertainty relation that appears in this way must also be able to appear as a statistical fluctuation in a corresponding operator, which must, of course, be calculated from an appropriate wave function. To discuss this side of the uncertainty relations, it is clear that we must change the position of the cut, so that the corresponding variables now fall on the quantum-mechanical side.

In the subsequent discussion of how the uncertainty relations appear in the mathematical formalism, we shall begin with the case in which the time determining variables are placed on the classical side of the cut. In this case, the time variables can be reflected in the Schrödinger equation only in the time parameter l which can, of course, have an arbitrarily well-defined value. This time parameter is related to measurement in several ways.

First of all such a relation comes about in the preparation of a system in a definite quantum state, and in observations carried out later on that system. Consider, for example, a quantum state prepared at a time determined by means of a shutter (which we are, of course, now regarding as being on the classical side of the cut). There must be some relationship between the time, t_a, at which the shutter functions and the time parameter, t appearing the Schrödinger's equation. Indeed, if the Hamiltonian of the observed system does not depend on time, then it is easily seen that the wave function takes the form

$$\psi = \psi\left(\mathbf{x}, l - l_s\right), \tag{9}$$

where ψ is a solution of Schrödinger's equation for the system in question. The form of ψ is determined by choosing that solution which at $l = l_s$ becomes equal to the function, $\psi_0(\mathbf{x})$, representing the quantum state in which the "preparing" measurement leaves the system. Then, when an observation is made, the time t_m, of the measurement is likewise determined by suitable variables on the classical side of the cut. The probability of any given result is, of course, computed in the wellknown way from the wave function, $\psi = \psi\left(\mathbf{x}, t_m - t_s\right)$.

It is clear that as far as this one-body treatment is concerned, there is certainly nothing in the formalism which would prevent the system under discussion from being either prepared or

observed in a state of definite energy, when t_m and t_s are as well defined as we please. Thus, if the system is in a state of definite energy, E (so that the uncertainty, ΔE, in its energy is zero, while the lifetime $\tau > \hbar/\Delta E$ of the state is infinite), its wave function, $\psi - \psi_k(\mathbf{x})e^{-iE_{t/h}}$ [where $\psi_E(\mathbf{x})$ is the eigenfunction of the Hamiltonian operator belonging to the eigenvalue, E] is evidently able to represent such a state, no matter what value is given to %. A wave function of this kind is therefore evidently compatible with the statement that at some time, $l = l_s$, the system was prepared in the eigenstate of the energy represented by $\psi_E(\mathbf{x})$. Thus, in the one-body treatment alone, no reason for an uncertainty relation between the energy of the system and the time of measurement can be found. And
this is indeed basically the reason why Fock and Krylov were led to postulate such an uncertainty relation independently, and to try to justify this relationship by means of illustrative examples of measurement processes (see Sec. 1).

Let us now go on to consider the time-energy uncertainty relation from the other aspect, in which the variables determining the time of measurement are placed on the quantum-mechnical side of the cut. In this case, we must introduce these variables into the wave function, so that we are in this way led to a manybody Schrödinger equation. Let us recall, however, that the "cut" has not been abolished, but merely pushed back another stage. Thus, as was pointed out in the discussion of the treatment of Fock and Krylov given in Sec. 1, there is implied an additional observing apparatus on the classical side of the cut, with the aid of which the many-body system under discussion can be observed. The probabilities for the results of such observations are determined by the wave functions, which take the form

$$\Psi = \Psi\left(\mathbf{x}, y_i, t\right) \tag{10}$$

where y_i, represents the apparatus variables on the quantum-mechanical side of the cut (which include those that describe the time of measurement). The time parameter i here plays a role similar to that which it had in the one-body problem; viz., through it the time frame on the large-scale classical side of the cut is brought into relationship with the quantum mechanical formalism by means of suitable observations.

We shall now consider as an example of the approach described above, the measurement of energy and time by means of a collision of two particles, as treated in Sec. 1. The initial wave function of the combined system is, for this case, a product of two packet functions, one representing the test particle coming in with a very high velocity, V, and the other representing the observed particle, essentially at rest (with a velocity that is negligible in comparison to V) and with its center at the origin. After the collision, it is well known [12,13] that the wave function becomes a sum of products of such packets, conclated in such a way that an observation of the properties of the test particle can yield information about the particle under discussion.

As far as this particular example is concerned, it will not be relevant here to go into a more detailed discussion of the problem of solving Schrödinger's equation. All that is important here is that as we saw in Sec. 2, the time of collision is given essentially by the operator,

$$t_c = \tfrac{1}{2}M \begin{pmatrix} 1 & & 1 \\ y+ & + & \\ p_y & & p_y \end{pmatrix}$$

(where y and p_y refer to the position and momentum of
the test particle, respectively), so that the operator, l_c, commutes with the Hamiltonian, H_s, of the observed system. As a result, there is, as we have already stated in Sec. 2, no

[8][12] See reference 1, Chap. 22.
13 J. von Neumann, Mathematical Foundations of Quantum Mechanics (Princeton University Press, Princeton, New Jersey, 1955), Chap. 6.

uncertainty relation between the time of measurement and the energy of the observed system. But in the treatment that we are now using, we have obtained this result by allowing the variables determining the time of measurement to fall on the quantummechanical side of the cut. (As was to be expected, of course, the actual physical consequences of the theory do not depend on which side of the cut these variables are placed.)

In the example given above, the samc apparatus was used to determine both the time of measurement and the momentum of the particle. However, it is possible, and in fact frequently advantageous, to consider a more general situation, in which the time determining variables are separated from those which are used to measure other quantities (such as momentum). This, in fact, would be the correct way of completing the treatment of the example given by Landau and Peierls [5,6] (see Sec. 1), in which the time of measurement was determined by an interaction between the test particle and the observed particle which was assumed to last for some interval Δt.

If there is a time-dependent interaction between apparatus and observed system which lasts for an interval Δt, then the Schrödinger equation will have to have a corresponding potential, which represents this interaction. The form of this potential will depend on where we place the cut.

If the apparatus determining the time of interaction is taken to be on the classical side, then the potential will be a certain well defined function of time, which is nonzero only in the specified interval of length Δt. We may write this potential as

$$V = V(\mathbf{x}, y, t), \tag{11}$$

where $\mathbf{x}$ represents the coordinate of the observed particle, and y that of the test particle. This is indeed the usual way by which measurements are represented in the mathematical formalism. [12,13]

In the next section we shall apply this method in order to treat a specific example, in which it will be shown in detail that the energy of a system can be measured in an arbitrarily short time.

If, on the other hand, the variables determining the time of interaction are placed on the quantum mechanical side of the cut, then we cannot regard the potential as a well-defined function of time. Instead, we must write

$$V = V(\mathbf{x}, y, z), \tag{12}$$

where z is the variable that determines the time of interaction.

If the particles determining the time of interaction are heavy enough, then they will move in an essentially classical way, very nearly following a definite orbit,
$Z = Z(t)$. To the extent that this happens, we obtain, as a good approximation,

$$V'(\mathbf{x}, y, z) = V'(\mathbf{x}, y, z(l)). \tag{13}$$

To treat this problem mathematically, we begin with the Schrödinger equation for the whole system.
$i\hbar\frac{\partial\Psi}{\partial t}(\mathbf{x}, y, z, t) = [H_p + H_y + H_z + V(\mathbf{x}, y, z)]\,\Psi(\mathbf{x}, y, z, t)$,
where H_p represents the Hamiltonian of the observed particle, H_y that of the apparatus, H_z that of the timedetermining variable, z. We must then show the equivalence of this treatment with that obtained by placing the time-determining variable on the classical side of the cui. Tu du this, it is sufficient to demonstrate that in a suitable approximation, equation (14) leads to the timedependent Schrödinger equation for the $\mathbf{x}$ and y variables alone, viz.,

$$i\hbar\frac{\partial\psi}{\partial t}(\mathbf{x}, y, t) = [H_p + H_y + V(\mathbf{x}, y, z(l))]\,\psi(\mathbf{x}, y, t) \tag{15}$$

We shall simplify the problem [14] by letting the time determining variable be represented by a heavy free particle mass M, for which we have $H_z = {p_z}^2/2M$. We suppose that the initial state of the time-determining variable can be represented by a wave packet narrow enough in z space, so that $\Delta t = \Delta z/|\dot{z}|$ can be made as small as is necessary. This packet is

$$\Phi_0(z,t) = \sum_{p_z} C_{p_z} \exp\left\{\frac{i}{\hbar}\left[zp_z - \frac{p_z^2}{2M}t\right]\right\}. \tag{16}$$

Because M is very large, the wave packet will spread very slowly, and to a good approximation, we shall have

$$\Phi_0(z,t) = \Phi\left(z - v_z l\right) \exp\left\{\frac{i}{\hbar}\left[\bar{p}_z z - \frac{(\vec{p_z})^2}{2M}t\right]\right\}, \tag{i7}$$

where $v_\varepsilon = \bar{p}_z/M$ is the mean velocity, and $\Phi\left(z - v_z l\right)$ is just a form factor for the wave packet which is, in general, a fairly regular function which varies slowly in comparison with the wavelength, $\bar{\lambda} = h/\bar{p}_z$.

If the interaction, $V(x,y,z)$ is neglected, a solution for the whole problem will be

$$\Psi\left(\mathbf{x}, y', z, t\right) = \Phi_0(z,t)\psi_0(\mathbf{x},y,t), \tag{18}$$

where $\psi_0(\mathbf{x},y,t)$ is a solution of the equation

$$i\hbar\partial\psi_0(\mathbf{x},y,i)/\partial t = \left(H_p + H_y\right)\psi_0(\mathbf{x},y,t). \tag{19}$$

When this interaction is taken into account, the solution will, in general, take the form

where the sum is taken ovei the respective eigenfunctions, $\Phi_n(z,t)$ and $\psi_n(\mathbf{x},y,t)$ of H_z and $(H_p + H_y)$. If such a sum is necessary, there will be correlations between the time-determining variable and the other variables, with the result that there will be no valid approximation in which an equation such as (15) involving only $\mathbf{x}$ and y can be separated out. However, if the mass, M, of the time determining particle is great enough, so that the potential $V(\mathbf{x},y,z)$ does not vary significantly in a wavelength, $\lambda = h/p_2$, then, as is well known, the adiabatic approximation will apply. In this case, one can obtain a simple solution, consisting of a single product, even when interaction is taken into account. To show in more detail how this comes about, we first write the solution in the form

$$\Psi = \Phi_0(z,t)\psi(\mathbf{x},y,z,t).$$

When this function is substituted into Schrödinger's equation (15), the result is

$$\begin{aligned} i\hbar\frac{\partial\psi}{\partial t} = [&H_p + H_y + V(\mathbf{x},y,z) \\ &-\frac{\hbar^2}{M}\frac{\partial \ln\Phi_0}{\partial z}\frac{\partial}{\partial z} - \frac{\hbar^2}{2M}\frac{\partial^2}{\partial z^2}\Bigg]\psi. \end{aligned} \tag{20}$$

If M is large, and if the potential does not vary too rapidly as a function of z, the last term on the right-hand side of (20) can be neglected. [15] Moreover,

$$\frac{\partial \ln\Phi_0}{\partial z} = \frac{i}{\hbar}\left[\bar{p}_z + \hbar\frac{\partial \ln\Phi^\Psi\left(z - {v_z}'\right)}{\partial z}\right].$$

[8] $\Psi(\mathbf{x},y,z,l) = \sum_n \Phi_n(z,l)\psi_n(\mathbf{x},y,l)C_n$,

[14] Our procedure is along lines similar to those developed by H. L. Armstrong, Am. J. Phys. 22, 195 (1957).

Because $\Phi(z - v_z t)$ does not vary significantly in a wavelength, this term too can be neglected in the above equation, and we obtain

$$i\hbar \frac{\partial \psi(\mathbf{x}, y, z, t)}{\partial t} = \left[H_p + H_y + V(\mathbf{x}, y, z) - i\hbar v_z \frac{\partial}{\partial z} \right] \psi(\mathbf{x}, y, z, t).$$

We then make the substitution, $z - v_z t = u$, and

$$\psi'(\mathbf{x}, y, u, t) = \psi(\mathbf{x}, y, z, t) = \psi(\mathbf{x}, y, u + v_z t, t).$$

With the relation

$$\partial \psi' / \partial t = (\phi \psi / \partial t) + (v_z \partial \psi / \partial z),$$

we have

$$i\hbar \partial \psi' / \partial t = [H_p + H_v + V(\mathbf{x}, y, u + v_z t)] \psi'(\mathbf{x}, y, u, t). \tag{21}$$

Note that this equation does not contain derivatives of u, so that u can be given a definite value in it.

The complete wave function is, of course, obtained by multiplying $\psi'(\mathbf{x}, y, u, t)$ by $\Phi_0(z - v_z t) = \Phi_0(u)$. Now, this was assumed to be a narrow packet centering at $u = 0$, such that the spread of u can be neglected. As a result, we can write $u = 0$ in the above equation. The

result is

$$i\hbar \frac{\partial \psi'(\mathbf{x}, y, 0, l)}{\partial l} = [H_p + H_u + V(\mathbf{x}, y, v_2, t)] \psi'(\mathbf{x}, y, 0, t). \tag{22}$$

In this way, we have obtained the Schrödinger equation for x, y, with the appropriate time-dependent potential $V(\mathbf{x}, y, v_z t)$, the relationship between the time parameter t and the time determining variable z being, in this case, $t = z/v_z$. We have therefore completed the demonstration of the equivalence of the two treatments, in which the time-determining variables are placed on different sides of the cut.

29.5.4 4. Example of a Reproducible Measurement of Energy in a Well-defined Time

We saw in Secs. 2 and 3 that there is no reason inherent in the principles of the quantum theory why a reproducible and exact measurement of energy cannot be made in an arbitrarily short period of time. Since Landau and Peierls, [5] Fock and Krylov, [6] and many others have considered examples leading to a contrary conclusion, it is necessary to complete the discussion by giving a specific example of a method of measuring energy precisely in as short a time as we please. This we shall do in the present section. Following the development of our example, it will become clear in what way the previous treatments of this problem were inadequate.

As a preliminary step, we discuss the treatment of the measurement of energy by means of the Schrödinger equation for the apparatus and the observed system together. The Hamiltonian of the combined system is

$$H = H_0(p_x, x) + H_0'(p_y, y) + H_I(p_x, x; p_y, y, t), \tag{23}$$

where $H_0(p_x, x)$ is the Hamiltonian of the observed system, $H_0'(p_y, y)$, that of the apparatus, and $H_I(p_x, x;\ p_y, y, t)$ is the interaction, which is zero except during a certain interval of time

[815] If $V(z, y, z)$ varies too rapidly, then $(\hbar^2/2M)\,\partial^2\psi/\partial z^2$ will not be negligible, even when M is large.

between t_0 and $t_0 + \Delta t$. (Here we are adopting the point of view described in Sec. 3, in which we regard the time determining variables as being on the classical side of the cut, so that they do not appear explicitly in Schrödinger's equation.) It will be adequate for our purposes to assume that both the observed system and the apparatus are free particles, with respective Hamiltonians

$$H_0 = {p_x}^2/2M; \quad {H_0}' = {p_y}^2/2M. \tag{24}$$

To simplify the problem, we consider the ideal case of a measurement of p_x which does not change p_x. This will happen if H_I is not a function of x. (The satisfaction of this condition will evidentily guarantee that reproducible measurements of p_x, and therefore $H_0 = {p_x}^2/2M$ will be possible). The Hamiltonian of the whole system will then be taken as

$$H = \left({p_x}^2/2M\right) + \left({p_y}^2/2M\right) + y p_x g(t), \tag{25}$$

where $g(t)$ is everywhere zero, except between t_0 and $t_0 + \Delta t$, where it is constant. (The interaction Hamiltonian is similar to a vector potential in its effects).

With the Hamiltonian (25), p_x is, of course, a constant of the motion. The equations of motion for the remaining variables are then

$$\begin{aligned} &\dot{x} = (p_x/m) + y g(t), \quad \dot{p} = -p_x g(t), \\ &\dot{y} = p_y/M. \end{aligned} \tag{26}$$

On solving for p_y, we obtain (using p_x = constant)

$$p_y - {p_y}^0 = -p_x g(t) \Delta t. \tag{27}$$

This equation implies a correlation between $p_y - {p_y}^0$ and p_x, such that if $p_y - {p_y}^0$ is observed, we can calculate p_x.

It is important also to consider the behavior of $\dot{x}$. Although p_x is constant, $\dot{x}$ shifts suddenly at $t = t_0$ from p_x/m to $p_x/m + g(l)y$, and remains at this value until $t = t_i$, after which it returns to its initial value. (In a similar way, the velocity and momentum differ in the case of a vector potential.)

The above behavior of the velocity is, as a simple calculation shows, just what is needed to produce the uncertainty in position, which is required by the improved definition of the momentum resulting from the measurement.

It is easily seen that if $g(t)$ is large enough, the measurement described above can be carried out in as short a time as we please. In order that a given accuracy, Δp_x, be possible, the change of deflection of the apparatus, $\Delta\left(p_y - {p_y}^0\right)$ due to the shift Δp_x, must be greater than the uncertainty, $\Delta\left({p_y}^0\right)$ in the initial state of the apparatus. This means that we must have

$$\Delta p_{xg}(t) \Delta t \cong \Delta {p_y}^0$$

and if $g(l)$ is large enough, both Δt and Δp_x can be made arbitrarily small for a given $\Delta {p_y}^0$. This hypothetical example confirms our conclusion once again that accurate energy measurements can be reproduced in an arbitrarily short time. We shall now show how to carry out such a measurement by means of a concrete experiment. To guide us in the choice of this experiment, we note that the essential feature of the interaction described in Eq. (25) is that it implies a force that is independent of the x coordinate of the particle, and which alters the velocity suddenly at $t = t_0$ to bring it back to its original value at $t = t_1$.[16] This force is therefore equivalent in its effect to a pair of equal and opposite pulses in a uniform electric field, the first at t_0 and the second at t_1. In order to approximate such pulses, we shall consider two condensers, the

fields of which cross the observed particle at the times t_0 and t_1. The condensers are assumed to have a length, l, in the

Y direction which is much greater than their thickness, d, in the X direction. Therefore, they will produce a uniform electric field in the X direction, except for edge effects which can be neglected when $l \gg d$. Each condenser will go by the particle at a velocity, V_y in the Y direction, which is assumed to be so great that the electric field acts for a very short time, l/V_y, with the result that the field approximates the one cited in our mathematical example, where the period of action was infinitesimal. If the two condensers follow each other, one at $t = t_0$, the other at $t = t_1$, then we shall approach the case treated in Eq. (25).

As in the case of the collision treated in Secs. 1 and 3, the time of measurement is defined as the time at which the condenser passes the observed particle. (This means that we are now shifting to the point of view in which the time-determining variables are on the quantummechanical side of the cut, but as we saw in Sec. 3, both both points of view are equivalent and can be used interchangeably). As in the case of collision, the uncertainty Δt in this time will be given by $\Delta y/V_u$, provided that the observed particle is initially localized in the Y direction, with a velocity v_y much smaller than V_y. This will imply an uncertainty in the energy of the condenser, $\Delta E_c = V_y \Delta P_y > \hbar/\Delta t$.

In the interaction between particle and condenser, the transfer of X component of the momentum (neglecting edge effects) is

$$\Delta p_x = {p_x}^0 = F'\tau = e\mathcal{E}_\tau = e\mathcal{E}l/V_u \tag{28}$$

where τ is the time taken by the condenser to pass the particle. (Notc that r and Δt are different quantities). This transfer is independent of initial conditions, and is calculable to arbitrary accuracy. (Since V_y is as large as you please, the V component of the velocity of the particle can be neglected in the above calculation.) The above transfer of momentum implies a transfer of energy to the particle,

$$\epsilon - \epsilon_0 = \frac{\left({p_x}^0 + \Delta p_x\right)^2}{2m} - \frac{{p_x}^2}{2m} = \frac{{p_x}^0}{m}\Delta p_x + \frac{\left(\Delta p_x\right)^2}{2m}. \tag{29}$$

By conservation, this transfer must be equal to the energy loss $E_0 - E_1$ of the condenser. Since the initial momentum P_x of the condenser in the X direction is zero, and since the mass M of the condenser is large, the term $\left(\Delta p_x\right)^2/2M$ which represents the energy of the condenser due to momentum transfer in the X direction, will be negligible. The energy change must therefore be the result of alteration in the V component of the condenser momentum, so that it will be equal to $E_0 - E_1 \cong V_y \Delta P_y$.

Equation (29) can now be used to permit ${p_x}^0$ to be measured if $E_0 - E = \boldsymbol{\epsilon} - \boldsymbol{\epsilon}_0$ is known. For since $\boldsymbol{\epsilon} - \boldsymbol{\epsilon}_0$ depends on ${p_x}^0$ and since Δp_x can be obtained from Eq. (28), ${p_x}^0$ can be calculated in terms of $E_0 - E_1$.

There is, however, a limitation on how accurately $E_0 - E_1$ can be measured because we require that the

Y coordinate of the condenser shall serve as a clock to an accuracy, δt, with the result that the uncertainty relation, $\delta E S\hbar/\delta t$ will hold for the energy of the con denser. By conservation, the same uncertainty relation must hoid for the energy $\epsilon - \epsilon_0$ transferred to the particie. By evaluating $\delta\left(\epsilon - \epsilon_0\right)$ from Eq. (29), we obtain

$$\delta\left(\boldsymbol{\epsilon}_0 - \boldsymbol{\epsilon}\right)\delta t = \delta {p_x}^\mu \frac{\Delta p_x}{m}\delta t = \delta {p_x}^\mu \Delta v_x \delta l = \delta {p_x}'\left({v_x}' - v_x\right)\delta t > \bar{h}.$$

[816] In the hypothetical example of Eq. (25), this force resulted from the time-dependent interaction, which was equivalent to a corresponding vector potential, which would produce a field, $\mathcal{E} = -(1/c)\partial\mathbf{\Lambda}/\partial t$, that is nonzero only when $\mathbf{\Lambda}(i)$ changes; i.e., at the beginning and the end of the interval.

This is exactly the same relation as was obtained in the collision example given in Sec. 1. In other words, the measurement on the first condenser alone, must satisfy the condition that if it is carried out in a time defined as $\hat{o}i$, there will be an uncertain energy transfer, $\delta E > h/\delta t$. It is at this point, however, that the second condenser plays an essential role. For immediately after the interaction with the first condenser is over, it will bring about a transfer of X component of the momentum, which is cqual and opposite to that transferred to the first condenser. As a result, the velocity of the observed particle will return to its initial value, just as happened in the mathematical example discussed in the beginning of this section. Thus, the momentum and the energy have been measured without their being changed. There is, therefore, no limitation on the accuracy with which the energy of the particle can be measured, regardless of the value of δt, which can be made as small as we please by making V_y very large.

A similar two-stage interaction can be carried out in the collision example described in Sec. 1. To do this, we recall that the uncertainty in energy transfer, $\delta(\epsilon' - \epsilon) = |v - v'|\,\delta p$ is large because $|v - v'|$ is large. Nevertheless $v - v'$ can be determined with arbitrary accuracy from the results of the measurement. After this is done, one can then send in a second test particle, with initial momentum calculated to be such as to change v' back to v. After the two collisions, there will be, as in the case of the condensers, no uncertainty in energy of the observed particle. In the collision experiment, the change of velocity depends on the value of the momentum of the observed particle, so that the initial conditions in the second collision must be arranged, in accordance with this value, which is learned from the first collision. On the other hand, in the condenser experiment, $v'_x - v_x$ is independent of initial conditions so that the second condenser can be prearranged to cancel out this shift of velocity without any information from the results of the first interaction.

At first sight, one might raise the question as to whether our conclusions could be invalidated by effects of radiation, or by currents which might be induced in the condenser. Since we are discussing only the probiem of nonrelativistic quantum mechanics, we can assume tion and relativistic effects, in general, can be made negligible, no matter how sudden the shift of potential is. As for currents induced in the condenser, these can

be avoided by charging an insulator instead of a metal plate. The field will still be uniform, but the charges will not be mobile, so that no currents will be induced in the condenser.

The error in the ireatments of Landau and Peieris, Fock, and Krylov, and others, as discussed in Sec. 1, is now evident. For in all of these treatments, the example used was that of a single collision of a pair of particles. For this case, our own treatment also gave the result that energy transfer in a short time must be uncertain. But as shown in our general canonical treatment of the problem [see Eqs. (25)-(28)], it is clear that this is not the correct way to measure momentum and energy without changing them. To accomplish this purpose we need an interaction of the kind described in the ahove equations, which changes the velocity only while interaction is taking place, but which brings it back tu the initial value after interaction is over. And, as we have seen, it is possible to realize such a measurement in a concrete example.

29.5.5 5. Summary and Conclusions

There has been an erroneous interpretation of uncertainty relations of energy and time. It is commonly realized, of -course, that the "inner" times of the observed system (defined as, for example, by Mandelstamm and Tamm [4]) do obey an uncertainty relation $\Delta E, \Delta t \geqslant h$, where ΔE is the uncertainty of the energy of the system, and Δi is, in effect, a lifetime of states in that system. It goes without saying that whenever the energy of any system is measured, these "inner" times must become uncertain in accordance with the above relation, and that this uncertainty will follow in any treatment of the measurement process. In addition, however, there has been a widespread impression that there is a further uncertainty relation

between the duration of measurement and the energy transfer to the observed system. Since this cannot be deduced directly from the operators of the observed system and their statistical fluctuation, it was regarded as an additional principle that had to be postulated independently and justificd by suitable illustrative examples. As was shown by us, however, this procedure is not consistent with the general principles of the quantum theory, and its justification was based on examples that are not general enough. Our conclusion is then that there are no limitation on measurability which are not obtainable from the mathematical formalism by considering the appropriate special case we see that energy can be measured reproducibly in an arbitrarily short time.

29.6 VI.5 The Fundamental Noise Limit of Linear Amplifiers by Heffner

29.6.1 Summary

If the uncertainty principle of quantum mechanics is applied to the process of signal measurement, two theorems relating to amplifier noise performance can be deduceu. Finst, it can be shown that it is impossible to construct a linear noiseless amplifier. Second, if the amplifier is characterized as having additive white Gaussian noise, it can be shown that the minimum possible noise temperature of any linear amplifier is

$$T_n = \left[\ln \frac{\hat{2} - 1/G}{1 - 1/G}\right]^{-1} \frac{i\nu}{k}.$$

In the limit of high gain G this expression reduces to that previously derived for the ideal maser and parametric amplifier. It is shown that the minimum noise amplifier does not degrade the signal but rather allows the use of an inaccurate detector to make measurements on an incoming signal to the greatest accuracy concistent with the uncertainty principle.

29.6.2 Introduction

SNCE The advent of the maser, there have been a number of treatments of the noise figure or noise temperature of this and other potentially low noise devices such as the parametric amplifier. [1–4] Most of these have treated each specific device as a quantum system and have determined a limiting noise temperature arising because of amplified spontaneous emission. Although the details of the calculations differ, investigations of the minimum noise temperature due to this effect yield values of the order of $h\nu/k$ for both the maser and the parametric amplifier.

The maser and the parametric amplifiers are phase preserving amplifiers, or, in the terminology employed here, linear amplifiers. They have been characterized

- Received January 8, 1962; revised manuscript received, April 30, 1962.
  † Stanford Electronics Laboratories, Stanford University, Calif. amplification of quanta with application to maser amplifiers," *J.* Phys. Soc. Japan, vol. 12, pp. 686-700; June, 1957.
  [2] J. Weber, "Maser noise considerations," Phys. Rev., vol. 108, pp. 537-541; November, 1957.
  [3] M. W. Muller, "Noise in a molecular amplifier," Phys. Rev., vol. 1 W, pp. 8-12; April, 1957.
  tions and noise in par Yariv, and A. E. Siegman, "Quantum fluctua-1646-1654: December 1961 processes," Phys. Rev., vol. 124, pp. 654: December, 1961.

broadly as voltage amplifiers. There is another type of amplifier which does not preserve the signal phase which can be classed as a quantum counter. Weber [2,5] has proposed two forms of such amplifiers and has pointed out that they have no spontaneous emission noise. Thus these phase-insensitive counters have a zero-limiting noise temperature. This result opens the question of whether there are possible forms of linear amplifiers-linear in the sense of phase preservingwhich also have a limiting noise temperature approaching zero.

In order to settle this question one needs to look for a general physical principle which will apply to ail amplifiers regardless of the details of the specific amplification process. An appropriate one is the uncertainty principle of quantum mechanics which forms one of the basic postulates of quantum theory. Although it has resulted in important limitations on the accuracy of measurements possible in atomic systems, its corresponding limitations on the accuracy of signal measurements have until recently gone unnoticed. At the 1959 Quantum Electronics Conference, Serber and Townes [6] investigated the role of the uncertainty principle in maser noise and Friedburg [7] considered its implication on the noise figure of a general amplifier. Each of these papers is open to some criticism. First, the uncertainty principle as generally interpreted is a statement about the results obtained in a physical measurement. As such it can be applied to a signal detector but not to an amplifier. An amplifier is not a measuring instrument which produces a set of data. Amplification is rather a process, a transformation of the signal. The uncertainty principle can be applied to the measurement of the results of that processing but not directly to the processing itself. A second objection to both papers concerns their lack of rigor in problems of statistical averaging, particularly in regard to the phase of a signal. Finally, in the case of Friedburg, the wrong constant was used in the statement

[5] J. Wcber, "Masers," Rev. Mod. Phys., vol. 31, pp. 681-710; July, 1959. See also N. Bloembergen, "Solid-state infrared quantum ounter," Phys. Rev. Lett., vol. 2, pp. 84-85; February, 1959.

[6] R. Serber and C. H. Townes, "Amplification and ComplemenUniversity Press, New York, N. Y., pp. 233-255; 1960.

7 H . Friedburg "General amplifier noise limit" "Quantum

Electronics" C.H. Townes, Ed.; Columbia University Press, New York, N. Y., pp. 228-232; 1960.

of the uncertainty principle. As implied before, Friedburg's conclusions strictly speaking apply only to a detector, not to an amplifier, and as such do not indicate what class of amplifier falls under the uncertainty limitation, nor how this limitation is affected by the gain.

This purpose of this paper is to develop in a simple but rigorous fashion the limitations on the noise performance of linear amplifiers which are implied by the uncertainty principle. First it will be shown that there is no such thing as a noiseless linear amplifier. Next, by characterizing the amplifier as adding white noise, the minimum possible noise temperature is derived. The resulting expression when the gain is large is exactly that derived for the limiting noise performance of the maser and the parametric amplifier.

29.6.3 The Uncertainty Principle

The uncertainty principle, first formulated by Heisenberg in 1927, claims that complete accuracy is impossible to obtain in the simultaneous measurements of certain physical quantities. In its most familiar form, it asserts the fundamental inaccuracy which must result in the simultaneous measurement of a particle's momentum p and position x. If we define the uncertainty in measurement to be the rms deviation from the mean in the distribution obtained from an

ensemble of measurements, then the uncertainty in the measurement of momentum Δp and the uncertainty in the measurement of position Δx are related by

$$\Delta p \Delta x \geq h/4\pi. \tag{1}$$

This relation can be interpreted in the following way. The process of measuring cannot be divorced from the physical process being measured. Not only does the act of observing affect the system being observed, but it does this in a way which cannot be precisely predicted. It is this quality of unpredictability which formed the new content of the uncertainty principle.

In its most general form, the uncertainty principle applies to measurements of any two canonically conjugate quantities [8] such as, for example, the energy of

8 In mathematical form, the uncertainty principle states that if
a system and the precise time at which the system possesses this energy,

$$\Delta E \Delta t \geq h/4\pi \tag{2}$$

Still another form of the principle applies to the measurement of the number of quanta in an oscillation and its phase

$$\Delta\pi\Delta\dot{\psi} \geq \frac{1}{2} \tag{3}$$

This latter statement of the principle may be made plausible by substituting the relations $\underline{E} = nhy$ and $\phi = 2\pi\nu t$ into the preceding equation. We shall use this last formulation of the uncertainty principle to derive two basic theorems on amplifier noise performance.

The Unavoidable Noisiness of Linear Amplifiers

The first conclusion which emerges from the uncertainty principle is: It is impossible to construct a noiseless linear amplifier. We can prove this statement by postulating the existence of a noiseless linear amplifier and then showing that it violates the uncertainty principle.

Suppose we have a perfect linear duplifier by which we mean the following. If during any given interval we measure the number of photons n_2 produced at the output, we find that it is related to the number of input photons n_1 by a constant G, the gain of the amplifier.

$$n_2 = Gn_1 \tag{4}$$

Secondly, if we measure the phase ϕ_2 of the output, we find that it is equivalent to the input phase ϕ_1 with perhaps the inclusion of an additive phase shift θ.[9]

$$\phi_2 = \phi_1 + \theta \tag{5}$$

the operators A and B which represent physical observables a and b satisfy the commutation relation

$$AB - BA = iC$$

then the uncertainties in the measurement of a and b satisfy the relation

$$\Delta a \Delta b = \frac{1}{2}\langle C\rangle$$

where the term uncertainty stands for the root mean square deviation from expectation value, e.g.,

$$\Delta a = \left[\left\langle A^2\right\rangle - \langle A\rangle^2\right]^{1/2}$$

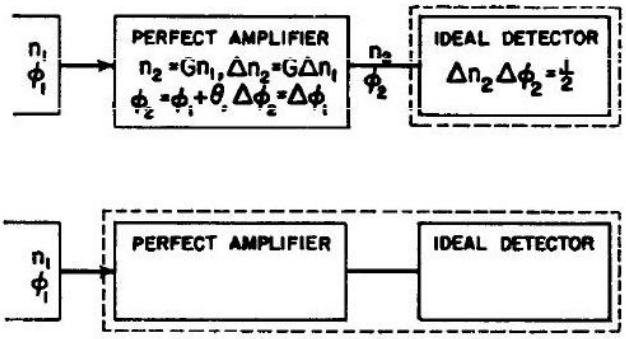
[9] These are operationally valid constructs since we can prepare two signal sources, one of which has an accurately known photon
output and the other of which has an accurately known phase. If

Such an amplifier is linear in the sense that the phase is preserved and the output quanta are linearly related to the imput quanta. It is perfect in that no noise is added. Note that frequency converters which derive their gain solely by the frequency conversion factor do not fall under this definition of a linear amplifier in that the photon gain G is unity.

Let us now attach to the perfect linear amplifier an ideal detector, ideal in the sense that it is capable of detecting the number n_2 of output photons and the output phase ϕ_2 within an uncertainty,

$$\Delta n_2 \Delta \phi_2 = \frac{1}{2} \tag{6}$$

the minimum value allowed by the uncertainty principle. (See Fig. 1.) Thus we imagine that we make a measurement of the output photons and phase which together with the uncertainties introduced by the detector we write symbolically as ($n_2 \pm \Delta n_2$) and ($\phi_2 \pm \Delta \phi_2$).



NEW MEASURING INSTRUMENT INFERS INPUT $\Delta n_1 \Delta \phi_1 = (I/G)\frac{1}{2}$ IMPOSSIBLE

Fig. 1-Thought experiment to show the nonexistence
of a perfect amplifier. of a perfect amplifier.

We now change our point of view and look upon the combination of perfect amplifier and ideal detector as a
each of these is applied in succession to the amplifier input and if in succession two detectors are applied to the amplifier output, one of which measures number of photons without giving phase information and another which measures phase without giving photon number information, we can determine the constants of the amplifier to arbisingle signal source and a single detector if a sufficiently large signal level is used since the accuracy in the determination of phase and the relative accuracy in the simultaneous determination of photon number are each proportional to $1/n^{1/2}$.
single measuring instrument. The measurement of ($n_2 \pm \Delta n_2$) and ($\phi_2 \pm \Delta \phi_2$) when referred to the input of the amplifier implies an input number of photons $(n_1 \pm \Delta n_1) = 1/G\,(n_2 \pm \Delta n_2)$ and an input phase $(\phi_1 \pm \Delta \phi_1) = (\phi_2 \pm \Delta \phi_2) - \theta$. Thus the uncertainty in the measurement of input photons and phase is such that

$$\Delta n_1 \Delta \phi_1 = \frac{1}{G} \cdot \frac{1}{2}. \tag{7}$$

This conclusion is clearly impossible since it violates the uncertainty principle. Therefore our postulated perfect linear amplifier cannot exist. It must add some uncertainty, that is, noise.

29.6.4 Minimum Noise Temperature of a Linear Amplifier

We can pursue this argument even further to prove the foliowing resuit. The minimum noise temperature of a linear amplifier characterized by additive white Gaussian noise is

$$T_n = \left[\ln \frac{2 - 1/G}{1 - 1/G}\right]^{-1} \quad \frac{h\nu}{k}, \tag{8}$$

and the minimum mean square phase fuctuation is

$$\Delta\phi_a{}^2 = \frac{(G-1)h\nu B}{2P}. \tag{9}$$

Here h is Planck's constant, ν is the frequency, k is Boltzmann's constant, B is the bandwidth and P is the signal power.

The proof of this assertion cmploys the same conceptual scheme used previously, a linear amplifier (no longer considered noiseless) followed by an ideal detector. Again a measurement is made by the detector of the output phase ϕ_2 and photon number n_2. This measurement will include as before the same uncertainties introduced by the detection process but will also include the uncertainties which we have seen must be added by the amplifier. Let us label the uncertainties introduced by the detector Δn_d and $\Delta\phi_d$ and those added by the amplifier Δn_a and $\Delta\phi_a$. If we assume the processes which give rise to these two sets of uncertainties are uncorrelated, then the total uncertainties as actually measured, Δn_2 and $\Delta\phi_2$, can be obtained from

$$\begin{aligned} \Delta n_2^2 &= \Delta n_a^2 + \Delta n_d^2 \\ \Delta\phi_2^2 &= \Delta\phi_a^2 + \Delta\phi_d^2. \end{aligned} \tag{10}$$

These equations merely assert that the variances of two uncorrelated random processes add.

Let us again shift our point of view and look upon the combination of amplifier and detector as a single measuring instrument. The measured uncertainties Δn_2, $\Delta\phi_2$ now impiy an uncertainty in the measurement of the input phase and photon number given by

$$\begin{aligned} \Delta n_1^2 &= \frac{1}{G^2}\left(\Delta n_a^2 + \Delta n_d^2\right) \\ \Delta\phi_1^2 &= \Delta\phi_a^2 + \Delta\phi_d^2 \end{aligned} \tag{11}$$

Our proof proceeds by first demanding that the inferred input uncertainties be the least allowed by the uncertainty principle, i.e., $\Delta n_1 \Delta\phi_1 = \frac{1}{2}$. This condition insures that the amplifier uncertainty is the smallest possible. We then characterize this amplifier uncertainty by white Gaussian noise and determine the noise temperature corresponding to this minimum uncertainty.

First, however, we must make sure that the detector is matched to the amplifier, for although the product of the uncertainties $\Delta n_d \Delta\phi_d$ is set, their ratio is not. We can assure the best detection performance by minimizing the product $\Delta n_1 \Delta\phi_1$ given by (11) with respect to the ratio ($\Delta n_d/\Delta\phi_d$) while still demanding that

$$\Delta n_d \Delta\phi_d = \frac{1}{2} \tag{12}$$

This process results in the relation

$$\frac{\Delta w_i}{\Delta\phi_i} = \frac{\Delta w_a}{\Delta\phi_a} \tag{13}$$

which simply states that the minimum over-all uncertainty comes about when the detector-measures number and phase with the same relative uncertainties as those introduced by the amplifier.

We must make sure that the detector is matched to the amplifier in another sense. Let us assume that the amplifier has a bandwidth B. This characteristic implies that the detector should sample the output at intervals of $\tau = \frac{1}{2}B$. If the interval is made longer, the full information transmission capabilities of the amplifier are not being used, while if it is shorter, not only are some of the
data redundant, but also, because of the fluctuations in the output, the uncertainties are greater than necessary. Thus the matching of the detector to the amplifier implies two things, first that the ratios of the uncertainties are made equal and second that the time interval over which the number of output photons and the phase are detected is one half of the reciprocal bandwidth.

Let us now multiply (11) together, introduce the conditions of (i2) and (13), and demand that the uncertainty in the measurements referred to the input be the minimum allowed by the uncertainty principle, that is

$$\Delta n_1 \Delta \phi_1 = \frac{1}{2}. \tag{14}$$

The resulting equation is

$$\frac{G^2 - 1}{4} = \dot{\Delta} n_a^2 \dot{\Delta} \phi_a^2 + \dot{\Delta} n_a \Delta \phi_a. \tag{15}$$

If we put this equation in the form

$$\left(\frac{\Delta \phi_a}{\Delta n_a}\right)^2 \Delta n_a^4 + \left(\frac{\Delta \phi_a}{\Delta n_a}\right) \Delta n_a^2 - \left(\frac{G^2 - 1}{4}\right) = 0 \tag{16}$$

we can solve for Δn_a^2 in terms of the ratio ($\Delta n_a / \Delta \phi_a$) to give

$$\Delta n_a^2 = \frac{G - 1}{2} \left(\frac{\Delta n_a}{\Delta \phi_a}\right). \tag{17}$$

Little more can be done unless we specify the nature of the amplifier uncertainty. Let us characterize the uncertainty as additive white noise. The statistical properties of a signal contaminated by white Gaussian noise have been extensively studied. [10] One result is that the probability density function for the output phase approaches a Gaussian distribution for large SNR's and has a variance given by

$$\Delta {\phi_a}^2 = \frac{\Delta P}{2P} \tag{18}$$

Here ΔP is the noise power and P is the signal power. For large SNR's the variance in the power distribution is given by

[10] S. O. Rice, "Mathematical analysis of random noise," Bell Sys. Jech. J., vol. 23, pp. 282-332, January, 1944; vol. 24, pp. 46-156, noise," Bell Sys. Tech. J., vol. 27, pp. 109-157, January plus random noise," Bell Sys. Tech. J., vol. 27, pp. 109-157, January, 1948.

$$\Delta P^2 = 2P \Delta P \tag{19}$$

so that (18) beromes

$$\Delta \phi_a^2 = \frac{\Delta P^2}{4P^2}. \tag{20}$$

Since the integration time of the amplifier is $\tau = \frac{1}{2}B$, (20) can be put in terms of the variance of the number of photons ${\Delta n_a}^2$ detected during this interval

$$\frac{\Delta n_a}{\Delta \dot{\phi}_a} = \frac{2P_\tau}{\dot{h\nu}}. \tag{21}$$

This result inserted in (17) together with the relation

$$\Delta n_a^2 = \frac{\Delta P^2 \tau^2}{(h\nu)^2} = \frac{2P\Delta P\tau^2}{(h\nu)^2} \tag{22}$$

gives for the minimum noise power introduced in the output of the amplifier

$$\Delta P = (G-1)h\nu B. \tag{23}$$

The effective noise temperature T_n is obtained by dividing by the amplifier gain to refer the noise power to the input and then determining what temperature is required for a black body to radiate the same power. That is, we must find the value T_n for which

$$\frac{h\nu B}{e^{h\nu/kT_n} - 1} = \left(1 - \frac{1}{G}\right) h\nu B. \tag{24}$$

The result is

$$T_n = \left[\ln \frac{2 - 1/G}{1 - 1/G}\right]^{-1} \frac{hv}{k}. \tag{8}$$

According to (19) and (23), the minimum mean square phase fluctuations are

$${\Delta \phi_a}^2 = \frac{(G-1)h\nu B}{2P}. \tag{9}$$

These last two equations give relations for the best possible noise performance of any linear amplifier whose
uncertainty is characterized by white Gaussian noise. It is interesting to note that in the limit of high gain, the minimum noise temperature becomes

$$T_n = \frac{1}{\ln 2}\frac{h\nu}{k} \tag{25}$$

which is precisely the value obtained for the minimum noise temperature of the maser and the parametric amplifier derived from detailed consideration of the amplification mechanisms in the two cases. Thus we can say that both the maser and the parametric amplifier represent ideal amplifiers in so far as their ultimate noise performance is concerned.

We should also remark in passing. (8) and (9) indicate that the parametric up-converter which has power gain by virtue of the change in frequency but has unity photon gain ($G = 1$), possesses a limiting noise temperature and phase uncertainty of zero. This result is in agreement with the detailed calculations of Louisell, Yaiiv and Siegman. [4] This sort of amplifice which does not multiply the number of photons, however, does not improve the capability of detecting a signal. The accuracy of the detection process at the output of the upconverter is no better than if it were performed at the input. The change in photon frequency and hence energy is immaterial since the limiting detector uncertainty is dependent solely on the number of photons arriving, not upon their energy.

29.6.5 The Implications of the Minimum Noise Limit

At conventional communications requencies, the minimum noise temperature given by (8) is entirely negligible. At optical frequencies though, it can amount to several tens of thousands of degrees. Such a number is mislcading, however, for it implies that the insertion of even the best amplifier has seriously degraded our ability to detect a signal. We can show that such is not the case by recasting the results of the previous section in slightly different form. Eqs. (22) and (23) can be combined to give the uncertainty produced by the amplifier in the number of photons as

$$\Delta n_a^2 = (G-1)n_a, \tag{26}$$

and (9) can be rewritten in the form

$$\Delta\phi_a^2 = \frac{(G-1)}{4n_a} \tag{27}$$

to give the uncertainty in phase produced by the amplifier. If we refer these quantities to the input we have

$$\Delta n_{ai}^2 = \frac{1}{G^2}\Delta n_a^2 = (1-1/G)n_1 \tag{28}$$

and

$$\Delta {\phi_a}^2 = \frac{(1-1/G)}{4n_1}. \tag{29}$$

From (20) and (27) we see that if the amplifier gain is high, the output uncertainties introduced by the amplifier are considerably larger than those of even a poor matched detector. In this case, the total uncertainty Δn_1 in the inferred measurement of the input photon number and $\Delta\phi_1$ in the inferred measurement of input phase are closely given by (28) and (29), which relate to the amplifier alone. In the limit of high gain, the product of these uncertainties is

$$\Delta n_1 \Delta\phi_1 \cong \Delta n_{ai}\Delta\phi_a \cong \frac{1}{2} \tag{30}$$

This is, of course, the minimum value allowed by the uncertainty principle. Thus the minimum noise amplifier allows us to use a poor detector, one which introduces uncertainties considerably larger than the minimum necessary, and still measure an incoming signal with an accuracy approaching the best allowed by the uncertainty principle. There still remains a question of what limitation is put on the rate of information transmission by this maximum allowable accuracy of detection. The answer to this question, however, must await the development of a quantum theory of communication.

29.7 VI.6 Quantum Noise in Linear Amplifiers by Haus, Mullen

Abstract

The classical definition of noise figure, based on signal-to-noise ratio, is adapted to the case when quantum noise is predominant. The noise figure is normalized to "uncertainty noise." General quantum mechanical equations for linear amplifiers are set up using the condition of linearity and the requirement that the commutator brackets of the pertinent operators are conserved in the amplification. These equations include as special cases the maser, the parametric amplifier, and the parametric up-converter. Using these equations the noise figure of a general amplifier is derived. The minimum value of this noise figure is equal to 2 . The significance of the result with regard to a simultaneous phase and amplitude measurement is explored.

29.7.1 Introduction

The availability of coherent signals at optical frequencies has stimulated research in their use for communication purposes. Ways of processing optical frequencies are considered that are similar to those of the low end of the coherent frequency spectrum. With the use of classical communication techniques, classical performance criteria will be applied. One purpose of this paper is to extend classical noise performance criteria to linear quantum amplifiers in which the predominant noise is quantum mechanical in nature. These criteria will be applied to a wide class of linear quantum mechanical amplifiers.

The purpose of a sensitive linear amplifier is to increase the power, or photon flux, of an incoming signal with as small a noise contamination as possible so that the signal may be conveniently detected at high power levels. The incoming signal, if used for communication purposes, carries amplitude modulation, phase modulation, frequency modulation, or some other type of modulation. Here we shall discuss noise problems mainly in the context of amplifiers processing sinusoidal carriers with narrow band amplitude and/or phase modulation. In this connection it must be noted that the presence of a modulation of bandwidth B calls for a minimum rate of detection. The received signal must be detected within a succession of observation times each of duration τ, where $\tau = \frac{1}{2}B$, in order to utilize the information contained in the modulation.

Noise in masers, including sponteneous emission noise, has been analyzed in many papers including the classical papers by Shimoda, Takahasi, and Townes, [1] and Serber and Townes. [2] A quantum mechanical treatment of the parametric amplifier and up-converter has

Originally published in Physical Review, 128, 2407-13 (1962).

been presented in a paper by Louisell et al. [3] We shall develop a unified set of equations for all "linear" amplifiers, special cases of which are the maser, the parametric amplifier, and the parametric up-converter. On the basis of these equations and the criteria of noise performance, it will be possible to present a proof on the limiting noise performance achievable by any one of these amplifiers used singly or in combination with other linear amplifiers. The connection of the fundamental noise of these amplifiers with the uncertainty principle will be studied.

29.7.2 I. Noise Figure

In the noise theory of classical amplifiers (i.e., amplifiers operating with a very large number of quanta) the deterioration of the signal-to-noise ratio as the signal passes the amplifier is used as a measure of amplitier noise performance. The signal-to-noise ratio (SNR) is defined in the classical limit as the ratio of signal power to noise power. Mathematically one may describe a phase and amplitude modulated signal in the presence of noise by

$$A(t) = A_0(t)\cos\left[\omega_0 t + \phi_0(t)\right] + \delta A_p \cos\left[\omega_0 t + \phi_0(t)\right] + \delta A_q \sin\left[\omega_0 t + \phi_0(t)\right]. \tag{1.1}$$

The first term in this equation represents the signal in the absence of noise. The remaining two terms are the inphase and quadrature perturbations of the amplitude due to the noise. These are slowly varying with time if the noise is narrowband. We envisage an ensemble of identical signal waveforms with accompanying noise. The signal part may be extracted from the waveform by taking an ensemble average indicated by the brackets $\rangle$

[81] K. Shimoda, H. Takahasi, and C. H. Townes, J. Phys. Soc. Japan 12, 686 (1957).

[2] R. Serber and C. H. Townes, in Quantum Electronics, edited by C. H. Townes (Columbia University Press, New York, 1960), pp. 233-255.

$$\langle A(t)\rangle = A_0(t)\cos\left[\omega_0 t + \phi_0(t)\right]. \tag{1.2}$$

[3] W. H. Louisell, A. Yariv, and A. E. Siegman, Phys. Rev. 124, 1646 (1961).

The noise part is extracted as follows:

$$\begin{aligned}\left\langle A(l)^2\right\rangle - \langle A(t)\rangle^2 \\ = \left\langle \delta {A_p}^2\right\rangle \cos^2\left[\omega_0 t + \phi_0(t)\right] + \left\langle \delta {A_q}^2\right\rangle \sin^2\left[\omega_0 t + \phi_0(l)\right] \\ + \langle \delta A_p \delta A_q\rangle \sin 2\left[\omega_0 t + \phi_0(t)\right].\end{aligned} \tag{1.3}$$

Additive stationary noise is characterized by

$$\left\langle \delta.1_p{}^2\right\rangle = \left\langle \delta {A_q}^2\right\rangle \quad \text{and} \quad \langle \delta.1_p \delta.1_q\rangle = 0. \tag{1.4}$$

The noise as defined here measures the mean square deviation from the signal of the measured ensemble of waveforms all containing the same signal. If the noise is stationary, this mean square deviation becomes

$$\left\langle A(t)^2\right\rangle - \langle A(t)\rangle^2 = \left\langle \delta {A_p}^2\right\rangle. \tag{1.5}$$

A signal-to-noise ratio may be defined, based on a time average, over an observation time T, long compared to the inverse bandwidth of signal and noise. The signal power is

$$S = \frac{1}{T}\int_0^T A_0^2(t)\cos^2\left(\omega_0 t + \phi_0\right) dl = \frac{1}{2}\left[A_0^2(l)\right]_{\text{av}} \tag{1.6}$$

where the square bracket indicates a time average.

The noise is defined correspondingly as

$$\begin{aligned}N = \frac{1}{T}\int_0^T \left\{\left\langle A^2(t)\right\rangle - \langle A(t)\rangle^2\right\} dt \\ = \frac{1}{2}\left\{\left\langle \delta {A_p}^2\right\rangle + \left\langle \delta {A_q}^2\right\rangle\right\}_{\text{av}} = \left\langle \delta {A_p}^2\right\rangle.\end{aligned} \tag{1.7}$$

The last equality holds for stationary noise. The noise figure of an amplifier is defined as the signal-to-noise ratio at the input of the amplifier divided by the signal-to-noise ratio at the output [4]

$$F = \left(S_i/N_i\right) / \left(S_0/N_0\right). \tag{1.8}$$

In defining S_i/N_i one envisages measurements of the signal and noise at the amplifier input and output by a noise-free measurement apparatus. The noise figure is usually defined by choosing a standard input noise corresponding to thermal noise of the input source of 290°K. If the amplifier is linear,

$$S_0 = GS_i, \tag{1.9}$$

and the amplifier noise is additive,

$$\Lambda_0 = GN_i + \Lambda_a^-, \tag{1.10}$$

then, one has for the "excess noise figure," $F - 1$,

$$F - 1 = N_a/GN_i. \tag{1.11}$$

The excess noise figure measures the increase of the mean square deviation of the normalized signal as caused by the amplifier noise.

When adapting the noise figure of linear amplifiers for the quantum case, one faces two problems. First of all, one must establish that linear quantum mechanical

amplifiers, like linear classical amplifiers, introduce additive noise. Secondly, in the limit when quantum effects are of importance, physical measurements, in general, introduce uncertainties, i.e., noise, and it is not clear that the concept of a noise-free measurement as envisaged in the classical noise figure definition can be applied. Thus, for example, simultaneous measurements of amplitude and phase of an electric field cannot be carried out with arbitrarily high precision but must obey the principle of complementarity. It is clear, therefore, that special measures have to be taken if the uncertainty introduced by the measurement is to be negligible compared to the noise in the system.

In quantum theory, a physical quantity is described by an operator. The expectation value of the operator represents the result of a set of measurements on an ensemble of identically prepared systems. In the evaluation of quantum noise we shall consider field amplitude measurements on an ensemble of amplifiers all of which are fed by a transmitter signal that is non-thermally attenuated (such as the attenuation of a radiation field by the inverse square law). At the transmitter the signal has a classical power level and, thus, can be accurately phase and amplitude controlled. If a measurement of the electric field $E(t)$ at the receiver inputs is performed at the time t, the signal is defined by $\langle E(t)\rangle$, and the noise by [5] $\langle E(t)^2\rangle - \langle E(t)\rangle^2$. By performing many such measurements at random time instants delayed with respect to each other by times long compared to the inverse bandwidth of the receivers, one finds the signal power

$$S = \left[\langle E(t)\rangle^2\right]_{\text{av}}, \tag{1.12}$$

and the noise power

$$N = \left[\left\langle E(t)^2\right\rangle - \langle E(t)\rangle^2\right] \text{av}. \tag{1.13}$$

Such measurements do not mutually intefere, and, therefore, are not accompanied by a fundamental uncertainty. These measurements are analogous to the "noise-free" measurements implied in the classical signal-to-noise ratio definition. The signal-to-noise ratio is thus

$$S/N = \left[\langle E(t)\rangle^2\right]_{\text{av}} / \left[\left\langle E(t)^2\right\rangle - \langle E(t)\rangle^2\right]_{\text{av}}. \tag{1.14}$$

With the aid of definition (1.14), Eq. (1.8) may bc used as the definition for the quantum noise figure. In the case of linear quantum amplifiers, as discussed in this paper, Eqs. (1.9), (1.10), and (1.11) are also made valid. It is not expedient to normalize the quantum noise figure to thermal noise. It is more appropriate to normalizc it to the minimum noise within the observation time τ of $h\nu/2$ that is associated with attenuated signals that before attenuation were classically phase and amplitude controlled (see Appendix). Then, if we express the amplifier noise power multiplied by the observation time τ in terms of a photon number n_a at

the amplifier output,

$$N_a = h\nu n_a \tag{1.15}$$

one has

$$F - 1 = 2n_a/G. \tag{1.16}$$

[84] H. T. Friis, Proc. Inst. Radio Engrs. 33, 458 (1945).
[85] R. Senitzky, Phys. Rev. 111, 3 (1958).

Since the basic noise energy to which we compare the amplifier noise corresponds to half a photon within the observation time, it is natural to measure the output noise content, referred to the input by division through G, in terms of the energy of half a photon at the oulput frequency. In this sense, Eq. (1.16) can be applied to the general case for different input and output frequencies if G is interpreted as the photon number gain.

29.7.3 II. The Equations of Linear Amplifiers

Consider a system of weakly interacting particles that, in the absence of radiation, has N available energy levels. If the particles obey Bose-Einstein statistics, the entry of a particle into a particular level (i) and its exit from this level may be described by creation and annihilation operators, ${b_i}^\dagger$ and b_i that obey commutator relations.

$$\left[b_i, b_j^\dagger\right] = \delta_{ij} \tag{2.1}$$

$$[b_i, b_j] = 0 \tag{2.2}$$

The operation of b_i on a wave function of the system with n_i particles in level i produces a wave function with $n_i - 1$ particles in that level, the operation of ${b_i}^\dagger$ produces one with $n_i + 1$ particles in the level i. The number of particles in level i is given by

$$n_i = b_i^\dagger b_i \tag{2.3}$$

If the particles obey Fermi-Dirac statistics, a BoseEinstein description is possible, [2] provided that the number of available states in a particular level is much greater than the number of particles occupying it. If the states within a particular energy level are all equivalent for the physical processes envisaged, wave functions may be constructed that correspond to a discrete number of particles in a particular energy level with no distinction made between different states within that level. [6] Creation operators ${b_i}^\dagger$ and annihilation operators b_i that increase or decrease the number of particles in a particular energy level upon operation on a wave function can be shown to obey the commutation relations (2.1) and (2.2), provided the number of particles in the energy level is much less than the number of states of the level. [7] Linear quantum amplifiers must of necessity operate by means of transitions from and to weakly occupied levels since nonlinear effects occur as soon as the deviation from Bose-Einstein behavior of these levels becomes appreciable.

The electromagnetic field is represented by the creation and annihilation operators ${a_i}^\dagger$ and a_i for photons in the modes i, j, etc., of the electromagnetic system. These obey the usual commutation relations

$$a_i a_j^\dagger - a_j^\dagger a_i = \delta_{ij} \tag{2.4}$$

$$a_i a_j - a_j a_i = 0 \tag{2.5}$$

When the fields are made to interact with matter, coupling results among the various operators of the system. In the interaction representation, differential equations in time are obtained relating the time rate of change of every operator to all the other operators of energy levels and electromagnetic modes partaking in the interaction. These equations are, in general,

[86] For example, if one is interested only in the interaction with an electromagnetic field of the spin of weakly interacting particles, all states of the particles that have the same spin are equivalent.

[7] H. A. Haus, Internal Memorandum, Massachusetts Institute of Technology Research Laboratory of Electronics, 1962 (unpublished).

nonlinear. However, under proper "biasing" or "pumping" conditions linear interactions may result among some of the energy-level and photon operators of the system. Thus, consider a system like the three-level maser in which a pumping excitation establishes a steady state in the occupation of two energy levels. If a small signal is applied with a frequency corresponding to the energy difference between one of the pumped levels and an intermediate level, the small perturbations produced in the steady state of the strongly excited levels may be disregarded, and linear equations are obtained for the operators of the weakly excited level and the photons of the small applied signal. In more complicated devices, more level and photon operators may he particpating in the interaction initiated by the applied small signal. In any case, if the device is to act as a linear amplifier for some photons it is a necessary recluirement that the equations of motion permit a linearization of the equattions for the signal photon operators and the operators directly involved in the small signal interaction. If the amplifier is to be time independent, a further requirement is that the coefficients of the differential equations be time independent. These two requirements strongly restrict the form of the equations. Integration of the differential equations in time leads to linear relations among the operators at an initial time t_0, and final time l_1.

Taking as an example a system within which a photon operator interacts with an energy level operator, one has two possible cases:

$$\begin{aligned} a(t_1) &= M_{aa}a(t_0) + M_{ab}b^\dagger(t_0) \\ b(t_1) &= M_{ba}a(t_0) + M_{bb}b^\dagger(t_0) \end{aligned} \tag{2.6}$$

or

$$\begin{aligned} a(t_1) &= M_{au}a(t_0) + M_{ab}b(t_0) \\ b(t_1) &= M_{bu}a(t_0) + M_{bb}b(t_0) \end{aligned} \tag{2.7}$$

The first system of equations is of the type obtained by Serber and Townes [2] for the ideal maser. In this system, the creation operator $b^\dagger$ of the energy level couples to the annihilation operator a of the photons. In the second system the annihilation operators of the energy level b couples to a. We shall later see the significance of this
latter type of coupling. An analysis of the parametric amplifier leads to equations of the form (2.6) where $b^\dagger$ is replaced by a creation operator representing the photons at the idler frequency. [3]

The general form of the linear equations is immediately apparent for a lincar system of arbitrary degree of complexity. If one comprises all operators representing "output" quantities at $t = t_1$ in a column matrix $\mathbf{v}$, those representing "input" quantities at $t = t_0$ in a column matrix $\mathbf{u}$, one may write the general linear relations in matrix form as

$$\mathbf{v} = \mathbf{M}\mathbf{u}. \tag{2.8}$$

In the example of Eq. (2.6)

$$\mathbf{u} = \begin{bmatrix} a(t_0) \\ b^\dagger(t_0) \end{bmatrix}, \quad \text{and} \quad \mathbf{v} = \begin{bmatrix} a(t_1) \\ b^\dagger(t_1) \end{bmatrix}.$$

The requirements of linearity and time independence have led to an equation of the form of (2.8). There is another important condition that has to be met by Eq. (2.8) which restricts the matrix $\mathbf{M}$: The commutator brackets of the operators must be conserved. Indeed, considering a system with photons and Bose-Einstein particles, the commutator brackets are invariants of

the complete (nonlinear) equations of motion. The linearized equations that describe the small signal interactions, must conserve commutator brackets insofar as they are good approximations to the behavior of the same set of operators in the complete equations. Consider next a system with photons and Fermi-Dirac particles. One notes that the complete equations of motion preserve the commutator brackets of the photon operators and anticommutator brackets of the particle operators. As mentioned before, one may construct effectively Bose-Einstein operators from the input Formi-Dirac operators. Corresponding operators may be constructed for the output. These will also be effectively Bose-Einstein provided the number of particles in the level of interest has remained small compared to the number of states in the level (as needs be if the amplification is to be linear). Therefore, the commutator brackets of the constructed operators are also conserved in the amplification. Let us study the matrix C consisting of the commutator brackets of the operators contained in the input matrix **u**. It is easily seen that this matrix is constructed by

$$\mathbf{C} = \mathbf{u}\mathbf{u}^\dagger - \left(\mathbf{u}_t^\dagger \mathbf{u}_t\right)_t \tag{2.9}$$

Here the subscripts t indicate the transpose. The operators obey initially the commutation relations (2.1), (2.2), (2.4), and (2.5). Photon operators and level operators commute. The commutator relations can be conveniently summarized by defining a matrix **P** of the same order as **u** by

$$\mathbf{P} = \mathrm{diag}(\pm 1, \pm 1, \pm 1, \cdots \pm 1) \tag{2.10}$$

where for the i th diagonal element, the plus sign is chosen when an annihilation operator appears in the i th row of the matrix **u**, and the minus sign if a creation operator appears. Using this definition for **P**, one has from Eq. (2.9)

$$\mathbf{C} = \mathbf{u}\mathbf{n}^\dagger - \left(\mathbf{u}_t^\dagger \mathbf{u}_t\right)_t = \mathbf{P} \tag{2.11}$$

at $t = t_0$. Because

$$\mathbf{C}\,(t_1) = \mathbf{C}\,(t_0) \tag{2.12}$$

one has from Eqs. (2.8) and (2.12)

$$\mathbf{v}\mathbf{v}^\dagger - \left(\mathbf{v}_t^\dagger \mathbf{v}_t\right)_t = \mathbf{P} = \mathbf{M}\mathbf{u}\mathbf{u}^\dagger\mathbf{M}^\dagger - \left[\left(\mathbf{u}^\dagger\mathbf{M}^\dagger\right)_t (\mathbf{M}\mathbf{u})_t\right]_t$$
$$= \mathbf{M}\left(\mathbf{u}\mathbf{u}^\dagger - \mathbf{u}_t^\dagger \mathbf{u}_i\right)\mathbf{M}^\dagger = \mathbf{M}\mathbf{P}\mathbf{M}^\dagger$$

It follows that

$$\mathbf{M}\mathbf{P}\mathbf{M}^\dagger = \mathbf{P} \tag{2.13}$$

One may easily check that in the special cases of an ideal maser and parametric amplifier mentioned previously, the expressions as derived in references 2 and 3 obey the relation (2.13). Here this relation has been derived in general as a consequence of the requirement of conservation of commutator brackets. It is this relation that imposes a fundamental limit on the noise performance of all linear amplifiers. It is of interest to show that in an amplifier with photon gain greater than unity the signal creation (annihilation) operator must couple to at least one annihilation (creation) operator of a molecular state or of a photon of frequency different from the signal frequency. Suppose the output photons pertain to the operator a_j, the input photons to a_h. Let these, in turn, correspond to v_m or ${v_m}^\dagger$ and u_n or ${u_n}^\dagger$. If the signal level is sufficiently

large, one may disregard the uncertainty contained in the commutator relations, i.e., one may set

$$\left\langle i'_m \eta'_{l_m} \right\rangle = n_m \cong \left\langle i'_m {l'_m}^{\dagger} \right\rangle \tag{2.14}$$

where n_m is the number of output photons,

$$\left\langle u_n^{\dagger} u_n \right\rangle = n_n \cong \left\langle u_n u_n^{\dagger} \right\rangle \tag{2.15}$$

with n_n, the number of input photons. All the other input quantities are assumed unexcited

$$\left\langle u_i^{\dagger} u_i \right\rangle = 0, \quad \left\langle u_i u_i^{\dagger} \right\rangle = 1, \quad i \neq n \tag{2.16}$$

We thus have from Eqs. (2.8), (2.14) (2.16),

$$n_m \cong |M_{mn}|^2 n_n \tag{2.17}$$

$|M_{mn}|^2$ is the photon gain of the amplifier. But, from Eq. (2.13)

$$\sum_{\imath} P_{\imath} |M_{mi,}|^2 = P_{mm} \tag{2.18}$$

We recall that $l_n = \pm 1$, depending upon whether u_i stands for an annihilation operator or creation operator. Thus, this equation shows that $|\boldsymbol{M}_{mn}|^2$ is necessarily less than unity, unless at least one of the P_{ii} 's is of opposite sign to P_{mm}. A simple situation exists when u_m interacts with only one other operator u_l,

$$|M_{mm}|^2 + (P_{lu}/P_{mm}) |M_{ml}|^2 = 1 \tag{2.19}$$

The ideal maser, Eq. (2.6), uses the same input and output frequency, the photons of which couple to a single level operator $b^{\dagger} (= u_l)$. The gain $|M_{mm}|^2$ is greater than unity, because P_{ll}/P_{mm} is equal to -1 .

The parametric amplifier using the same input and output frequency couples the signal photon operator $a_1 = u_m$ to the idier photon operator ${a_2}^{\dagger} = u_l$. Again $P_{ll}/P_{mm} = -1$ and the gain $|M_{mm}|^2 > 1$.

The ideal parametric up-converter couples the input signal frequency operator $a_1 = u_m$ to the output frequency operator $a_2 = u_l . P_{ll}/P_{mm} = 1$ and the gain $|M_{ml}|^2 < 1$.

A system within which a photon operator $a = u_m$ couples to a level operator $b = u_l$ exhibits gain less than, or at most equal to, unity since $P_{ll}/P_{mm} = 1$. [Compare Eq. (2.7).]

An interesting special case is the "lossless scatterer," with the P_{ii} 's all of the same sign. The coupling between a transmitting antenna and a receiver may be represented in this way. Here all u 's represent annihilation operators a_i pertaining to the same frequency, but different spatial modes. The relation (2.13) assures conservation of the total photon number, but only a fraction $|M_{jk}|^2$ of the input (transmitter) photons represented by, say $\left\langle {u_k}^{\dagger} u_k \right\rangle$ reach the receiver as output photons $\left\langle v_j^{\dagger} v_j \right\rangle$.

29.7.4 III. Amplifier Noise

It should be recalled that the u 's contain the a 's and b 's, or their Hermitian conjugates. In the study of signal and noise we are interested in averages of expectation values of electric field components, whose operators are given by

$$E_j(t) = k_j i \left(a_j^{\dagger} e^{i\omega_j t} - a_j e^{-i\omega_l t} \right) \tag{3.1}$$

where k_j is some real constant dependent upon the geometry of the system.
Let the photon operator a_j, or $a_j{}^\dagger$, be represented by u_j, so that

$$\begin{aligned}\langle E_j(t)\rangle &= \pm k_j i \left\langle u_j^\dagger e^{\pm i\omega_j t} \; -u_j e^{\mp i\omega_j t}\right\rangle \\ &= \pm 2k_j \left|\langle u_j\rangle\right| \cos\left(\omega_j l + \Phi\right) \end{aligned} \tag{3.2}$$

and

$$\left[\langle E,(t)\rangle^2\right]_{\text{av}} = 2k_j^2 \left[\left|\langle u_j\rangle\right|^2\right]_{\text{av}} = 2k_j^2 \left[\left|\left\langle u_j^\dagger\right\rangle\right|^2\right]_{\text{av}} \tag{3.3}$$

because the average indicated by the square bracket is equivalent to a time average. Similarly,

$$\left[\left\langle E_j(t)^2\right\rangle\right]_{\text{av}} = k_j^2 \left[\left\langle u_j^\dagger u_j + u_j u_j^\dagger\right\rangle\right]_{\text{av}} \tag{3.4}$$

Since the final expressions are symmetric in u and $u^\dagger$ and do not depend on time, both cases $u_j = a_j$ and $u_j = a_j{}^\dagger$ lead to the same final expressions for $[\langle E(t)\rangle^2]_{\text{av}}$ and $[\langle E(t)^2\rangle]_{\text{av}}$. Thus one may use the u 's directly to obtain the required averages.

Suppose the matrix $\mathbf{M}$ of Eq. (2.8) represents an amplifier with its input described by the operator u_n and its output by v_m. Then the output signal-to-noise ratio is given by [compare Eqs. (1.14) and (3.2)-(3.4)]

$$\frac{S_0}{N_0} = \frac{\left[2\left|\langle v_m\rangle\right|^2\right]_{\text{av}}}{\left[\langle v_m{}^\dagger v_m\rangle + \langle v_m v_m{}^\dagger\rangle - 2\left|\langle v_m\rangle\right|^2\right]_{\text{av}}}. \tag{3.5}$$

Now, from Eq. (2.8)

$$v_m = \sum_i M_{mi} u_i \tag{3.6}$$

Because all inputs but the signal input m are fed by incoherent noise, we have for $i, j \neq m, n$

$$\langle u_i\rangle = \left\langle u_i{}^\dagger\right\rangle = 0 \tag{3.7}$$

$$\begin{aligned}\left\langle u_i{}^\dagger u_j\right\rangle &= 0, \text{ if } u_i \text{ stands for an annihilation operator} \\ &= \delta_{ij}, \text{ if } u_i \text{ stands for a creation operator,}\end{aligned} \tag{3.8}$$

$$\begin{aligned}\left\langle u_i u_i{}^\dagger\right\rangle &= 0, \text{ if } u_i \text{ stands for a creation operator,} \\ &= \delta_{ij}, \text{ if } u_i \text{ stands for an annihilation operator.}\end{aligned}$$

Thus

$$\langle \imath_m\rangle = \tilde{M}_{mn} \langle u_n\rangle \tag{3.9}$$

and

$$\begin{aligned}&\left\langle \imath_m{}^\dagger v_m\right\rangle + \left\langle \imath_m \imath_m{}^\dagger\right\rangle - 2\left|\langle v_m\rangle\right|^2 \\ &\quad = \sum_{i\neq n} |M_m|^2 + |M_{mn}|^2 \left\{\left\langle u_n{}^\dagger u_n + u_n u_n{}^\dagger\right\rangle - 2\left|\langle u_n\rangle\right|^2\right\}.\end{aligned} \tag{3.10}$$

But the input noise is taken as the noise accompanying a signal after a large radiative attenuation. This noise expressed in terms of a photon number is equal to the uncertainty noise of $\frac{1}{2}$ photon as shown in the Appendix. The input signal-to-noise ratio to which the noise figure will be normalized has the same form as Eq. (3.5) except that u_n replaces v_m and is equal to

$$S_i/N_i = 2\,[n_{i\pi}]_{\rm iv} \tag{3.11}$$

where $[n_n]_{\rm av}$ is the average number of input photons. Introducing Eqs. (3.9)-(3.11) into Eq. (3.5) and using the noise figure definition (1.8), we have

$$F = \left(\sum_i |M_{mi}|^2\right) / |M_{mn}|^2 \tag{3.12}$$

The input signal has dropped out as is characteristic of a linear amplifier. The noise figure F of (3.12) can be made unity. It is found, however, that the gain $|M_{mn}|^2$ of the "amplifier" is then also necessarily equal to unity. If one wants gain, F must be optimized for fixed gain. Another way of accomplishing this is to use the definition of "noise measure" M,

$$M = (F-1)/(1-1/G) \tag{3.13}$$

Here G is the photon number gain, in the present case $|M_{mn}|^2$. The noise measure M has a nontrivial minimum as we now proceed to show. We obtain

$$M = \left(\sum_{i\neq n} |M_{mi}|^2\right) / \left(|M_{mn}|^2 - 1\right). \tag{3.14}$$

According to Eq. (2.13)

$$\sum_i P_{ii}\,|M_{mi}|^2 = P_{mm}$$

Thus

$$|M_{mn}|^2 - 1 = -\sum_{i\neq n} (P_{ii}/P_{nn})\,|M_{mi}|^2 + (P_{mm}/P_{mn}) - 1 \tag{3.15}$$

Since we are, in general, interested in photon gain, $|M_{mn}|^2 > 1$, it follows that the right-hand side of (3.15) must be positive. In such a case, since $P_{ii}/P_{nn} = \pm 1$, it follows immediately that

$$\sum_{i\neq n} |M_{mi}|^2 \geq -\sum_{i\neq n} (P_{ii}/P_{nn})\,|M_{mi}|^2 + (P_{mm}/P_{nn}) - 1 \tag{3.16}$$

Thus, from (3.14)-(3.16) we find

$$M > 1. \tag{3.17}$$

At high gain $M = F - 1$. It follows that in that case

[88] H. A. Haus and R. B. Adler, Circuit Theory of Linear Noisy Networks (Technology Press, Cambridge, Massachusetts, 1959).

$$F \geq 2. \tag{3.18}$$

The quantum noise introduced in an amplifier leads to a noise-to-signal ratio at its output double of that at its input, if the input signal-to-noise ratio is assumed to be that of uncertainty noise. Considering specific devices, we note that the ideal maser characterized by Eq. (2.6) has a noise measure of unity, because the equality sign in Eq. (3.18) applies, as one can easily see. The same is true for the parametric amplifier. In general, one can see that coupling of the signal photon annihilation operator to other annihilation operators tends to increase the noise figure by virtue of the fact that negative terms appear in the sum on the right-hand side of Eq. (3.16).

We have introduced the concept of noise measure because it possessed a nontrivial minimum, whereas the noise figure could be made equal to unity at a complete sarrifice of gain. There are other advantages in the use of "noise measure" that have been successfully employed in the analysis of noise in classical linear amplifiers. [8] Using the concept of noise measure one may state in simple terms the limit on the optimum noise performance of a passive interconnection of linear two-port amplifiers (amplifiers with one input terminal pair and one output terminal pair). In the classical circuit-theoretical application for which this theorem was originally derived it states [8] that any passive interconnection of two-port amplifiers resulting in an overall two-port amplifier (amplifier with one input terminal pair and one output terminal pair) leads to an optimum (minimum) noisc measure that cannot be lower than that of the best amplifier, namely, the amplifier with the lowest value of optimum noise measure. This proof can now be easily extended to the case of an interconnection of linear quantum amplifiers. In the quantum case, two-port amplifiers are those that are described by one input signal photon operator and one output signal photon operator as discussed in this
section. A passive interconnection is one with a net positive (or zero) internal loss of photons. Systems with linear frequency transformations are not ruled out. Thus the proof in the present section, extended along the lines of reference 8 , in effect shows that the optimum noise measure of a linear quantum mechanical system with one input and one output cannot be better than unity ($F = 2$ at high gain).

29.7.5 IV. Simultaneous Phase and Amplitude Measurements

The technical purpose of amplifiers is to raise signal levels so that signal processing may be effected at conveniently high power levels. In the process, amplifiers must introduce as little noise as possible. Since we have found that all linear quantum amplifiers introduce noise, one may ask the question whether, in those cases in which ultimate sensitivity is desired, one should not dispense with linear amplification. We shall discuss this question as one of principle, although it is clear that technical requirements may call for linear amplification for rcasons other than those considered here.

We have defined the quantum noise figure on the basis of a noise-free measurement. In this context it is immediately apparent that the use of an amplifier is not desired in those cases in which a "noise-free" measurement can be administered to the incoming signal, namely, an instantaneous amplitude neasurement alone.

If one envisages simultaneous amplitude and phase measurement the situation is not that simple and deserves further study. [2,9] Suppose we intend to measure with an ideal measuring apparatus the phase ϕ_0 and amplitude A_0 of an incoming wave. The measurement introduces an rms uncertainty in phase $\Delta\phi$ and in photon number Δn such that at best

$$\Delta n \Delta\phi = \frac{1}{2}. \tag{4.1}$$

- But if ${A_0}^2$ is measured in units of power, Δn is related to the inphase uncertainty of amplitude ΔA_p by (cf. Eq. (1.1)]

$$\tau A_0 \left(\left\langle \delta {A_p}^2 \right\rangle\right)^{1/2} = \tau A_0 \Delta A_p = h\nu \Delta n, \tag{4.2}$$

where ΔA_p is defined as $\left(\langle \delta {A_p}^2 \rangle\right)^{1/2}$. Further

$$\Delta\phi = \Delta A_q / A_0 \tag{4.3}$$

We thus have

$$\tau \Delta A_p \Delta A_q = \frac{1}{2} h v \tag{4.4}$$

for an ideal measurement apparatus. If the measurement apparatus is preceded by an ideal linear amplifier of high gain then the measurement does not have to introduce an uncertainty beyond that introduced by the amplifier noise. The minimum amplifier noise at high gain rcferred to the input is equal to that caused by quantum attenuation and, when measured in terms of energy, is according to Eq. (3.18) equal to half a

photon within an observation time. Further, the noise ratio at the receiver, as in Eq. (3.5), is stativuary. It follows from (i.i.)

$$\left\langle \delta {A_p}^2 \right\rangle = \left\langle \delta {A_q}^2 \right\rangle . \tag{A1}$$

Using Eq. (1.7),

$$\tau \left\langle \hat{O} A_p \hat{p} \right\rangle = \tau \left(\hat{\Delta} A_p \right)^{\hat{2}} = \frac{1}{\hat{2}} h\nu.$$

L'sing (4.5) and (4.6) we find that the uncertainty introduced into the final measurement by the amplifier noise is just equal to that introduced by an ideal detector not preceded by an amplifier, Eq. (4.4). It is characteristic of linear amplifiers that the final measurement results in equal inphase and quadrature uncertainties whereas a measurement performed without the use of a preamplifier may choose the relative magnitudes of each, subject only to Eq. (4.1).

29.7.6 APPENDIX. Radiative Attenuation Noise

Using Eq. (2.8) to represent radiative attenuation, we interpret u_l as the annihilation operator of the input photons at the transmitter, v_k as the annihilation operator of the output photons at the receiver. All the other operators in $\mathbf{u}$ represent spatial modes not used for the transmission process and are unexcited, $\langle u_i \rangle = 0, \left\langle {u_i}^\dagger u_i \right\rangle = 0, \left\langle u_i {u_i}^\dagger \right\rangle = 1$ for $i \neq l$. We have for the signal-to noise

$$\left(\frac{S}{N}\right)_{\text{rec}} = \frac{2\left[\left|\langle v_k \rangle\right|^2\right]_{\text{av}}}{\left[\left\langle {v_k}^\dagger v_k + v_k {v_k}^\dagger \right\rangle - 2\left|\langle v_k \rangle\right|^2\right]_{\text{av}}}. \tag{4.5}$$

Introducing Eq. (2.8), where according to Eq. (2.13), with P = 1,

$$\mathbf{M}\mathbf{M}^+ = 1 \tag{4.6}$$

$\left(\frac{S}{T}\right)_{\text{rec}}$

$$2\left|M_{kl}\right|^2 \left[1\left\langle u_l \right\rangle\right|^2\Big]_{\text{av}}$$

[89] H. Heffner, Proc. Inst. Radio Engrs. 50, 1604 (1962).

$$\left(|M_{kl}|^2 \left[u_l^\dagger u_l + u_l u_l^\dagger - 2 \left| \left\langle u_l \right|_l^2 \right]_{\text{av}} + \sum_{i \neq k} \left| M_{ki} \right|^2 \right) \right)$$

The first term in the denominator represents the attenuated noise of the transmitted signal. The additive noise introduced in the transmission process is represented by $\sum_{i \neq k} |M_{kl}|^2$ and is stationary. If the attenuation is very large, $|M_{kl}|^2 \ll 1$, and if the noise accompanying the signal at the input is not inordinately larger than that imposed by the uncertainty relation, then this term is negligible compared to the second one. Then the noise at the receiver is entirely determined by the zero-point fluctuations of the modes other than the one used for transmission regardless of the input noise. Further, using Eq. (A2)

$$\text{Finally,} \quad \begin{array}{l} \displaystyle\sum_{i \neq l} |M_{ki}|^2 \cong \sum |M_{ki}|^2 = 1. \\ |M_{ki}|^2 \left[| \left\{ \hat{w}_{ij} | |^2 \right]_{\text{av}} \cong \left[\hat{n}^n \right]_{\text{av}} , \end{array} \tag{A4}$$

the average number of received photons as long as this number is much larger than unity. We find
$(S/N)_{\text{rco}} \cong 2[n]_{\text{av}}$.

29.8 VI.7 Optical Channels: Practical Limits with Photon Counting

Abstract

In optical communication, ideal amplification of the received signal leads to a limiting signaling rate of 1 nat per photon. This is much inferior to the optimum limit of kT joules/nat, which we can theoretically approach by counting photons. Practically, the rates we can attain by photon counting will be limited by how elaborate codes we can instrument rather than by themal photons.

Theory

Consider a free-space path such as we might have between snace vehicles. For a wavelength λ, a distance I and transmitting antennas of effective areas A_T and A_R the ratio of received power $\hat{P}_R$ to transmitted power $\bar{P}_T$ is [1]

$$P_R/P_T = A_T A_R/\lambda^2 L^2. \tag{1}$$

This suggests the use of a short wavelength.
Going to optical wavelengths requires very smooth antenna surfaces and very precise pointing. Furthcr, at optical ficquencies we encounter quantum effects. Here we disregard antenna and pointing problems and consider how quantum effects will limit a communication system.

In receiving a signal mixed with Johnson noise, we have the option of amplifying the signal with an ideal amplifier of power gain G and bandwidth B. The Gaussian noise power P_n in the output of the amplifier will be e[2,3,6]

$$P_n - \frac{hf}{e^{hf/hT} - 1} B + (G-1) hfB. \tag{2}$$

When $hf \ll kT$, the noise power density at the input of the amplifier is nearly kT. According to Shannon [4,5] when noise of this power density is added to a signal, the limiting information rate R in nats per joule of transmitted power, which is attained as B approaches infinity, is

$$R = 1/kT \text{ nats / joule} \tag{3}$$

Paper approved by the Editor for Communication Theory of the IEEE Communications Society for publication without oral presentation. Manuscript received April 7, 1978; revised June 14, 1978.
The author is with the Department of Electrical Engineering. California Institute of Technology, Pasadena, CA 91125.

Originally published in IEEE Transactions on Communications, COM-26, 1819-21 (1978).

When $hf \gg kT$ the second term on the right of (2) dominates. We see that this second term is not amplified noise because hf B is multiplied by ($G - 1$), not G. However, when the gain G is very large, the second term is very nearly equal to a Gaussian noise density hf multiplied by the gain G. Thus, following Shannon the limiting information rate in nats per joule of transmitted power will be

$$R = 1/hf \text{ nats/joule.} \tag{4}$$

The energy per photon is hf. Thus, the limiting rate given by (4) is 1 nat per photon. This limit holds only if we amplify

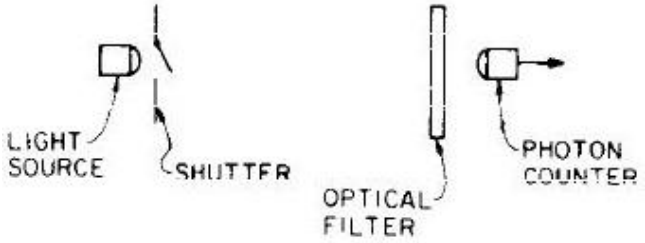


Figure 1. A Photon Channel. A light source transmits photons during intervals when the shutter is open. Received signal and thermal photons pass through an optical filter intended to eliminate out-ofband thermal photons. Each photon that passes the optical filter is counted by a photon counter. In a real system, the light source and shutter could be replaced by a pulsed laser.

the received signal with an ideal amplifier. It dpes not hold for simple photon counting or for various other forms of transmission and reception. [6–9]

Indeed, if no noise is added to the signal, the number of nats we can transmit per photon is unbounded. [6–9] We can see this by a very simple argument.

Consider the signaling system shown in Figure 1. The transmitter consists of a light source and a shutter.* The receiver consists of an optical filter and a photon counter, which we will assume to emit a pulse when one or more photons strike it The purpose of the ortical filter is to exclude thermal photons Initillyose of he optical that are no thermal photons a

In signaling, we intervals, each of "pulse" in one timuration t. Each of these code of signaling is quantized pulse poterval only, so the

In signaling, we open the shutter during only one time interval out of the N in the code word. If we impose no bandwidth limitation in the transmission path, so that classically the path has a constant loss and delay, we can never receive a

photon during any time interval except the one corresponding to the time interval during which the shutter was open**.

8

- In a "practical" system we could send a pulse by pulsing a semiconductor laser rather than by opening a shutter.

Let us assume that the average number of photons received in the time interval corresponding to the opening of the shutter is M. If M is fairly large, we will almost always receive at least one photon, and thus we will almost always receive a proper code word. The information per code word will then be
$\ln N$ nats.
The average number of photons per code word is
M photons.
Hence, the number of nats per photon is
$(\ln N)/M$ nats/photon.

By making N large, we can make the information rate in nats/photon as large as we wish. But growth is only as the logarithm of N, and is impractical to make $\ln N$ very large.

What about the effects of thermal photons in limiting the rate of signaing? Oddiy enough, the theoretical iimit for very small signal strength and unlimited bandwidth is the classical limit given by (3), that is, kT joules/nat. [6,7] I have included in Appendix A a simple demonstration that for a coherent signal source, kT joules/nat can be approached when $hf \gg kT$.

Let us now ask, how many nats per photon do we need in order to attain the limiting kT joules/nat?

A photon has an energy hf. If we require kT joules/nat, the number Q of nats per photon must be

$$Q = hf/kT = 4.80 \times 10^{-11}(f/T) \text{ nats/photon} . \tag{6}$$

How big will Q be for optical frequencies and low temperatures? Let us assume a wavelength of $5,000$Å, corresponding to a frequency of 6×10^{14} Hz, and a temperature of 6 K . For these values,

$$Q = 4,800 \text{ nats/photon.}$$

** One can quibble here or later that P_R/P_T in (1) changes with frequency or that propagation near the source may be slightly dispersive, or that the actual energy of the emitted photon cannot be known. But, for a signaling rate far less than the frequency of the light used, transmission is practically the same for all frequency components of small. small.

If we tried to attain this by means of quantized pulse position modulation, length N of our code words would have to be at least

$$N = e^{4,800}$$

This, of course, is ridiculous.
The practical conclusion is that in optical signaling at low temperatures we encounter insuperable problems of encoding long before we approach the theoretical limit of kT joules/nat.

This seems plausible from another point of view. At what rate do we receive thermal photons? P_n of (2) gives the thermai photon power in one mode of propagation if we sei $\widehat{G} - \mathbf{1}$. The rate p at which we receive thermal photons in a coherent (one-mode) system is thus

$$p = \left(e^{hf/kT} - 1\right)^{-1} B \text{ photons/second} . \tag{7}$$

Let us set $B = 1$, which allows time intervals t of around 1 s . For $B = 1$, $f = 6 \times 10^{14}$ and $T = 6$,

$$p = e^{-4,200}.$$

This is almost no noise photons per time interval.
With codes of any reasonable length and elaborateness, we will fall far short of kT joules/nat,

so far short that we can afford to ignore thermal photons. For optical frequencies and low temperatures, the rate at which we can signal, measured in nats per photon, will be limited by our ability to implement codes, not by thermal photons.

APPENDIX

Here we will consider a single-mode photon communication system in which there is a noise source of photons with an average of n_0 photons per time interval, and a signal source of photons with an average of n photons per time interval when the transmitter is on (when the shutter is open).

According to Shannon, [4] the rate of transmission R measured in nats per symbol (that is, per time interval) is

$$R = H(Y) - H(Y \mid X).$$

Here X represents shutter position (0 = closed; 1 = open) and Y represents photons received (0 = none ; 1 = 1 or more). R is a function of n, n_0 and the probability α that the shutter will be open.

In order to compute $H(Y)$ we need to know the probabilities $p(0)$ (that will receive no photons in an interval) and $p(1)$ (tirat will receive some photons in an interval), assuming that we have no knowledge of X. We see that

$$p(0) = \alpha p(0 \mid 1) + (1 - \alpha)p(0 \mid 0) \tag{A-2}$$
$$p(1) = 1 - p(0) \tag{A-3}$$

It turns out that the number of nats per photon is greatest when the number n of signal photons and the number n_0 of noise photons are much smaller than unity. When this is so, we can use the following approximate expressions for the case in which the shutter is closed, so that there are thermal photons only, and no signal photons

$$p(0 \mid 0) = 1 - n_0 \tag{A-4}$$
$$p(1 \mid 0) = n_0.$$

We have no expression for the case in which the shutter is open and we receive both coherent signal photons and noise photons. However, if we assume that we will receive more photons than the number of signal photons alone, we will underestimate R by disregarding the effect of noise photons when the shutter is open and taking

$$p(0 \mid 1) = 1 - n \tag{A-5}$$
$$p(1 \mid 1) = n$$

Making these assumptions, and assuming that $n_0 \ll n$ and $\alpha \ll 1$, we find

$$\frac{R}{\Omega!} = -\ln n_0. \tag{A-6}$$

This is the number of nats per photon transmitted. Equation (A-6) leads to the classical limit of kT joules/nat when the frequency is high enough so that quantum effects are very strong.

From (2) we see that for a single-mode transmission system, when $hf \gg kT$ the number n_0 of thermal photons in a time t can be taken as

$$n_0 = Bte^{-hf/kT} \tag{A-7}$$

From (A-6) and (A-7)

$$\frac{R}{\alpha n} = \frac{hf}{kT} - \ln Bt. \tag{A-8}$$

Because we have assumed that $hf \gg kT$, the first term on the · right is much larger than unity. What about $\ln Bt$?
B is really a sort of mean bandwidth of the optical filter in Fig. 1. This must be made wide enough so as not to lose many signal photons when the shutter is open, but narrow enough not to let in too many noise photons. This means that Bt should be around unity, but probably somewhat larger.

Thus, when quantum effects are most pronounced, we can disregard the second term in (A-9). Then

$$\frac{R}{\omega n} = \frac{hf}{kT} \text{ nats/photon.} \tag{A-9}$$

This corresponds to

$$\frac{1}{kT} \text{ nats/ioule.} \tag{A-10}$$

Gordon [6] makes a somewhat similar calculation of channel canacity but does not carry the argument to (A-10) above. Equation (A-10) appears to be implicit in Helstrom et al [7] but is not stated explicitly.

References

1. Schelkunoff, S. A. and Friis, H. T., Antenna Theory and Practice, Wiley and Sons, New York, 1952, p. 43.

2. Heffner, H., The Fundamental Noise Limit for Linear Amplifiers, Proc. IRE, 50, 1604-1608, 1962.

3. Gordon, J. P., Louisell, W. H., and Walker, L. R., Quantum Fluctuations and Noise in Parametric Processes, II, Phys. Rev., 129, Januarv, 1963, pp. 481-485.

4. Shannon, C. E. and Weaver, W., The Mathematical Theory of Communication, The University of Illinois Press, 1959.

5. Pierce, J. R., Symbols, Signals and Noise, Harper and Row, 1961, Chapter 10.

6. Gordon, J. P., Quantum Effects in Communication Systems,

Proc. Inst. Radio Eng., 50, 1898-1908, September, 1962.

7. Helstrom, C. W., Liu, J. W. S., and Gordon, P., Quantum Mechanical Communication Theory, Proc. IEEE, 58, October. 1970, pp. 1578-1598.

8. Helstrom, C. W., Capacity of the Purc-State Quantum Channel, Proc. IEEE, 62, January, 1974, pp. 140-141.

9. Yuen, Horace P., Kennedy, Robert S. and Lax, Melvin, Optimum Testing of Multiple Hypotheses in Quantum Detection Theory, IEEE Trans. Information Theory, IT-21, March, 1975, pp. 125− 134.

Scientists have understood since the 1920's that the physical laws which govern atoms, molecules, and elementary particles are very different from the laws of everyday experience. The special laws of the atomic and molecular "microworid" are called quantum mechan-

As an example, if a person measures the position of an electron in space with complete accuracy, his measurement inevitably will kick the electron with a totally unpredictable force. A second measurement of the electron's position, immediately after the first one, wiii give the ics; those of everyday experience are classical mechanics. The laws of quantum mechanics were forced on physicists and chemists in the 1920° s as the only possible way to understand the spectral properties of the light emitted by atoms and molecules.

Quantum mechanics tells us that, whenever a person measures some property of an electron (or of any other object in the microworld), his measurement inevitably will disturb the electron in a somewhat unpredictable way. The more accurate the measurement, the bigger and more unpredictable the disturbance. The disturbance is not due to the person's in trinsic and inevitable feature of the laws of quantum mechanics.

29.9 VI. 8 Quantum Nondemolition Measurements by Braginsky, Vuruntsuv, Thorne

Summary. Some iuture gravitationai-wave antennas will be cylinders of mass - 100 kilograms, whose end-to-end vibrations must be measured so accurately (10^{-19} centimeter) that they behave quantum mechanically. Moreover, the vibration amplitude must be measured over and over again without perturbing it (quantum nondemolition measurement). This contrasts with quantum chemistry, quantum optics, or atomic, nuclear, and elementary particle physics, where one usually makes measurements on an ensemble of identical objects and does not care whether any single object is perturbed or destroyed by the measurement. This article describes the new electronic techniques required for quantum nondemolition measurements and the theory underlying them. Quantum nondemolition measurements may find application elsewhere in science and technology.

Scientists have understood since the 1920's that the physical laws which govern atoms, molecules, and elementary particles are very different from the laws of everyday experience. The special laws of the atomic and molecular "microworld" are called quantum mechanics; those of everyday experience are classical mechanics. The laws of quantum mechanics were forced on physicists and chemists in the 1920's as the only possible way to understand the spectral properties of the light emitted by atoms and molecules.

Quantum mechanics tells us that, whenever a person measures some property of an electron (or of any other object in the microworld), his measurement inevitably will disturb the electron in a somewhat unpredictable way. The more accurate the measurement. the bigger and more unpredictable the disturbance. The disturbance is not due to the person's incompetence; rather, it is an intrinsic and inevitable feature of the laws of quantum mechanics.

As an example, if a person measures he position of an electron in space with complete accuracy, his measurement inevitably will kick the electron with a totally unpredictable force. A second measurement of the electron's position, immediately after the first one, will give the same position as the first one did; but a measurement of the electron's momentum will give a completely unexpected result.

If, nevertheless, the momentum is measured very carefully and some definite result is obtained, that momentum measurement inevitably will disturb the electron's position by an unpredictable amount. If a second momentum measurement is made, the result is known in advance: it will be the same as just obtained. But if the next measurement is of position, nobody can know the result in dvance.

It matters not at all how the person makes his measurements-with the best technology of the 1920's, or the best of the 1980's, or the best of the 23rd century: an accurate position measurement must completely disturb the momentum; an accurate momentum measurement must completely disturb the position.

As bizarre as this situation may seem, it is even more bizarre when studied in greater depth-as was done theoretically by Nicls Bohr, Weinet Heisentetg, John von Neumann, Wolfgang Pauli, and others in the 1920's and 1930's. [See the textbook of Bohm (!) for details; see (2) for a detailed illustrative example.] It turns out that the unpredictable disturbance is a direct result of the extraction of information about the particle's position or momentum. It matters not how the information is extracted, nor where it is stored-in a person's brain, on magnetic tape, or in some minute change of the state of some other particle. So long as the information exists somewhere in the universe outside the original particle (more precisely, "outside the particle's wave function"), future measurements of the particle will reveal that the disturbance has occurred. The only way to undo the disturbance is to "run the measuring apparatus perfectly backward" and thereby reinsert all the information back into the particie. Only if no trace of the information remains anywhere, not even in the experimenter's brain, can the particle return to its original undisturbed state.

The quantum theory of measurement (I), which tells us these things and more, is very widely but not universally accepted by physicists. Einstein never fully accepted it (3); Lamb, a Nobel Prize winner for his experimental work in quantum physics, does not fully accept it (4). The authors of this article do accept it, and will presume it to be correct throughout this article.

The quantum theory of measurement tells us that, if a measurement is somewhat imprecise, then the magnitude of its disturbance is somewhat but not entirely predictable. For example, a very careful measurement of the east west position of an electron, with an imprecision Δx, can be guaranteed to disturb its east-west momentum by not much more than $\Delta p = \hbar/(2\Delta x)$, where $\hbar\,(\equiv 1.054 \times 10^{-27}$ cmgcm/sec) is Planck's constant. However o 1 er careful the measure er, neasurement may be, the mometitum uncertainty afterward will be at least $n^2/(2\Delta x)$. Similarly, a momentum measurement of precision Δp will leave the position uncertain by at least $\Delta x = k/\,(2\Delta_p)$-but if the measurement is very careful, the position disturbance need not be much larger than this. The limit $\Delta r \Delta p \geq \hbar/2$, which holds for either type of measurement, is called the Heisenberg uncertainty principle.

The ultimate limits imposed by the uncertainty principie have been explored in great detail during the past decade by C. W. Helstrom, R. L. Stratanovich, J. P. Gordon, and vihers. They have deveioped a beautiful, mathematical theory of optimum quantum mechanical measurements (quantum detection and estimation theory) (5). Unfortunately, this theory assumes one can make a precise measurement of one observable or another, or of some combination of observabies: but it does not spell out ables; but it does not spell out how such precise measurements can he realized technically-even in principle.

This gap in the theory is being confronted today in the effort to detect cosmic gravitational waves (6). Gravitywave detectors consist of aluminum (or sapphire or silicon or niobium) bars, weighing between 10 kilograms and 10 tons, which are driven into motion by passing waves of gravity. The motions are very tiny: for the gravity waves that theorists predict are bathing the earth, a displacement $\delta x \cong 10^{-19}$ centimeter might be typical (6). And this displacement may oscillate, due to oscillations of the gravity wave, with a period $P \sim 10^{-3}$ second. To see the details of the gravity wave, one must thus make repeated measurements of the bar's position with precision $\Delta_x \leq 10^{-19}$ cm, and with time intervals between measurements of $\bar{\tau} \leq 10^{-3}$ second.

For all measurements ever made in the past on a heavy bar, the effects of quantum mechanics were totally negligible; the classical mechanics of everyday experience gave a perfectly adequate description of the bar's behavior. But one never before tried to make measurements of such

enormous precision as 10^{-19} cin. If the bai is suspended fieely like a pendulum, as it is in some detectors (6), then over time intervals $\boldsymbol{\nabla}\cdot \sim 10^{-3}$ second it will behave as though it were not suspended at all. It will be as free to move horizontally as the electron described above-and like the electron it will be subject to the laws of quantum mechanics: an "initial" measurement of the har's east-west position with precision $\Delta x_{\mathrm{i}} \cong 10^{-19}$ cm will inevitably disurb the bar's east-west momentum by $\Delta p \geq (\hbar/2\Delta x_i)$, and correspondingly will disturb its velocity by $\Delta v = \Delta p/m \geq (\hbar/2m\Delta x_{\mathrm{i}})$, where m is the bar's mass. During the time interval $\tilde{\tau} \sim 10^{-3}$ second between measurements, the mass will move away from its initial position by an amount, $\Delta x_{\mathrm{m}} = \Delta\nu \quad \bar{\tau} \geq (\hbar\bar{\tau}/2m\Delta x_{\mathrm{i}})$, which is unpredictable because Δv is unpredictable. Putting in numbers ($\bar{\tau} = 10^{-3}$ second, $m = 10$ tons, $\Delta x_1 = 10^{-19}$ cm), we find $\Delta x_{\mathrm{m}} \geq 5 \times 10^{-19}$ cm-which is somewhat larger than the desired precision of our sequence of measurements. If the next measurement reveals a position changed by as much as 5×10^{-19} cm, we have no way of knowing whether the change was due to a passing gravity wave or to the unpredictable, quantum mechanical disturbance made by our first measurement. In effect, our first measurement plus subsequent free motion of the bar has "demolished" all pos-
sibility of making a second measurement of the same precision, $\Delta x \sim 10^{-19}$ cm, as the first, and of thereby monitoring the bar and detecting the expected gravity waves.

In principle one can circumvent this problem by making the bar much heavier than 10 tons (recall that Δx_{m} is inversely proportional to the mass). However, this is impractical. In principle another solution is to shorten the time between measurements (recall that Δx_m is directly proportional to $\tilde{\tau}$). However, this will weaken the graviiational-wave signai ($\delta x_{\mathrm{GW}} \propto \tilde{\tau}^2$ for $\bar{\tau} \leqslant 10^{-3}$ second) even more than it reduces the unpredictable movement of the bar ($A_{x_m} \approx \bar{T}$).

The best solution is cleverness: find some way to make the gravity-wave effect stronger; this is being done in laserinterferometer gravity-wave detectors (6), but only at the price of having to (6), 10^{-16} cm the price of having to makingtive displacement of two bars as far apart as several kilometers. Alternatively, find some way to circumvent the effects of the Heisenberg uncertainty principlethat is, some way to prevent the inevitable disturbance due to the first measurement, plus subsequent free motion, from demolishing the possibility of a second accurate measurement: a quantum nondemolition (QND) method.

One QND method which could work
principle is this: instead of measuring the position of the 10 -ton bar, measure its momentum with a small enough initial error, $\Delta p_{\mathrm{i}} \sim 10^{-9}$ g cm/sec, to detect the expected gravity waves. Thereby inevitably disturb the bar's position by an unknown amount $\Delta x \geq \hbar/2\Delta p_{\mathrm{i}} \sim 5 \times 10^{-19}$ cm . Wait a time $\bar{\tau} - 10^{-3}$ second and then make another momentum measurement. As the bar moves freely between the measurements, its momentum remains fixed. The uncertainty Δx in the bar's position does not by free evolution produce a new uncertainty Δp_m in the momentum. Consequently the second measurement can have as good accura-
cy, 10^{-9} g cm/sec. as the initial measurement; and a momentum change of (a few) $\times i\hat{0}^{-4}$ g cm/sec due to a passing gravity wave can be seen.

Momentum measurements can be quutum nondemolition, but position measurements cannot be, for this simple reason: in its free motion between mearear keeps its momentum surcments the bar keeps to momention by constant, but it changes its position by an amount $\delta x = (p/m)\tau$ that depends on the momentum, and that therefore is uncertain because of measurement-induced uncertainties of the momentum. We say that momentum is a QND variable, but position is not.

Unfortunateiy, however, it is fa casier to measure position than momentum. Nobody has yet invented a technically realizable way of making momentum measurements with the required precision.

The problem of inventing a technically realizable QND measurement scheme was first posed in 1974 (8). This reference also formalized the concept of QND measurements. Subsequent developments in the theory of **QND** are due largely to Unruh (9, 10); Braginsky, Vorontsov, and Khalili (11. 12); Caves, Thorne, Drever, Zimmermann, and Sandberg (13-15): and Hollenhorst (16). Salle All of this work has been has shown that in principle QND measurement schemes can completely circumvent the disturbing back-action effects of onc's measurements, and it has led to several tentative designs for practical QND measurements in gravitywave detectors-designs which do not involve measuring momentum.

Actual laboratory work on QND measurement schemes is only now beginning to get under way, and the levels of sensitivity required are so great that we cannot hope for any laboratory results until several years from now. Nevertheless, it is reasonable to expect QND measurements to be a routine part of gravitywave technology by the late 1980's.

The purpose of this article is to make as wide an audience as possible aware of these developments, so that people can begin to ask whether the QND idea might be useful in other areas of science and technology. To achieve this purpose effectively, we feel it necessary to write the rest of this article at a somewhat technical level. We hope thereby to convey to physicists, engineers, chemists, and familiar with elementary and others ramiliar with elementary quantum mechanics and elementary electronics, a deep enough understanding of the QND idea that they can begin to think creatively about it themselves.

29.9.1 Resonant-bar Gravitational-wave

Antennas

Although the QND idea is explained most easily, as we have done, in terms of bars which move freely (free masses), QND measurements are most needed for a different type of gravity-wave antenna: one made of a bar which oscillates mechanically in its fundamental mode (bar mass, $m = 10$ to $10,000$ kg, oscillation frequency, $\omega/2\pi \approx 500$ to 10,000 hertz) (6). The expected gravity waves should produce changes of oscillation amplitude $\delta x = 10^{-18}$ to 10^{-19} cm, which are less than or of order the width of the quantum mechanical wave packet of the oscillator $\delta x_{\rm QM} = (\hbar/2m\omega)^{1/2}$, if the oscillator is in its ground state or in a coherent (minimal-wave-packet) state. Here, by contrast with nuclear, atomic, and elementaryparticle physics, there is only one quantum mechanical system being measured (the oscillator), rather than an ensemble of systems. ous sequence of this one system.

Such an oscillator will actually behave quantum mechanically even in the presence of thermal Brownian motion and at bar temperatures $kT \gg \hbar\omega$, so long as its quality factor O is sufficiently highthat is, so long as the fundamental mode that is, so long as the fundamental mode of the bar is coupled sufficiently weakly to the other, thermalized modes (7). In particular, when one is making energy measurements which put the oscillator in an energy eigenstate, Brownian motion during one cycle will change the number of quanta n in the oscillator by less than unity if (7)

$$\left(n + \frac{1}{2}\right) KT/Q < n\omega/4\pi \tag{ia}$$

and if one is making amplitude measurements, Brownian motion during the measurement time $\tilde{\tau}$ will change the amplitude by less than the coherent state wave-packet width $(\hbar/2m\omega)^{1/2}$ if (7)

$$2kT\bar{\tau}/Q < \hbar \tag{lb}$$

(see Eqs. 40 and 41 below).

In order to monitor the effects of a weak gravity-wave force on such an oscillator, one must use

a measurement technique whose back action on the oscillator, together with subsequent free evolution, does not substantially disturb the probability distributions of the observables being measured-a QND technique. In the following sections we shall uscribe the theory of such QND measurement techniques as applied to oscillators, to free masses, and more generally to any quantum mechanical system. Throughout our description we shall try to give short, elementary proofs of most of the results quoted. More elegant and rigorous proofs will be found in the prito undersiand our dismary iterature. To understand cussion, the reader must be familar with elementary quantum mechanics and elementary electronic circuit theory, but little other specialized knowledge should be needed.

29.9.2 General Theory of Quantum

Nondemolition Measurements

Consider a system, such as an oscillator, that has some observable $\hat{A}$ which an experimenter wishes to monitor. For the moment, assume that the system's

only coupling to the external world is through the experimenter's measuring annaratus. We define a OND measurement of $\hat{A}$ as a sequence of precise measurements of $\hat{A}$ such inat the result of each measurement is completely predictable from the result of the first measure-ment-plus, perhaps, other information about the initial state of the system. This definition, and the ramifications which follow, are a refinement by Caves [in (15)] of Braginsky and Vorontsov's (8) original concept of quantum nondemolition. A similar refinement has heen developed independently by Unruh (10).

Quantum nondemolition measurements are ideal tools for use in the detection of weak external forces (such as gravity waves) that act on the system. One need only perform a QND monitoring of the evolution of A and watch for deviations from the predicted evolution.

Most observables cannot, even in principlc, be monitored in a QND way. In any precise measurement of an observable $\hat{A}$, the back action of the measuring apparatus uncontrollably and unpredictably kicks all observables C which fail to commute with $\hat{A}$; and then, in the subsequent free evolution of the system, the contamination in $\hat{C}$ may be fed into $\hat{A}$, making the results of future measurements of $\hat{A}$ unpredictable. Only very special observables can be immune to such feedback contamination; they are called QND observables [or sometimes generalized QND observables (15) Mathematically, $\hat{A}$ is a QND observable if and only if, when the system is evolving freely in the Heisenberg picture, $\hat{A}$ commutes with itself at the different moments of time t_j, t_k when one makes one's measurements (10,15)

$$\left[\hat{A}\left(t_j\right), \hat{A}\left(t_k\right)\right] = 0 \tag{2}$$

If this condition is satisfied at all times t_j and t_k, then $\hat{A}$ is called a continuous QND observable; if it is satisfied only at

QND observable. If $\hat{A}$ is conserved during free evolution ($d\hat{A}/dt = 0$), then it is guaranieed to satisfy Eq. 2 for all i_j, i_k and therefore to be a continuous QND observable.

In the case of a free particle, the energy and momentum are conserved and are continuous QND observables, but the position is not: $\hat{x}(t+\tau) = \hat{x}(t) + \hat{r}\tau/m$, so

$$[\hat{x}(t), \hat{x}(t+\tau)] = i\hbar\tau/m \tag{3}$$

Precise measurements of $\hat{x}$ perturb $\hat{p}$ uncontrollably, and the contamination in $\hat{p}$ subsequently feeds back into $\hat{x}$ as the particle moves freely.

For a hammonic oscillator the position and momentum satisfy the commutation relations

$$[\hat{x}(t), \hat{x}(t+\tau)] = (i\hbar/m\omega)\sin\omega\tau \tag{4a}$$
$$[\hat{p}(t), \hat{p}(t+\tau)] = i\hbar m\omega \sin\omega\tau$$

(4b)

These imply that $\hat{x}$ and $\hat{p}$ are not continuous QND observables. However, if one makes one's measurements stroboscopically at times separated by an integral number of half-periods ($\tau = \kappa\pi i\omega$; $\sin\omega\tau = 0$), then the commutators in Eqs. 4 a and 4 b vanish. This means that $\hat{x}$ and $\hat{p}$ are stroboscopic QND observables (I2, 13). Stroboscopic QND measurements (12, 13) of $\hat{x}$ or $\hat{p}$ drive the oscillator into a state where $\hat{x}$ is known precise-ly-for example, at moments $t = k\pi/\omega$ and $\hat{p}$ is known precisely at $t = \left(k + \frac{1}{2}\right)\pi t\omega$; but at other times $\hat{x}$ and $\hat{p}$ are highly uncertain. For an oscillator the conserved quantities, which are guaranteed to be QND observables at any and all times, include the energy (8) and the real and imaginary parts of the complex amplitude (/3)

$\hat{X}_1 = \hat{x}(t)\cos\omega t - [\hat{p}(t)/m\omega]\sin\omega t$

$$\hat{X}_2 = \hat{x}(t)\sin\omega t + [\hat{p}(t)/m\omega]\cos\omega t \tag{5b}$$

High-precision measurements of $\hat{X}\hat{X}_{\text{ext}}$ (when full $\hat{X}$ back-action-evading measurements (14, 15) because they enable the measured component of the amplitude (for example, $\hat{X}_1$) to avoid back-action contamination by the measuring device, at the price of strongly contaminating the other component ($\hat{X}_2$). (The uncertainty relation

$$\dot{\Delta}\ddot{X}_1\dot{\Delta}\ddot{X}_2 \geq \check{n}/2m\omega \tag{5c}$$

is enforced by the commutation relations $\left[\hat{X}_1, \hat{X}_2\right] = i\hbar/m\omega$, which follow from [$\hat{x}, \hat{p}$] = i $\hbar$.)

Let $\hat{A}$ be a QND observable which is to be monitored by a sequence of perfect QND measurements at times t_0, t_1, t_2,

Since $\hat{A}(t_0)$ and $\hat{A}(t_j)$ commute (QND assumption; Heisenberg picture), one can perform a perfect "state-preparation measurement" at time t_0, which puts the system into a simultaneous eigenstate $\langle\psi_0\rangle$ of the observables $\hat{A}(t_0)$, $\hat{A}(t_1), \hat{A}(t_2)\ldots$ with some (not previously predictable) eigenvalues $A(t_0)$, $\dot{A}(t_1), \dot{A}(t_2), \ldots$. . From ile results of this firt measurement one can compute the e $A(t), A(t), A(t)$ in $A(t_0), A(t_2), \ldots$ Lat(ψ) remains fixed in time, while its observable $\hat{A}$ evolves through the values $\hat{A}(t_1), \hat{A}(t_2), \ldots$ Subsequent perfect measurements of $\hat{A}$ at times t_1, t_2, . must give the known eigenvalues $A(t_1)$, $A(t_2)$ and must leave the state of the system $|\psi_0\rangle$ unchanged. If $\hat{A}$ is a continuous QND observable, then the QND measurements can be made continuously, and each measurement can last as long or as short a time as one wishes. If $\hat{A}$ is a stroboscopic QND observable, then each measurement must be made very quickly (stroboscopically) to avoid contamination. Examples will be given below, and further detail will be found in section IV of (15).

The apparatus used in any measurement consists of a sequence of stages, through which information flows toward de experimenter's eyes and brain. Measurement theory asserts that, although the early stages of the apparatus may behave quantum mechanically, the late stages must be classical. There is no universaily accepied definition of classical. We shall regard a stage as classical if the quantum mechanical uncertainties of it and of subsequent stages have no significant influence on the overall accuracy of the measurement. If the system being studied interacts directly with a classical stage, the measurement is called direct. When, between the system and the first classical stage, there is a quantum stage (quantum mechanical readout system, QRS), the measurement is cailed indirect (17). For

example, the measurement of the position of a particle by its blackening of a photographic plate is direct. The measurement of position by the particle's scattering of light or of an electron is indirect. The vast majority of measurements are indirect. In electronic measuring systems the first classical stage is often the first amplifier.

In deducing quantum limitations on the sensitivity of a specific measuring scheme, one must analyze quantum mechanically everything that precedes the first classical stage. The overall accuracy of the measurement is governed not only by quantum fluctuations in the quantum stages, but also by the details of the couplings between those stages and between them and the measured system. These all influence the signal which enters the first clasical stage and that signal ultimately classical the quantum errors of meadetermines the quantum rrors of measurement.

In practice, if not in principle, the reduction of the wave function occurs when the signal enters the first classical stage. If that signal carries information not only about the observable $\hat{A}$ which interests us but also about observables $\hat{C}$ terests us, but also about observables that an to bemeasurement is impossible. This is because any flow of information about C into the first classical stage will, accord-
ing to the uncertainty principle, be accompanied by unpredictable back-action forces into the quantum stages-backaction forces which must ultimately contaminate all obscrvables that fail to commute with $\hat{C}$, including $\hat{A}$.

Because of this back action, the measurement error must always exceed an ultimate quantum limit. We shall derive that limit under the special assumption that in the Heisenberg picture $\hat{A}$ and $\hat{C}$ are time-independent-either because they are constants of the motion such as $\hat{X}_1$ and $\hat{X}_2$, or because they are timeevolving observables [such as $\hat{x}(t)$ and $\hat{p}(i)$ jevaluated at some fixed moment of time [such as $\hat{A} = \hat{x}(0), \hat{C} = \hat{p}(0)$]. We assume that the "readout observable" of the last quantum stage, $\hat{Q}_{\mathrm{H}}$, which couples into the first classical stage, is expressible as

$$\hat{Q}_{\mathrm{R}} = f(\alpha\hat{A} + \beta\hat{C}) \tag{6a}$$

where

$$[\hat{A}, \hat{C}] = 2i\gamma\dot{n} \quad \text{so} \quad \dot{\Delta A}\dot{A}\dot{\Delta C} \geq \gamma^n \tag{b}$$

with γ a real number. The time evolution of the readout observable $\hat{Q}_{\mathrm{R}}$ is embodied in the function f and/or in the real parameters α and β. Typically, α and β will be sinusoidal functions of time, which are used to code and separate the $\hat{A}$ and $\hat{C}$ signals. We assume that the first classical stage (usually an amplifier) is equally sensitive to signals at the $\hat{A}$ and $\hat{C}$ frequencies. Then no matter how accurately the first classical stage monitors Q_{R}, it must give errors in $\hat{A}$ and $\hat{C}$ related by $\Delta A = (\dot{\beta}/\dot{\alpha})\Delta C$, where $\bar{\alpha}$ and $\bar{\beta}$ are the root-mean-square (r.m.s.) values of α and β. These relative errors, combined with the uncertainty relation (Eq. 6b), with the unceranty ration. imply the ultimate quantum limit

$$\Delta A \geq [(\bar{\beta}/\bar{\alpha})\gamma\hbar]^{1/2} \tag{6c}$$

Return now to the general situation where $\hat{A}$ and $\hat{C}$ might be time-dependent. In order that the instantaneous signal at time t not contain any contaminant infor-
mation about observables $\hat{C}(t)$ which fail to commute with $\hat{A}(t)$, it is necessary and sufficient that $\hat{A}(t)$ commute with that part of the Hamiltonian $\hat{H}_1(t)$ which de scribes the interaction of (I) Grive hell the measuring apparatus (1)

$$\left[\hat{A}(t), \hat{H}_1(t)\right] = 0 \tag{7}$$

In order that information about $\hat{A}$ enter the measuring apparatus, H_1 must depend upon $\hat{A}$. Usually one achieves these conditions by direct coupling of $\hat{A}$ to some observable $\dot{M}$ of the measuring apparatus

$$\hat{H}_{\mathrm{i}} = K\hat{A}\hat{M} \qquad ()$$

In summary, the condition in Eq. 7 guarantees no direct, instantaneous back action of the measuring apparatus on the quantity $\hat{A}$ being measured; and the condition in Eq. 2 guarantees that variables $\hat{C}$ which have been contaminated by back action will not subsequently, by free evolution (with H_1 turned off), feed their contamination into $\hat{A}$. Often, how ever, $\hat{H}_1$ is turned on for a long timeeven for all time. Then there is danger that $\hat{H}_{\mathrm{i}}$ may catalyze an evolutionary feeding of $\hat{C}$ into $\hat{A}$. One can be sure this does not happen if an analysis of the system plus measuring apparatus. including all couplings, reveals that $\left[\hat{A}\left(t_1\right),\ \hat{A}\left(t_2\right)\right] = 0$ for all times t_1 and t_2 at which signals enter the classical stage. However, such a full analysis may be prohibitively difficult.

Fortunately, in one common situation a full analysis is not necessary: Caves [in (15)] has shown that, if A is a continuous QND observable and $\hat{H}_1$ contains no system observables except $\hat{A}$. then the Heisenberg picture evolution of $\hat{A}$ with couplings turned on is identical to its free evolution, and consequentiy $\hat{A}$ is fully isolated from back action-both direct and indirect. Caves (15) has also proved "full isolation of $\hat{A}$ with $\hat{H}_1$ turned on" under more general circumstances.

Just as $\hat{H}_1$ might catalyze an indirect feeding of contaminated variabies $\hat{\hat{C}}$ into $\hat{A}$. so also such feeding might be catalyzed by the coupling of the system to a ciassical exiernal force $F(i)$ (for example, to a gravitational wave). This coupling is embodied in a piece of the Hamiltonian

$$\hat{I}_{\mathrm{F}} = \mu\Gamma\hat{I} \qquad (7)$$

where μ is a coupling constant and $\hat{x}$ is a dynamical variable of the system ($\hat{x}$ is position in the case of a gravitationalwave antenna). If $\hat{A}$ satisfies the selfcommutation condition (Eq. 2) even in the presence of $\hat{H}_{\mathrm{F}}$, then $\hat{A}$ can remain free from contamination. If in addition, free evolution with $\hat{H}_{\mathrm{F}}$ turned on causes an eigenvalue $A(t)$ of $\hat{\boldsymbol{A}}(t)$ to evolve in such a way that, from a precise knowledge of $A(t)$, one can deduce $F(t)$, then A is called a QNDF observable [(15); see also Unruh (10), where this is denoted QNDD]. QNDF observables are ideal tools for monitoring weak, classical forces.

If, on the other hand, the term H_{F} in the Hamiltonian catalyzes an evolutionary feeding of contaminated observables $\hat{C}$ into $\hat{A}$ (that is, if $\left[\hat{A}\left(t_j\right), \hat{A}\left(t_k\right)\right] \neq 0$ in the presence of $\hat{H}_F$), then although $\hat{A}$ may be highly sensitive to the presence of an external force, one cannot hope to monitor the details of the force by measurements of $\hat{A}$.

in the case of an oscillator with position $\hat{x}$ coupled to the force (for example, a gravitational-wave detector), X_1 and $\hat{X}_2$ (Eqs. 5) are QNDF observables and thus can be used for perfect monitoring of the forces (13, 15). By contrast, the oscillator's energy, although a QND observable, is not QNDF. As a result, precise measurements of the energy can reveal the presence of an arbitrarily weak force: but they cannot determine the strength of the force with a precision better than a factor of 3 ($13, 10, 15$)-unless the force is so strong that it increases the energy by an amount large compared to the initial energy. Examples and proofs will be sketched later.

When one is using a quantum system to monitor a classical force F, one can increase one's scnsitivity by increasing the response of the measured quantity $\hat{A}$ to F. In (8) and (18) it is shown that, if $\hat{A}$ is the energy of an oscillator, F produces change of $\hat{A}$ his a change of A which is larger, the larger the oscillator's initial energy. Formally, such a measuring scheme satisfies Unruh's (10) general condition for the dependence of $\hat{\hat{A}}$'s response on the initial state of the detector (detector-dependent response, or DDR)

$$[\hat{\boldsymbol{A}}, \hat{x}] \neq \text{ a } C\text{-number} \tag{10}$$

In the case of (8) and (/8) $\hat{A}$ is the detector's (oscillator's) Hamiltonian, $\hat{A}$ is its position, and $[\hat{A}, \hat{x}] = -(i\hbar/m)\hat{p}$. The larger the initial energy of oscillation, the larger will be $\langle\hat{p}^2\rangle$, and the !arger will be $d\hat{A}/dt$. Further details will be given later.
This completes our sketch of the gen eral theory of QND measurements. This theory will now be applied to various types of measurements of harmonic oscillators, with emphasis on issues relevant to gravitational-wave detection.

29.9.3 Position Measurements

A resonant-bar gravity-wave antenna is an oscillator with mass m, frequency ω, position $\hat{x}$, and momentum $\hat{p}$, which couples to a gravitational wave (classical external force F) with a coupling energy $\hat{H}_{\rm F} = -\hat{x}F(t)$. In most experiments the antenna's position $\hat{x}$ is coupled by a transducer $(H_1 = K\hat{x}\hat{q}; \quad K \equiv$ coupling constant) to an electromagnetic circuit (quantum readout system), which we shall describe as an oscillator with capacitance C, inductance L, generalized coordinate (equal to charge on the ca pacitor) $\hat{q}$, and generalized momentum (equal to flux in the inductor) $\hat{\pi}$. More complicated QRS's can be used; but this is the typical case. The voltage on the capacitor, which is proportional to $\hat{q}$, is monitored by an amplifier-the first classical stage of the measuring system. Thus $\hat{q}$ is the readout observable $\hat{Q}_{\rm R}$ (see Eqs. 6). ps. 6).
The coupled antenna, force, and QRS are governed by the Hamiltonian

$$\begin{aligned}\dot{H} =& \frac{\hat{p}^2}{2m} + \frac{1}{2}m\omega^2\hat{x}^2 \\ &+ \frac{\hat{\pi}^2}{2L} + \frac{\hat{q}^2}{2C} + \hat{H}_F + \hat{H}_{!} \\ \hat{H}_F = -x\bar{F}(t) \quad & \hat{H}_1 = K\hat{x}\hat{q}\end{aligned} \tag{11}$$

for which the Heisenberg evolution cquations are

$$\begin{aligned} d\hat{x}/dt &= \hat{p}/m \\ d\hat{p}/dt &= -m\omega^2\hat{x} + F(t) - K\hat{q} \\ d\hat{q}/dt &= \hat{\pi}/L \\ d\hat{\pi}/dt &= -\hat{q}/C - K\hat{x} \end{aligned} \tag{12}$$

Because these equations ignore the first ciassicai stage (ampiifier) and its detailed back action on the QRS. they cannot tell us the actual sensitivity of the measuring system. On the other hand, they can tell us the ultimate quantum mechanical limit on the sensitivity.

Suppose, as a first case, that the signal $\hat{Q}_{\rm R} = \hat{q}$ is fed continuously into the amplifier for a time much longer than a quarter-cycle of the antenna, and that one's goal is to measure $\hat{x}_0$, the initial value of the oscillator's position. During the measurement $\hat{x}(t)$, which feeds $\hat{\pi}$ and thence $\hat{Q}_{\rm R} \equiv \hat{q}$, oscillates between $\hat{x}_0$ and $\hat{p}_0$. $[\hat{x}(t) = \hat{x}_0 \cos\omega t + (\hat{p}_0/m\omega)\sin\omega t$, aside from minor modifications due to the couplings. Note that $\hat{x}_0 \equiv \hat{X}_1$, $\hat{p}_0/m\omega \equiv X_2$; Eqs. 5.] Consequently, the signal $Q_{\rm R}$ entering the amplifier contains not only $\hat{x}_0$ but also, unavoidably, $\hat{p}_0$. Since their relative strengths in the signal are $p_0/x_0 = m\omega$, the measurement determines them with relative precisions $\Delta p_0 = m\omega\Delta x_0$. Taking account of the un- certainty reiation $\Delta x_0 \Delta p_0 \geq \hbar/2$. we find (19, 18, 12, 15)

$$\Delta x_0 = \Delta p_0/m\omega \geq (\hbar/2m\omega)^{1/2} \tag{13}$$

(This is a specific example of the general quantum limit of Eqs. 6.) Such a mea- surement is called an amplitude-and- phase measurement because it gives in- formation about both the amplitude $\left[{x_0}^2 + (p_0/m\omega)^2\right]^{1/2}$ and the phase $\psi_0 = \tan^{-1}(p_0/m\omega x_0)$ of the antenna's motions. An ideal amplitude-and-phase measurement with the limiting sensitivi- ty in Eq. 13 drives the antenna into a co- herent (minimai-wave-packet) state. If such a measurement (state preparation) has put the antenna into a coherent state ($\tilde{m}\omega$) $\sin\omega t$, win $(\lambda(i)\rangle - \lambda_0 \cos\omega t((\rho)$ then a classical force $F = F_0\cos(\omega t + \varphi)$ acting for a time $\tau \gg 2\pi/\omega$ will leave the state coherent but change its am- plitudes by $\delta x_0 = (F_0\tilde{\tau}/2m\omega)\sin\varphi$, $\delta p_0/m\omega = (F_0\tilde{\tau}/2m\omega)\cos\varphi(15)$. A sub- sequent ideal amplitude-and-phase mea- surement can reveal this change if the force F_0 exceeds the quantum iimit (io)

$$F_0 \simeq (2/\tilde{\tau})(m\omega\hbar)^{1/2} \tag{14}$$

No amplitude-and-phase measurement can do better than this.

An alternative derivation of the quan- tum limits in Eqs. 13 and 14, due to Gif- fard (19) , takes detailed account of quan- tum fluctuations in the amplifier and their back action on the QRS.

The quantum limits in Eqs. 13 and 14 are traceable to the fact that $\hat{x}$ is not a continuous QND observable;a continu- ous measurement of $\hat{x}$ produces direct back action on $\hat{p}$, which then con- taminates $\hat{x}$ through free evolution. On the other hand, $\hat{x}$ is a stroboscopic QND observable (see Eq. 4a) . Consequently, by strobosconic measurements (12. 13) at times $t = 0, \pi/\omega, 2\pi/\omega, \ldots$ one can monitor $\hat{x}$ with perfect precision, in prin- ciple (except for the ridiculous limit from ciple (except for the ridiculous lowit relativistic quantum theory, $\Delta x \geq n/mc = 10^{4!}$cm for $m = 10$ kg) . Sirotosscopic measurements can be achieved with the system of Eq. 11 by pulsing on and off the transduccr's coupling constant K . By a sequence of perfect stroboscopic mea- surements one can monitor an arbitrarily weak force F_0 .

Perfect stroboscopic measurements require that x be coupled to the QRS for arbitrarily short time intervals τ at $t = 0$, $\pi/\omega, \ldots$ (and also that the QRS transfer its information to the first classical stage in a time less than π/ω) . If τ is finite then the momentum spread $\Delta p \geq \hbar/2\Delta x$, pro- duced by a measurement of precision Δx , causes a mean position spread $(\Delta x) \simeq (\Delta p/m)\tau \geq \hbar\tau/2m\Delta x$ during the next measurement. The resulting r. m. s. error is (18, 12, 13)

$$\Delta x \geq (\hbar\tau/m)^{1\geq} \tag{15}$$

The shorter the measurement time τ , the more accurate the measurement can be.

Unfortunately, short measurements

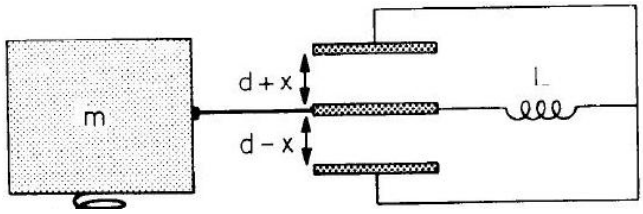


Fig. 1. Scheme for coupling a mechani- cal oscillators (posi- tion) ${ {2}=x{2}$ to an elec- tromagnetic QRS. }

require very strong coupling of the an- tenna to the QRS in order to surmount the quantum mechanical zero-point cincr- gy that accompanies the signal through the QRS and into the

amplifier. This is quantified in (20, 15, 14) for the case of a mechanical oscillator with transducer and QRS that feed the amplifier a sinus- oidal voltage signal

$$V = \sqrt{2}K \times \{\Omega_2 \mid C\cos\Omega\}$$

Here Ω (assumed $\gg 1/\tau$) is the signal frequency, K is the transducer's cou- pling constant, and g_{21} is the transfer function of the QRS. This signal carries an r. m. s. power $P_{\mathrm{s}} = (Kr\,|g_{21}|)^2 / 4\,\mathrm{Re}\,(g_{22})$, where $\mathrm{Re}\,(g_{22})$ is the real part of the oui- put impedance of the QRS. Accom- panying this signal in the experimental bandwidth $1/2T$ is a fuctuating quantum mechanical zero-point power $P_0 =$ the known phase of ^{2} hal27-half of the signat, the other hall at the other phase. This zero-point noise leads to $\Delta x \geq (\hbar/2m\omega)^{1/2}(1/\beta\omega\tau)^{1/2}$, where

$$\beta \equiv \frac{(K\,|g_{21}|)^2}{m\omega^2\,\mathrm{Re}\,(g_{22}\Omega)} \tag{16 h}$$

is a dimensionless coupling constant ($2I$, 20) . If one averages over N successive stroboscopic measurements (total band- width $1/2N\tau$) , then the accuracy im- proves as $N^{-1/2}$

$$\Delta x \approx \left(\frac{2}{n}/2m\omega\right)^{1/2} (1/\beta N\omega\tau)^{1/2} \tag{17}$$

Optimization of the measurement time τ in Eqs. 15 and 17 leads to an ultimate quantum limit for stroboscopic measure ments with finite coupling (14, 15, 20)

$$\tau_{\mathrm{optimal}} = \left(\beta N\omega^2\right)^{-1/2} \tag{18a}$$

$$\Delta x \geq (\hbar/m\omega)^{1/2}(\beta N)^{-14} \tag{18 h}$$

A coupling as large as $\beta = 1$ is dif- ficult to achieve. Therefore, to beat the amplitude-and-phase quantum limit $(\hbar/2m\omega)^{1/2}$, one will probably have to av- erage over a large number N of measure- ments.

By a sequence of stroboscopic mea- surements at the quantum limit of Eq. 18b, one can monitor a classical force $F = F_0\cos(\omega t + \varphi)$. If the phase φ is near $\pi/2$ or $3\pi/2$, then the optimal times for the stroboscopic measurements are $t = 0, \pi/\omega, 2\pi/\omega, \ldots$; the force pro- duces during N half-cycles $\delta x = (\pi/2)\,(NF_n/m\omega^2)$. and the force is mea- surable if

If the phase φ is near 0 or π , then the precision of Eq. 19 is achieved by sire- boscopic measurements at $t = \pi/2\omega$, $3\pi/2\omega, \ldots$ Since the phase of a gravi- tational wave is not predictable in ad- vance, two antennas are needed;one to be monitored at $t = 0, \pi/\omega, \ldots$, the other at $t - \pi/2\omega, 3\pi/2\omega, \ldots (12, 13)$.

The stroboscopic limits of Eqs. 15, 17,
and 19 strictly speaking refer to a har- monic occillator with only one degree of freedom. Unfortunately, a resonant-bar freedom. Unfortuna, a gravitational-wave antenna has many normal modes which can all be simulta- neously perturbed by the back action of each measuremeni. However, if the strongly perturbed modes have commen- surate eigenfrequencies, then strobo- scopic QND measurements on the fun- damental mode are also QND for the other modes (/2) , and results near the limits of Eqs. 15 to 18 may be achievable.
able.
Stroboscopic measurements can be carried out on electromagnetic oscilla- torssuch as inductance-capacitance (LC) circuitsas well as on mechanical oscillators. For example, one could send a collimated pulse of electrons through the capacitor so quickly that it spends a time $\tau \ll 2\pi/\omega$ between the capacitor plates. The electrons will be deflected by the electric

field of the capacitor, which is proportional to the oscillator's gener- alized coordinate q ($\equiv$ charge on plates) ; and hy measuring the deflection one can infer q . A stroboscopic sequence of such measurements can reveal q , in principle,
to an accuracy $(h\tau/L)^{1/2} = (hC\omega^2\tau)^{1/2}$ (see Eq. 15) and can reveal the corresponding voltage in the capacitor to $\Delta V = (\hbar\omega/C)^{1/2}(\omega\tau)^{1/2}-$ which is a factor $(\omega\tau)^{1/2}$ better than the standard ampli-tude-and-phase quantum limit.

29.9.4 Energy Mieasurements

Suppose that one has developed a method for making accurate measurements of a harmonic oscillator (antenna), and that an initial "state-preparation" measurement has put the oscillator into an eigenstate with energy E_0. A force $F_0 \cos(\omega t + \varphi)$ acting for time $\tilde{\tau}$ will change pe the oscitator s state. Because the phase of the initial state is completely indeterminate, no interference terms show up in the new state's energy expectation value (22)

$$\langle E\rangle = E_0 + W \quad W \equiv {F_0}^2\bar{\tau}^2/8m \tag{20a}$$

However, interference is a dominant effect in the variance of the new state's energy (22)

$$\sigma(E) = (2E_0W)^{1/2} \tag{20b}$$

The next measurement is likely to reveal a changed energy, and thereby tell us that a force has acted, if $\sigma(E) \approx \hbar\omega$. (Here we assume the force to be weak, $W < E_0$.) Rewritten in terms of F_0, this detection criterion is

$$F_0 \geq \frac{2}{\bar{\tau}}\left(\frac{m\omega\hbar}{n_0 + \frac{1}{2}}\right)^{1/2} \tag{21}$$

where $n_0 = E_0/\hbar\omega - 1/2$ is the number of quanta in the initial state. This forcedetection method can be arbitrarily sensitive if n_0 is made arbitrarily large (8 , 18). However, because there is no unique relationship between the measured energy and F_0 [$\sigma(E) \gg \langle E\rangle - E_0$], this method cannot tell us the precise magnitude of F_0. In other words, the energy is not a QNDF observable (13, 10, 15); see the discussion following Eq. 9.

A nerfect energy measurement (perfect up to one quantum) is possible only if (i) the interaction Hamilionian $f_1 f_0$ the oscillator and QRS involves the oscillator energy $\hat{H}_0$, and (ii) $\hat{H}_1$ commutes with $\hat{H}_0$; see Eq. 7 and associated discussion.

If instead $\hat{H}_1 = K\hat{x}\hat{q}$, as occurs in most measuring systems, then the directly measured quantity is $\hat{x}(t)$-or the amplitudes $\hat{x}_0$ and $\hat{p}_0$-and the measurement is of the amplitude-and-phase type with quantum limits $\Delta x_0 = \Delta p_0/m\omega \geq (\hbar/2m\omega)^{1/2}$ (Eq. 13). From the measured $x_{\hat{p}}$ and $p_{\hat{p}}$ one can compute the oscillator's energy
$E_0 = {p_0}^2/2m + m\omega^2{x_0}^2/2 = (n_0 + 1/2)\,\hbar\omega$ up to an accuracy, for $n_0 \gg 1$

$$\Delta E = p_0\Delta p_0/m + m\omega^2 x_0\Delta x_0 \geq n_0^{1/2}\hbar\omega \tag{22}$$

The effect of the force will be discerinible if this error is less than $\sigma(E)$ (Eqs. 20), which implies the same forcedetection criterion (Eq. 14) as we derived from our original amplitude-andphase discussion.

One way to achieve an $\hat{H}_1$ which involves $\hat{H}_0$ rather than $\hat{x}$-and to thereby beat the amplitude-and-phase limit (Eq. 14)-is to make the oscillator's mass m and spring constant $m\omega^2$ depend weakly on a variable $\hat{q}$ of the QRS : $m = m_0/(1 + K\hat{q}), m\omega^2 = m_0{\omega_0}^2(1 + K\hat{q})$ (10). Then the total Hamiltonian becomes

$$\hat{H} = \hat{H}_0 + \hat{H}_1 + \hat{H}_{\rm QRS}$$
$$\hat{H}_0 = \hat{p}^2/2m_0 + \frac{1}{2}m\omega_0^2\hat{x}^2 \tag{23}$$
$$\hat{H}_1 = K\hat{q}\hat{H}_0$$

where $\hat{H}_{\rm QRS}$ is the Hamiltonian of the free quantum readout system. Unruh (10) has given a pedagogical example of this for an electromagnetic oscillator: the "mass" m is an inductance; the "spring constant" $m\omega^2$ is $1/($ a capacitance $)$; and
the inductor coil and capacitor plates are attached to a mechanicai pivot with angular position $\hat{q}$. which varies the inductance and capacitance in the required manner. One can also vaty the inductance and capacitance by letting the mechanical QRS move appropriate materials in and out of the inductor and capacitor (11,13).

For a mechanical oscillator with electromagnetic QRS there are also several ways to make the mass and spring constant depend on a QRS variable. In Fig. 1 the oscillator's mass is attached to a abse cator plate of the QRS the energy in the capacitors electric fieid is

$$E_{\rm c} = \left[1 - (\hat{x}/d)^2\right]\hat{q}^2/2C \tag{24}$$

where C is the capacitance when $x = 0$: and consequently the charge $\hat{q}$ on the central plate of the QRS renormalizes the spring constant to $m\omega^2 = m_0{\omega_0}^2 - \hat{q}^2/2Cd^2$. The spring constant can also be renormalized by the QRS "momentum" $\hat{\pi}$ ($\equiv$ flux in inductor) by attaching the oscillator's mass to a current-carrying coil that resides between two oppositely wound coils of the QRS inductor. To renormalize the oscillator's mass m one might attach to it a conducting plate that resides in the inductor's magnetic field. The velocity of the plate through the magnetic field would induce an electric dipole moment on the plate, which in tuin would couple by its velocity to the magnetic field, giving an interaction energy proportional to $\hat{p}^2\hat{\pi}^2$ and thence a mass renormalization.

Unfortunately, these various ideas have not yet produced a viable design for clean coupling of a mechanical oscillator's energy $\hat{H}_0$ to a QRS. On the other hand, designs without clean coupling can still yield measurements of $\hat{H}_0$ more accurate than the amplitude-and-phase quantum limit $(n_0 + 1/2)^{12}\,\hbar\omega$. An example is a QRS that couples only to $\hat{x}^2$, but that averages $\hat{x}^2$ over a number of cy-
cles before sending it into the first classical siage (amplifier) ($9, 1i$). The measurement scheme of Fig. 1 will do this if the period of the circuit's (QRS) oscillathe period of the circuits (QRS) oscilathe memoriscillan period of the cuit's capacitance (Eq. 24) and resonant frequency will be sensitive to the time average of $\hat{x}^2$ and thence to H_0, with only small admixtures of sensitivity to the time-varying part of $\hat{x}^2$ and thence to the oscillator's phase ψ. This is equivalent to the statement in Eq. 6 that $\hat{Q}_{\rm R} = f\left(\hat{H}_0 + \alpha\left\langle\hat{H}_0\right\rangle\hat{\psi}\right)$ with $\bar{\alpha} \ll 1$, which in turn permits accuracies much better than $\Delta E - (n_0 + \mathbf{i}/2)^{1/9}$ nw. A ctailed analy sis of this type of scheme is given in (II), but for an electromagnetic oscillator with mechanical QRS and with $\hat{H}_1 = K\hat{x}^2\hat{q}$ a mechanical QRS and with $H_1 - Kxq$ rather than $K\hat{x}^2\hat{q}^2$ as in Fig. 1 and Eq. 24. That analysis reveals a limiting sensitivity

$$\Delta E \approx \left(n_0 + \frac{1}{2}\right)^{1/2}(\Omega/\omega)^{1/2k}\frac{k}{1/\omega} \tag{25a}$$

where $E = (n_0 + 1/2)\,\hbar\omega$ is the oscillator's energy, ω is its frequency, Ω is the ficuluency of the QRS, and $\Omega \ll \omega$. The corresponding limit on the detection of a classical force $F_0\cos(\omega t + \varphi)$, which drives changes in the oscillator's energy, is

$$F_0 \geq \frac{2}{\tau}\left(\frac{m\omega\hbar}{\omega/\Omega}\right)^{1/2} \tag{25b}$$

if $\omega/\Omega < n_0 + 1/2$. If $\omega/\Omega > n_0 + 1/2$, then the limit on ΔE in Eq. 25 a is replaced by $\hbar\omega$, the ultimate precision with which one can ever measure energy changes; correspondingly, the force limit in Eq. 25b is replaced by Eq. 21.

In measurements of the time average of $\hat{x}^2$ and thence $\hat{H}_0$, it is not essential that the interaction Hamiltonian $\hat{H}_1$ involve $\hat{x}^2$. Instead $\hat{H}_1$ can be proportional to $\hat{x}$, and then the internal workings of the QRS can produce the average of $\hat{x}^2$ at the entrance to the first classical stage.

29.9.5 Back-action-evading Measurements of $\hat{x}_1$

The QNDF observable $\hat{X}_1 = \hat{x}\cos\omega t$ - ($p/m\omega$) $\sin\omega t$ (real part of complex amplitude; Eq. 5), like the position $\hat{x}$. has a continuous spectrum of eigenvalues; and in principle it can be measured arbitrarily quickly and accurately (13, 15). Suppose that an initial state-preparation measurement at $t = 0$ has put the oscillator into an eigenstate $|\xi_0\rangle$ of $\hat{X}_1(0)$ with eige ξ classion for $F(t)$ eigenval so. A $\hat{H} - \hat{\hat{H}}$ for tal Hamiltonian $A - H_0 - \hat{x}F(t)]$ win change $\hat{X}_1$ as seen in the Heisenberg picture
$\hat{X}_1(t) = \hat{X}_1(0) - \int_0^i [F(t')/m\omega]\sin\omega t' dt'$
(26) In the Heisenberg picture the oscillator's state remains fixed in time at $|\xi_0\rangle$, but this is an eigenstate of $\hat{X}_1(t)$ with eigenvalue

$$\xi(t) = \xi_0 - \int_0^t [F(t')/m\omega]\sin\omega t' dt' \tag{27a}$$

Subsequent perfect measurements of $\hat{X}_1$ must yield this eigenvalue and will reveal the full details of its evolution. It evolves in exactly the same manner as X_1 would evolve for a classical oscillator (13,15). One pays the price, in these measurements, of not knowing anything about the imaginary part of the compiex ampii-
tude $\hat{X}_2$ (Eq. 5c). However, if one has a second oscillator coupled to the same force $F(t)$, one can measure the imaginary part $\hat{Y}_2$ of its complex amplitude, giving up alli information about the real part Y_1. One's measurements must give the eigenvalue

$$\eta(t) = \eta_0 + \int_0^t [F(t')/m\omega]\cos\omega t' dt' \tag{27b}$$

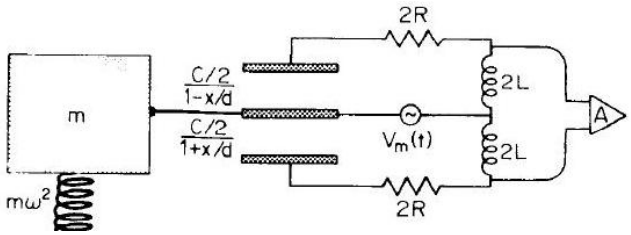
which evolves in exactly the same manner as the X_2 or Y_2 of a classical oscillator. From the output of either oscillator, or better from the two outputs, one can deduce all details of the evolution of $F(t)$, no matter how weak $F(t)$ may be (13,15). Thus $\hat{X}_1$ and $\hat{Y}_2$ are QNDF observables.
A perfect measurement of $\hat{X}_1$ (or $\hat{Y}_2$) requires (i) that the interaction Hamiltonian $\hat{H}_1$ depend on $\hat{X}_1$ and (ii) that $\hat{H}_1$ commute with $\hat{X}_1$ (Eq. 7 and associated discussion). The simplest example is

$$\begin{aligned}\hat{H}_1 =& K\hat{X}_1\hat{\mathfrak{J}} = K\hat{x}_{\hat{q}}\cos\omega t \\ &- (K/m\omega)\hat{p}\hat{q}\sin\omega t\end{aligned} \tag{28}$$

A coupling of this type can be achieved, for a mechanical oscillator, by using a capacitive position transducer with sinusoidally modulated coupling constant $\left(\hat{H}_1 = K\hat{x}\hat{q}\cos\omega t\right)$,

followed by an inductive momentum transducer with modulated coupling constant [H_1 = -$(K/m\omega)\hat{p}\hat{q}\sin\omega t$]. The two transducers iogeiner produce a voitage outpu

Fig. 2. Scheme for stroboscopic or continuous back-actionevading ments of a mechanical oscillator. This scheme was devised
independently in 1978 independently in 1978 and by R. W. P. Drever, but has not previously been published.



involve a standard mechanical current transducer (current $\equiv x$) pius a negative spring in the QRS (15). In principle negative springs can be noise-free (15).

The sinusoidal modulations required in the transducers must be regulated by an external, classical clock, which has the same frequency ω as one's oscillator. One cannot use the oscillator itself as the clock because in extracting the required oscillatory information from the oscillator one will produce an unacceptably large back action on $\dot{X}_1$. However, before the experiment begins one can creck the frequency of the clock againts that of the oscillator in principle they that or the oscilator. in principle they can be made to agree perfectly, and in principle the clock can be made fully classical so its outputs are real numbers, $\cos\omega t$ and $\sin\omega t$, rather than operators (10,15). In practice, frequency drifts and quantum features of the clock need not cause serious experimental problems (I5, 20).

A perfect measurement of $\hat{X}_1$, which
lasts a finite time $\bar{\tau}$, requires infinitely strong coupling in the transducers ($K \to \infty$) in order to give a signal that overwhelms zero-point noise in the QRS. If one has only finite coupling, then the zero-point noise accompanying the signal gives rise to a limit (Eqs. 16 and 17 with $x \to X_1$ and $N\tau \to \tilde{\tau}$)(13-15)

$$\Delta X_1 \geq (\hbar/2m\omega)^{1/2}(\beta\omega\tilde{\tau})^{-1/2} \tag{31}$$

Here β is the dimensionless coupiing constant (Fqs. 16). Thus, whereas stroboscopic measurements with limited coupling can beat the amplitude-andphase limit by a factor of only $(\beta\omega\bar{\tau})^{-1/4}$ (Eq. 18b with $N = \omega\tilde{\tau}/\pi$), continuous back-action-evading measurements of X_1 can beat it by $(\beta\omega\tilde{\tau})^{-1/2}$. Stroboscopic measurements are worse because of their smaller duty cycle.

In the realistic case of weak coupling, $\beta < 1$, one must average over many cycles ($\omega\tilde{\tau} \gg 1/\beta$) in order to substantially beat the amplitude-and-phase
limit. In this case one can make use of a trick analogous to measuring the energy hy copling to $\hat{x}^2$ and averaging: one can perform a "single-transducer, back-ac-tion-evading measurement" (i3-i5) by coupling to
$\hat{x}\cos\omega t\cos\Omega t = \frac{1}{2}\left(\hat{X}_1 + \hat{X}_1\cos 2\omega t\right.$

$$\left. + \hat{X}_2\sin 2\omega t\right)\cos\Omega t \tag{32}$$

(that is, $\hat{H}_1 = 2K\hat{x}\hat{q}\cos\omega t\cos\Omega t$) and then sending the signal through a filter (the QRS) with band pass at frequency $\Omega \gg \omega$ and bandwidth $\Delta f = 1/2\tau_* \ll \omega/2\pi$. The filter will "average the X_2 signal away" until its amplitude has fallen by $1/2\omega\tau_*$ relative to that of the X_1 signal. Since the initial r.m.s. X_2 signal strength is $1/\sqrt{2}$ that of the X_1. this corresponds to $\hat{Q}_{\mathrm{R}} = f\left(X_1 + X_2/2\sqrt{2\omega\tau_*}\right)$ in Eq. 6a, which together with the uncertainty relation in Eq. 5c and the argument of Eqs. 6 tells us that (20)

$$\Delta X_1 \gtrsim (\hbar/2m\omega)^{1/2} \left(2\sqrt{2}\omega\tau_*\right)^{-1/2} \tag{33}$$

This is the error in X_1 due to back action from measurement of X_2. The additional error due to zero-point noise accompanying the X_1 signal into the amplifier is (Eqs. 16 and 17 with $x \to X_1$ and $N\tau \to \tau$)(14, 15, 20)

$$\Delta X_1 \gtrsim (\hbar/2m\omega)^{1/2}(\beta\omega\tilde{\tau})^{-1/2} \tag{34}$$

Here $1/2\tau$ is the bandwidtio of time experiment ($\tilde{\tau}$ is the larger of the QRS averaging time τ_*, and the averaging time in subsequent electronics). The ultimate quantum limit on the sensitivity is Eq. 33 if $\beta > 2\sqrt{2}\tau_*/\tilde{\tau}$, and Eq. 34 if $\beta < 2\sqrt{2}\tau_*/\bar{\tau}$. Note that Eq. 34 is the same limit (to within factors of order unity) as in the case of exact coupling to $X_1 = \hat{x}\cos\omega t - (\hat{p}/m\omega)\sin\omega t$. Thus, when $\beta < 2\sqrt{2\tau_*/\tilde{\tau}}$ and $\omega\tilde{\tau} \gg 1$, one can abandon the momentum transducer without any serious loss of accuracy.

This type of single-transducer, timeaveraged, back-action-evading measurement of X_1 appears today to be the most viable technique for beating the ampli-td-and-phase limit (Eq. 14) in gravita-tional-wave detection. In place of Eq. 14 one will face the limiting measurable force

$$\begin{aligned} F_0 \equiv & (2/\tilde{\tau})(m\omega\tilde{n})^{1/2} \\ & \times \text{Max}\left[(\beta\omega\tilde{\tau})^{-1/2}, \left(2\sqrt{2}\omega\tau_*\right)^{-1/2}\right] \end{aligned} \tag{35}$$

29.9.6 Thermal Noise in the Oscillator and Amplifier

The quantum limits derived above are not achievable in the laboratory today because thermal noise exceeds quantum mechanical noise.

Ignore for the moment thermal (Nyquist) noise in the oscillator. Then if the resistors in the QRS are cooled sufficiently, the dominant nonquantum noise will be that in the amplifier (first classical stage). The amplifier, which we assume to be linear, can be characterized by its power gain G and its noise temperature $T_{\rm n}$. The QRS feeds the amplifier a signal at frequency $f = \Omega/2\pi$, to which the amplifier adds a noise power per unit bandwidth

$$\frac{dP_{\rm n}}{df} = \frac{\hbar\Omega}{\exp\left(\hbar\Omega/kT_{\rm n}\right) - 1} \tag{36}$$

Here k is Boltzmann's constant. If the incoming signal has power $P_{\rm s}$, then the amplified signal and noise have power (23)

$$GP_{\rm s} + \left\{G\frac{\hbar\Omega}{\exp\left(\hbar\Omega/kT_{\rm n}\right) - 1} + \frac{\hbar\Omega}{2}\right\}\Delta f \tag{37}$$

Here Δf is the bandwidth, and the $\hbar\Omega/2$ is a zero-point energy that accompanies the signal throughout its trek through the amplifier and other electronics, but does
not get amplified (23). The quantum limits of previous sections of this articie are attributable to this zero-point energy. In the presence of a real linear amplifier the presence T i nonneglight noise temperature $I_n \gg \hbar\Omega/k$ and large gain $G \gg 1$, the signal power $P_{\rm s}$ must fight not $(\hbar\Omega/2)\Delta f$, but rather
$\left(\frac{\hbar\Omega}{\exp(\hbar\Omega/kT_{\rm n})-1} + \frac{1}{G}\frac{\hbar\Omega}{2}\right)\Delta f$

$$= kT_{\rm n}\Delta f$$

(see Eq. 37). Consequently, it is reasonable to expect that the amplifier noise will modify our quantum limits (Eqs. 6c. 13-15, 17-19, 21, 22, 25, 31, and 33-35) by replacing * with (12)

$$\hbar \to \frac{2kT_{\text{n}}}{\Omega} \tag{39}$$

These modified quantum limits are sometimes called amplifier limits. It will never be possible, even in principle, to reduce these amplifier limits below the corresponding quantum limits (19, 24, 25).

The best linear amplifiers that have been built are parametric amplifiers and maser amplifiers, which operate at microwave frequencies and have (kT_{n}/Ω) as small as $\sim 10\hbar$. With such amplifiers one can only hope to get within a factor 20 or $\sqrt{20}$ of our quantum limits ($\hbar \to 20\hbar$). And even to achieve this one must design a QRS which upconverts the oscillator's signal frequency (kilohertz in the gravitational-wave case) to the mi crowave (gigahertz) region.

Any physical oscillator (such as the fundamental mode of a gravitationalwave bar antenna) is weakly coupled to a thermal bath of dynamical systems (sound waves in the bar). This coupling produces a frictional damping of largeamplitude motions, and it also produces a thermal-buffeting random walk of the oscillator's amplitude (Nyquist noise). The r.m.s. random-walk change of the oscillator's amplitude during time $\tilde{\tau}$ is

$(\Delta x_0)_{\text{Nyq}} = (\Delta p_0/m\omega)_{\text{Nyq}}$
$= (\Delta X_1)_{\text{Nyq}} = (\Delta X_2)_{\text{Nyq}}$

$$= \left(kT/m\omega^2\right)^{1/2} (\omega\tilde{\tau}/Q)^{1/2} \tag{40}$$

Here T is the temperature of the thermal bath (the bar's temperature), and Q is the oscillator's quality factor (number of radians of oscillation required for frictional damping of large-amplitude occillations by a factor e in energy). The cor-riorresponding r.m.s. energy change is

$(\Delta E)_{\text{Nya}} = (2E_0kT)^{1/2} (\omega\tilde{\tau}/Q)^{1/2}$ (4i) These Nyyist mses must mt exceed the amplifier limits (quantum limits with $\hbar \to 2kT_{\text{n}}/\Omega$) if one is to achieve the amplifier limits in real experiments. Some numbers will be given below.

29.9.7 Prospects For Stroboscopic Measurements

One possible scheme for stroboscopic measurements of a mechanical oscillator (gravitational-wave antenna with mass $m = 10$ kg and frequency $\omega \simeq 3 \times 10^4 \text{sec}^{-1}$) is shown schematically in Fig. 2. The mass of the oscillator is physically attached to the central, movable plate of a capacitor (capacitance between outer plates = C), which plays the role of transducer. The capacitor resides in the QRS-a high-frequency LC circuit [frequency $\Omega = (LC)^{-1/2} \simeq 10^{10}\text{sec}^{-1}$], which has small losses [amplitude damping time $\tau = 2\left(RC\Omega^2\right)^{-1} \ll 0.1/\omega$] and which is driven at its resonant frequency Ω by an external generator. In practice this circuit would be a microwave cavity (26). At the measurement times $\omega t = 0, \pi, 2\pi, \ldots$ the generator is turned on for a time $\tau/2$ and then turned off, and in an additional time $\tau/2$ the excitations in the circuit die out. During the brief on-time V time Durng bling $V_{\text{s}} = (V_0/d)\,\Omega\tau x \cos\Omega t$, where V_0/d is the amplitude of the oscillating electric
field between the capacitor plates. The experimenter averages the amplitude of this signal (with alternating sign) over N measurements to determine the position x of the oscillator.

It is straightforward to analyze the noise performance of this system by standard circuit theory. Alternatively, one can invoke the general formulas of Eqs. 15 to 19 for stroboscopic measurement schemes. Assuming that the resistor's physical temperature is less than the amplifier's noise temperature $T_{\text{n}} \simeq 10$ V an n in K, the amplifier noise dominates and in Eq. 18b we must replace

$\hbar \to 2kT_n/\Omega$. Assuming that the amplifier is properly impedance-matched to the circuit, the measurement will achieve the limiting precision (Eq. 18b)

$$\Delta x \simeq \left(\frac{2kT_{\rm n}/\Omega}{m\omega}\right)^{1/2} (\beta N)^{-1/4} \tag{42}$$

Comparison of the voltage signal with Eq. 16a reveals that $K\,|g_{21}| = \left(V_0/\sqrt{2}d\right)(\Omega\tau)$; scrutiny of Fig. 2 reveals that the QRS output impedance, as seen by the amplifier, is $g_{22} = 2\tau/C$; consequently the dimensionless coupling constant of Eq. 16b is $\beta = (V_0/d)^2\, C\Omega\tau/\,(4m\omega^2)$. Combining this with the required pulse time $\tau = (\beta N\omega^2)^{-1/2}$ (Eq. 18a), we find

$$\beta N = \left[\frac{(V_0/d)^2\, CN\Omega}{4m\omega^3}\right]^{2/3} \tag{43}$$

To avoid voitage breakiown in the capacitor, its electric field amplitude should not exceed $(V_0/d) \simeq 10^6$volt/cm. Assuming other reasonable parameters $C \simeq 1$pf$, \Omega \simeq 10^{10}$sec$^{-1}, N \simeq 1000$, $T_{\rm n} \simeq 10$ K$, m \simeq 10$ kg, and $\omega \approx 3 \times 10^4$sec^{-1}, we find

$$\beta N \simeq 20 \quad \Delta x \simeq 1 \times 10^{-17}\ \text{cm}$$

Thus this system can achieve a sensitivity that is a factor $(20)^{1/4} \simeq 2.1$ below the amplitude-and-phase amplifier limit; but this is still an order of magnitude worse
than the amplitude-and-phase quantum limit $(\hbar/2m\omega)^{1/\bar{z}} \simeq 1 \times 10^{-1\hat{6}}$ cm.
Nyguist noise in the antenna (Eq. 40 with $\omega\tilde{\tau} = \pi N$) will be less than the measurement precision $\Delta x = \mathrm{i} \times 10^{-17}$ cm if the antenna is cooled to 4 K and has a quality factor $Q \simeq 4 \times 10^9$. This is comparable to the best mechanical Q that has been achieved (27) for a sapphire crystal at 4 K .

29.9.8 Prospects For Single-transducer Back-action-evading Measurements

The configuration of Fig. 2 can also be used in a single-transducer, back-actionevading measurement of X_1. In this case the circuit's amplitude damping time $2\,(RC\Omega^2)^{-1}$ becomes the averaging time τ_* of the QRS filter (previously it was the stroboscopic pulse length), and we require $\tau_* \gg 1/\omega$ (previously it was $\ll 1/\omega$). Instead of being pulsed, the generator's modulating voltage has the steady-state form $V_{\rm m} = U_0 \sin\Omega t \sin\omega t$, which produces an electric field (V_0/d) cos Ω cos at in the capacitors ($V_0 = U_0\Omega/2\omega$). That electric field, interacting with the motions $x = X_1 \cos\omega t + X_2 \sin\omega t$ of the mechanical oscillator, produces a signal voltage

$$\begin{aligned} V_{\rm s} = (V_0/d)\,(\Omega\tau_*/2)\,[&X_1 \sin\Omega t \\ &+ (2\omega\tau_*)^{-1}\, X_1 \sin\Omega t \sin 2\omega t \\ &- (2\omega\tau_*)^{-1}\, X_2 \sin\Omega t \cos 2\omega t] \end{aligned}$$

at the output of the QRS. Amplification of this signal produces information about X_1 and X_2 with relative accuracies $\Delta X_1 = \left(2\sqrt{2}\omega\tau_*\right)^{-1} \Delta X_2$.

Assuming that the resistor noise is negligible compared to amplifier noise (which it will be if the physical temperature of the resistors is somewhat less than the noise temperature $T_{\rm n} = 10$ K of the amplifier), we can compute the noise performance of this system from Eqs.

16,33 , and 34 with $\hbar \to 2kT_{\rm n}/\Omega$. The best of the clock that regulates the voltage quality factor that has been achieved (26) generator.

for a sunerconducting microwave resonator (our QRS circuit) with ne resopacitive Q in a narrow ca- $_{\rm e} = \Omega\tau_*/L \simeq 10^{\bar{7}}$, corresecond. Consequently back-action forces (Eq. 33) limit

$$\Delta X_1 \simeq \left(\frac{kT_{\rm n}/\Omega}{m\omega}\right)^{1/2} \frac{1}{\left(2\sqrt{2}\omega\tau_*\right)^{1/2}}$$
$$\simeq 2\times 10^{-18}\ \text{cm} \tag{46}$$

a factor 9 below the amplitude-and-phase amplifier limit and approximately twice the amplitude-and-phase quantum limit. (Here we use $T_{\rm n} = 10\ \text{K}, \Omega = 10^{10}\text{sec}^{-1}$; $m = 10$ kg, and $\omega = 3\times 10^4\text{sec}^{-1}$ as before.) In order that Nyquist noise in the mechanical oscillator (Eq. 40) not exceed this sensitivity, the averaging time must not exceed $\tilde{\tau} = 0.01$sec. (Here we use the same oscillator temperature and Q as before, $T = 4$ K and $Q = 4\times 10^9$.) To achieve the limit in Eq. 46 we also require a coupling constant $\beta \simeq 2\sqrt{2}\tau_*/\tilde{\tau} \simeq 0.3$ (Eq. 34). To compute β, first derive $K\,|g_{2i}| = (V_0/d)\left(\Omega\tau_*/2\sqrt{2}\right)$ from Eqs. 16a and 45 with $x \to X_1$; then evaluate the impedance seen by the amplifier in Fig. 2 at the X_1 signal frequency $\Omega = (LC)^{-1/2}, g_{22} = 2\tau_*/C$; then evaluate Eq. 16b

$$\beta = (V_0/d)^2\, C\Omega\tau_*/\left(16m\omega^2\right) \tag{47}$$

The required β of 0.3 can be achicved with the same electric field in the capacitive gap as we used before: $V_0/d = 1\times 10^6$ V/cm.

This example and that of the last section contirm that it is easier to achieve a given level of sensitivity by continuous, single-sensor, back-action evasion than by stroboscopic techniques. However, along the route toward realization of such experiments there remain a series of difficult experimental problems-not least of which is the frequency stability

On the Limiting Frequency Stabiliity of a Generator

Although current technology can achieve the frequency stability required by the above examples, it is of longer term interest to know ultimate quantum mechanical limits on the stabilities of clocks.

At present the world's most stable clocks are the superconducting cavity stabilized oscillator (SCSO) (28) and the hydrogen maser (29). Both involve selfexcited electromagnetic oscillations inside a cavity. In the SCSO the clock frequency Ω is regulated by the cavity's normal mode, and a change Δl of a typical dimension l of the cavity will produce a frequency change

$$\Delta\Omega/\Omega \simeq \Delta l/l \tag{48}$$

In the maser, if the electromagnetic quality factory $Q_{\rm e}$ of the cavity (Teflon bubble) exceeds $\frac{1}{2}\Omega\times$ (mean time hydrogen atoms spend in cavity) $\equiv \Omega_{\rm a}$, then Eq. 48 will be true. Otherwise, $\Delta\Omega/\Omega \simeq (\Delta l/l)\,(Q_{\rm e}/Q_{\rm a})$, and the limit derived below is correspondingly modified.

A quantum limit on the frequency stability of any electromagnetic oscillator satisfying Eq. 48 is derived in (30). The source of the limit is quantum fluctuations in the deformation of the cavity walls by electromagnetic stresses. Since the stresses in the electromagnetic field are equal to its energy density $\hat{H}_{\rm e}/l^3$ (with $\hat{H}_{\rm e}$ the Hamiltonian of the electromagnetic oscillator), the force on the walls is $\hat{H}_{\rm e}/l$, and this deforms the walls by $\delta l = \hat{H}_{\rm e}/lk$, where k is the mechanical spring constant of the walls. The electromagnetic field is in a thermalized coherent state with n_0 quanta, which possesses quantum fluctuations $\Delta H_{\rm e} \geq {n_0}^{1/2}\hbar\Omega$;
consequently, $\Delta l \geq n_0^{1/2}\hbar\Omega/kl$, which leads to frequency fiuctuations (Eq. 48)

$$\Delta\Omega/\Omega l \geq {n_0}^{i/2}\dot{h}\Omega l/k\tilde{l}^2$$

This eieciromagnetic back-action iimit must be contrasted with the limiting precision for measurements of Ω during an averaging time $\tilde{\tau}$: $\Delta\Omega \geq \Delta\psi/\tilde{\tau}$, where $\Delta\psi \gtrsim n_0^{-1/2}$ is the quantum uncertainty in the phase of the oscillator's coherent state

$$\Lambda\Omega/\Omega \geq n_{\hat{v}}^{-1/2}(\Omega\tilde{\tau})^{-1} \tag{50}$$

(Townes-Schaulow limit). These two limits lead to an optimal number of quanta n_0 and an ultimate quantum limit

$$\frac{\Delta\Omega}{\Omega} \gtrsim \left(\frac{\frac{1}{n}}{kl^2\tilde{\tau}}\right)^{1:2} \tag{51}$$

For a cavity with wall thickness comparable to cavity dimensions l, or for a "cavity" made by coating the outside of a dielectric crystal with superconducting material (31), the spring constant k is related to the Young's modulus E_{M} of the cavity walls by $k \simeq E_{\mathrm{M}}V/l^2$, where V is the cavity volume. Then

$$\Delta\Omega/\Omega \geq (\hbar/E_{\mathrm{M}}V\tilde{\tau})^{1/2} \tag{/}$$

In practice $E_{\mathrm{M}} \leqslant 10^{13}$ dyne $/\mathrm{cm}^2, V \simeq 1\mathrm{cm}^3$, so $\Delta\Omega/\Omega \geq 10^{-20}(\tau/1\mathrm{sec})^{-1/2}$. This limit is achievable in principle, but current technology is far from it.

References and Notes

1. D. Dohm, Quantum Theory (Prentice-Hon!, Englewood Cliffs, N.J., 1951), especially chapters 6 and 22.

2. M. O. Scully, R. Shea, J. D. McCullen, Phys.

3. A. Einstein, "Autobiographical notes" and "Reply to criticisms," in Albert Einstein: Philosopher-Scientist, P. A. Shilpp. Ed. (Banta. W. Lamb, Phys. Today 22, 23 (1969).

4. C. W. Helstrom, Quantum Detection and Estimation Theory (Academic Press, New York, 6. V. B. B

46, 165 (1978); J. A. Tyson and R. P. Giffard, 46, 165 (1978); J. A. Tyson and R. P. Giffard, R. Weiss, in Sources of Gravitational Radiation, L. Smarr, Ed. (Cambridge Univ. Press, Cambridge, 1979); D. H. Douglass an Einstein Braginsky, in General Relativity And W. Israel, Eds. (Cambridge Univ. Press, Cambridge, 1979); K. S. Thome, Rev. Mod. Phys. 52. 285

7. V. B. Braginsky and V. S. Nazarenko, Zh.
Eksp. Teor. Fiz. 57, 1421 (1969); English translation in Sov. Phys. IFTP 30,770 (1970)
8. V. B. Braginsky and Yu. I. Vorontsov, Usp. Fiz. Naus. sp. 17, 644 (1975).
9. W. G. Unruh, Phys. Rev. D 18, 1764 (1978).
10 , ihid. 10, 2888 (1079).
V. B. Braginsky, Yu. I. Vorontsov, F. Ya. Khalili, Zh. Eksp. Teor. Fiz. 73, 1340 (1977); English lili, Zh. Eksp. Teor. Fiz. 73, 1340 (1977); English
translation in Sov. Phys. JETP 46, 705 (1977). Pis'ma Zh. Eksp. Teor. Fiz. 27, 296
translate Phys, JETP (1978); English translation in Sov. Phys. JETP Lett. 27, 276 (1978).
13. K. S. Thorne, R. W. P. Drever. C. M. Caves M. Zimmermann, V. D. Sandberg, Phys. Rev.
14. Lett. 40, 667 (1978). C. Thorne, C. M. Caves, V. D. Sandberg, M
14. Zimmermann, R. W. P. Drever, in Sources of Gravitational Radiation, 1 Smarr, Ed. (Cambridge Univ. Press, Cambridge, 1979).

C. M. Caves, K. S. Thorne, R. W. P. Drever, V D. Sandberg, M. Limmermann, Kev. Mod.
16. I. N. Hollenherst, Phys. Rev. D 19, 1669
(1979)
17. L. 1. Mandelstam, Complete Collected Works
18. V. B. Braginsk
Test Bodies (Nauka, Moscow Experiments with translation published as NAS A. 1970), English tional Technical Information Service. Springfield, Va.
19. R. P. Giffard, Phys. Rev. D 14, 2478 (1976).
M. Zimmermann, V. D. Sandberg, in preparation. Ge Gevens and S. W. Hawting Ph-
21. G. W. Gibbons and S. W. Hawking, Phys. Rev. 22. D 4, 2191 (1971).
22. 1. 1. Gol diman and V. D. Krivchenkov, Problems in Quantum Mechanics (Pergamon, Lon-
23. J. P. Gordon, in Quantum Electronics and Coherent Light, P. A. Miles, Ed. (Academic Press, New York, 1964), pp. 156-169.
24. J. Weber, Rev. Mod. Phys. 31, 681 (1959).
26. V. B. Braginsky V. I. Panov V
B. Braginsky, V. I. Panov, V. G. Petnikov, (1977); English translation in Instrum. Exp. 27. Tech. (USSR) 20, 269 (1977).
Kh. S. Bagdasarov, V. B. Braginsky, V. P. Mitrofonov, V. S. Shiyan, Vestn. Mosk. Univ. Fiz.
28. S. R. Stein and J. P. Turneaure, Proc. IEEE 63,
29. 1249 (1975),
R. F. C. Vessoi, in Experimeniui Graviation, 1974), p. 111 (Academic Press, New York,
30. V. B. Braginsky and S. P. Vyatchanin, Zh Eksp. Teor. Fiz, 74, 828 (1978): English translation in Sov. Phys. JETP 47.433 (1978).
31. Kh. S. Bagdasarov, V. B. Braginsky, P. I. English translation in Sov. Tech. Phys. Lett. 3. 406 (1977).
For valuable discussions we thank C. M. Caves R. W. P. Drever, and F. Ya. Khalili. For financial support we thank: (i) at Moscow University, U.S.S.R.; (ii) at Caltech, the U.S. National Aeronautics and Space Administration (NGR National Science Foundation (AST76-80801 A02); (iii) for collaborative aspects of this work. the Cooperative Program in Physics between the U.S.S.R. Academy of Sciences under the auspices of the U.S.-U.S.S.R. Joint Commission on tract NSF-C310, Task Order 379) tract NSF-C310, Task Order 379).

29.10 Guide To Some Further Literature

The following papers are cited, not with any thought of providing a comprehensive bibliography, but rather with the aim of providing a few points of entry to an enormous literature. The traditional detective novel is loaded with clues, most of them irrelevant, distractive or downright deceptive. The few truly decisive items have no star to distinguish them. That is how the author conceals his plot. If we have distinguished no items with a star in our bibliography, it is because we do not know the plot!

29.10.1 I. Questions of Principle

Consciousness: Wigner reasons that an observation is only then an observation when it becomes part of "the consciousness of the observer" (Wignei, 1969) and points to "the impressions which the observer receives as the basic entities between which quantum mechanics postulates correlations" (Wigner, 1971). For Bohr, the central point is not "consciousness"

(Kalckar, 1967), not even an "observer," but an experimental device-grain of silver bromide, Geiger counter-capable of an "irreversible act of amplification" (Bohr, 1958, p. 88) that brings the measuring process to a "close" (Bohr, 1958, p. 73). Only then, he emphasized, is one person able to describe the result of the measurement to the other "in plain language" (Bohr, 1963, p. 3). For more on consciousness, see Fuller and Putnam (1966), Popper and Eccles (1977), Pugh (1976), and

Wheeler (1981a,c) as a few items in an enormous literature. Moreover, "consciousness" may not be the unique faculty that thinkers of the past assumed, feature as it is of the brain. Thus, the eye, the "window of the mind" has evolved independently in at least forty different places and times, according to Salvini-Plawen and Mayi (1978). In addition. the very mechanism of that evolution, beautiful as it is, would appear (see, for example, Cooper, 1973, Nass and Cooper, 1975, and Cooper, 1975) a natural spelling out of the principles of computers and automata sketched out in a preliminary way by von Neumann (1958).

Is meaning-a term appropriate for a community-more relevant than the individual consciousness for understanding where the "individual quatum phenomenon" links up with human perception? Is this why it is so important that the result of a quantum phenomenon, being "closed by irreversible amplification" (Bohr, 1958, p. 73), is "unambiguously communicable" from one to another in "plain language"? (Bohr, 1963, pp. 5, 6, and 3). If so, a direct link would seem to be established with a central theme of American and British philosophical investigations in recent decades, work most briefly summarized in the phrase of Fllesdal (1975), "Meaning is the joint product of all the evidence that is available to those who communicate." It reflects the spread of views on a topic so elusive as this to recall the words of David Hume (1779): "What peculiar privilege has this little agitation of the brain that we call inoughi that we must make it a model for the entire universe?"

Bohr's phenomenon and philosophers' phenomenalism are to be distinguished. Phenomenon is an individual quantum process brought to a close by an irreversible act of amplification. Phenomenalism is "the view that the existence of a physical object is dependent upon its being perceived by some percipient, that a physical object is nothing but a construct made up of the percepts that are the immediate objects of perception. It follows directly from this that the physical world is completely dependent on some perceiver(s) for its existence and that if all perceivers were annihilated, the physical world would accordingly cease to exist" (Halverson, 1967). This view of physics has ancient antecedents. Parmenides of Elea argued that "what is ... is identical with the thought that recognizes it" (Parmenides, $\sim$ 550 b.c.). Bishop George Berkeley advocated the position "Esse est percipere aut percipi," "to be is to perceive or to be perceived." (Berkeley in Calkins, ed., 1929).

E. E. Thomas (1921), analyzing R. H. Lotze's philosophical system of teleological idealism (1874-1879), distinguishes it from Berkeley's and similar ideas with these words: "Many indeed have maintained that we create the world of being-that out of our minds, or out of some universal mind in whom we exist and have our being, we introduce into sense the individualising element and so exercise a creative activity in relation to the things which we perceive around us. Lotze tells us, however,

that we do no such thing, but that the sense qualities themselves are the creators of their own individuality; that indeed sense qualities are the constitutive elements in a continuously creative activity, and that the individual whole which lives in and through such activity is what we understand by a real thing... that a 'real thing is nothing but the realised individual law of its procedure.'" Husserl (1913) provides a still more widcly read and widcly influential account of phenomenology.

Ernst Mach, patron saint of positivism, and inspiration in Einstein's carly thinking about relativity, special and general, opposes any "dualism of feeling and motion" as arising "from an improper formulation of the questions involved." He goes on, "I maintaiin that every physical

concent is nothing but a certain definite connexion of the sensory elements which I denote by $ABC\ldots$, and ihat every physical fact rests therefore on such a connexion. These elements-elements in the sense that no further resolution has as yet been made of them-are the simplest building stones of the physical world that we have yet been able to reach" (Mach, 1897).

For an up-to-date account of the many steps by which the eye processes entering photons into visual perception, reference may be made to Hubel and Wiesel (1977) and Hubel (1978).

How concepts are formed from sensory experience has been elucidated in part by the famous and extensive studies of learning in children by Jean Piaget and his school, summarized by Richmond (1971). How decisive the difference is between Berkeley's "tree that falls in the forest"-a many quantum pro-cess-and the individual quantum phenomenon is stressed in Wheeler (1981a,c). He notes that in the tran sition from individual quantum effects to classical concepts, "Many a chance 'yes, no' gives rise to the substantiality 'how much."'
Popper (1982a.b; 1983) argues for an almost classical interpretation of Heisenberg's indeterminacy relations; he hopes for a "way in which the interference of the subject with the object may be visualized as something of no fundamental importance-a consequence of the prevailing laws of interaction, and therefore in no way capable of explaining these laws, or their indeterminist character" (1982b, p. 191).

The vasiness of the literaiure on "reality" is very inadequately indicated by the foregoing sampling; and as to the great scope of that literature, it may be enough to give one iny tasie by citing the article of Heath (1972) on "nothing."

From these links between quantum theory and epistemology, we turn in the following five sections of this bibliography to issues that lie more clearly in the traditional purview of physics. For surveys of quantum theory additional to those cited in the Preface, the following, among others, may be mentioned: d'Abro (1939, 1951), DeWitt and Graham (1971), Dirac (1971), Eisenbud (1971), Feyerabend (1962), Flato (1976), Gamow (1966), Heisenberg (1930), Hermann (1979), Hoffmann (1959), Hund (1974), Jammer (1966), Jauch (1973), Klein (1959, 1970), Kramers (1956), Land (1955, 1960. 1965), Mehra (1974), Pais (1979), Piron (1976), Price and Chissick (1976). Puli-
gandla (1966), Ruark and Urey (1930), Whittaker (1953), Yourgrau and van der Merwe (1971), and Bohr's Collected Works (Rosenfeld and Nielsen, 1972-1976); Nielsen, 1977).

29.10.2 II. Interpretations of the Act of Measurement

As early as 1909, G. I. Taylor showed that one obtains interference fringes even with feeble light; and other experiments with similar findings have been reported by Dempster and Batho(1927), Janossy and Naray (1957), Frisch (1965), Donstov and Baz' (1967), and Reynolds, Spartalian, and Scarl (1969)

An irreversible act of amplification is an essential feature of the elementary quantum phenomenon as conceived by Bohr; but not one mention of that term occurs in the formulation of the act of measurement as presented by von Ncumann (1932), London and Bauer (1939; printed here in translation as II.1), and Wigner (1976). This difference in outlook is far from having been resolved today, central though it is. Many issues have been and continue to be explored in the attempt to clarify the situation. One of them is irreversibility, on which we cite, for example, Davydov (1947), the discussions by Frisch, von Weizcker, Bohm, Aharonov and Petersen, Prosperi, and others in Bastin (1971) and Belinfante (1975).

Consider amplification as we know it from Bohr's discussion, as an "irreversible process" that brings the elementary quantum phenomenon to a close, and redundancy as that term is understood in information theory
(Pierce, 1961): What do they have in common? Can we construct a macroscopic redundant record of a certain observable by making sufficiently many microscopic copies of the same

observable? Several papers pursue this line of investigation (Green, 1958; Bell, 1975; Machida and Namiki, 1980a,b; Araki. 1980; Zurek, 1982a,b). In particular, Whitten-Wolf and Emch (1976), updating Hepp (1972) and Emch (1972), propose a model of an amplification device (two infinite non-interacting chains of $\frac{1}{2}$-spin), which, though rather idealized and unrealistic, nevertheless provides, they propose, an exactly solvable model in which one can see both the "reduction of the wavepacket" and the transfer of information from a microscopic to a macroscopic ievel.

Relativity of quantum observables is ignored in the usual treatments of the process of measurement. There obserabies are assumed to be absoiute. A preferred direction- z-axis-in the measurement of the spin is assumed to be "God-given." Zurek (1981, 1982a,b) points out that in fact physical obserables are always defined in a relative manner, with respect to other physical systems. This observation alone may be significant for reconciling distinct and definite outcomes of measurements as perceived by the individual observer with the indefinite superpositions of outcomes which follow from Schrödinger evolution of the combined ap-paratus-system wave function. In particular he shows that only the "open" apparatus interacting with the environment will "know" what observable of the measured system it is supposed to record. The very interaction which will
define the preferred "pointer observable" of the apparatus will also remove spurious correlation elements from the apparatus-system density matrix, thus accomplishing von Neumann's "second stage of the measurement," reduction of the wavepacket. In the absence of the environment, on Zurek's view, the observable measured by the quantum apparatus will be uncertain, but the outcome of the measurement may appear definite (Zurck, 1982a,b). This at first sight preposterous statement may be illustrated by an EPR-correlated pair of spin- $\frac{1}{2}$ particles, with their wave function given by
$|\sigma\rangle = \{|\uparrow\rangle_1 \otimes |\downarrow\rangle_2 - |\downarrow\rangle_1 \otimes |\uparrow\rangle_2\}/2^{1/2}$.
Zurek notes that "Nothing can keep one from thinking of the first spin as of the measured system and of the second spin as of a quantum apparatus. After the first stage of measurement, which has resulted in file wave function $|\sigma\rangle$, the state of the spin-system with respect to the spin-apparatus is quite definite: The (no. 1) spin-system always points in the direction which is opposite to the orientation of the (no. 2) spinapparatus. This is a definite, 'coordi-nate-independent' statement. Thus, from the point of view of the spinapparatus, the measurement has already yielded a definite result. However, from the point of view of an external observer the measurement has not been completed: the state of the spin remains indefinite with respect to the state of the coordinate system in which this observer describes physics."

The non-linear Schrödinger equation foreshadowed in Wigner's lecture notes (1976, printed here as section II.2)
appears in a concrete form in Wigner able of the measured system is recorded (in Meystre and Scuily, 1983). This is in many separate copies at the expentse different from the non-linear wave of the information about complemenequation proposed by Bialynicki-Birula tary observables.
and Mycielski (1976), and discussed by The relative state or "many-worlds" Shimony (1979), an upper iimit to the approach to measurement described critical parameter in which has been by Everett (1957; reprinted here as set by the observations of Shull, II.3) and independently put forward by Atwood, Arthur, and Horne (1980). Cooper and Van Vechten (1969) and Irreversible increase of entropy and other early papers on this line of the problem of measurement in quan- thought are brought together in the tum physics are intimately connected, book of Dewitt and Graham (1973); as pointed out by von Neumann (1929, and Cooper (1976) has written a further 1932): Irreversible evolution could get paper. This outlook, originaily defended rid of spurious correlations represented by off-diagonal elements in the apparatus-system density matrix. Assuming that irreversible evolutions are possible, one can accomplish reduction of the wavepacket. This conclusion stimulated many to seek the resolution of the measurement

problem by invoking irreversibility and the second law of thermodynamics, among them Green (1958); Daneri, Loinger, and Prosperi (1962); Prigogine, George, Henin, and Rosenfeld (1973); and Penrose (1981). The unitary and reversible evolution given and demanded by quantum theory cannot, however, dissipate any information. This circumstance leads to the fundamental difficulty discussed by Zeh (1971) among others. However, it may be possible to transfer the information rather than dissipate it (Davies, 1974, p. 168; Zeh, 1971; Zurek, 1982a). Then the forgetting of the off-diagonal correlation terms would not be due to the irreversible decay of information, but rather due to its transfer. This scenario ties in with the process of amplification, where the information about the chosen observby Wheeler (1957) has subsequently been judged wanting by him (1977), Bell (1971b), Zeh (1975), and Wigner (1976, printed here as 11.2).

Interpretation basis is the term used by Deutsch (1981) to describe a preferred basis system in which the splitting of the universes in Everett's manyworld interpretation takes place. His work aims to solve the problem of the non-uniqueness of the relative states as defined by Everett and exemplified by the many options open (Zurek, 1981) for the polarizations of the two photons produced in the annihilation of positronium. On the view of Deutsch, "At the instant of completion of a measurement, the interpretation basis is determined by the requirement that a measurement has indeed taken place"; and he provides a system of equations designed actually to calculate this interpretation basis.

Does Gödel's undecidability have any nection with quantum indeterminism? items of literature bearing on sue will be found in Section V, In connection with the theme of "law without law" (Wheeler, 1979-1981, reprinted here as I.13), special reference should be made to the philosophical arguments already put forward for indeterminacy before the advent of quantum theory by Fritz Exner, described in recent papers of Forman (1971) and Hanle (1979). No guide would seem more valuable in the further exploration of the thesis of "law without law" than the weil-known motto, "More is different" (P. W. Anderson, 1972). Charles S. Peirce (1897) asks, "May these forces of nature not be somehow amenabie to reason? May they not have naturally grown up?" In contrast, James Clerk Maxwell (in Campbell and Garnett, 1969) argues that "No theory of evolution can be formed to account for this similarity of molecules, for evolution necessarily implies continual change, and the molecule is incapable of growth, or decay, or generation, or destruction."

"Quantum logic" is a term occasionally used for one of the several mathematically equivalent ways available to state the content of quantum theory. It differs as much from wave mechanics in the mathematical machinery that it uses for this purpose, as wave mechanics differs from matrix mechanics or both from Dirac's abstract operator algebra. Its focus of attention is propositions, such as the proposition that the spin of this silver atom points in the $+z$ direction. The totality of all conceivable propositions forms a "lattice." There are subsets of this lattice which are "Boolean"; and if classical theory is applied, the lattice as a whole would be Boolean. In quantum theory one asks questions such as (1) Given a certain proposition, tell what Boolean sub-lattices of the total lattice are compatible with that proposition, (2) Derive the existence of the Hilbert space of quantum theory from the structure of the lattice of propositions; and conversely, derive the structure of the lattice of propositions from quantum mechanics in its Hilbert space formulation. There was a time when a few thought that "quantum logic" meant a new kind of logic. That mistaken illusion being by now demolished, one translates the phrase "quantum logic" today as the logic of the relations between each proposition and all the others. Thus, if the proposition is true that the spin of the silver atom is in the $+z$ direction, then the proposition is false that the spin of the silver atom is in the $-z$ direction; and the proposition that the spin of the silver atom is in the $+x$ direction is neither true nor false-from which one goes on to discuss probabilities. Jammer (1974) gives, in chapter VIII of his book, an extensive account of the history and litcrature of the subject,

from the pathbreaking paper of Birkhoff and von Neumann (1936) to the extended development in such books as Mackey (1963, pp. 61-85), Jauch (1968, chapters 5 and 8), Ludwig (1970), Hooker (1975), Mittelstaedt (1978, 1979), and Suppes (1976). It is a fortunate circumstance for the history and further development of this subject that the hitherto unpublished lecture notes of von Neumann have recently been edited and published in book form (von Neumann, 1981). Related to this outlook is a theorem of Gleason (1957) which simplified the axiomatics of quantum mechanics. In a separable real or complex

Hilbert space H of more than two dimensions, every measure $\mu(A)$ on the subspaces of H has the form $\mu(A) = \text{trace } (TP_A)$, where P_A denotes the orthogonal projection on the subspace A and T is a fixed operator of trace class.

When is a "measurement of nothing" a measuremeni? This question, considered by Epstein (1945) and Renninger (1960), has been illuminated by a recent paper of Dicke (1982).

It may give a final impression of the scope of the topic of "Interpretations of the Act of Measurement" to list a sampling of other items: a book of Audi (1973) on the interpretation of quantum mechanics, a review by Ballentine (1970) on the statistical interpretation of quantum mechanics, a book of Whyte (1974) on the "universe of experience," a paper of DeWitt (1970) on "quantum mechanics and reality," a discussion by Aharonov and Vardi (1980) on the meaning of an individual Feynman history, and papers of Aharonov and Albert (1980, 1981) on measurement in relativistic quantum mechanics.

Other general references include Bohm (1953), Ludwig (1953), Körner and Pryce (1957), d'Espagnat (1971a,b), Belinfante (1978), de Broglie (1941, 1953, 1962), Feynman (1951), Furry (1936), Moyal (1949), and Wigner (1961, 1963).

III. "Hidden Variables" versus "Phenomenon" and Complementarity

Bell's inequality (1966; III. 4 in this book) was extended by Clauser, Horne, Shimony, and Holt (1969) to cover actual systems (see also Fehrs and Shimony, 1974, and Shimony, 1974), providing an experimental test for all "local hidden-variable theories"; it has been shown also to apply to "objective local theories " (Clauser and Horne, 1974) and to "realistic local theories" (Clauser and Shimony, 1978). The latter paper contains an extensive review of the subject of Bell's inequality and hidden variables.

The polarizations of the two annihilation photons given out when positronium disappears have a correlation in angle that can be measured as suggested by Wheeler (1946; III. 1 here) and that has been calculated by Pryce and Ward (1947) and by Snyder, Pasternack, and Hornbostel (1948).

Maximum and minimum rates of coincidence between counters detecting annihilation quanta were measured for perpendicular and parallel orientations of the two polarizations by Bleuler and Bradt (1948), Hanna (1948), Vlasov and Dzeljepov (1949), Wu and Shakhov (1950), Hereford (1951), and by Bertolino, Beltoni, and Lazarini (1955). All of these investigators found qualitative agreement with the predictions of quantum theory, though less than perfect angular resolution made quantitative comparisons difficult.

The correlation in polarization of annihilation photons was measured anew by Langhoff (1960) with improved angular resolution, using both ^{22}Na and ^{64}Cu as radioactive sources of the positrons to be slowed down and annihilated in the sample. The dependence of coincidence rate upon angle between the two polarizations agreed well with quantum theory.

Still more precise measurements of coincidence rate in its dependence on angle between the two polarizations

(Kasday, Ullman, and Wu, 1970; Kasday, 1971; Kasday, Ullman, and Wu, 1975; Bruno, d'gostino, and Maconi, 1977; Mesenheimer, 1979), supplemented by reasonable additional symmetry assumptions, appear to indicate disagreement with Bell's inequality, agreement with quantum theory; they also to rule out the Bohm-Aharonov theory (1957, 1960) in which the state vector is assumed to change at random into one of the members of an ensemble of product

states.

Agreement with Bell's inequality and therefore disagreement with quantum theory was reported in measurements of the correlation of the polarizations of annihilation quanta by Faraci, Gutkowski, Nottarigo, and Penisi (1974). Morcover, their measurements made on annihilation photons, some of which had a coherence length of 7 cm , others 47 cm , suggest that there is a decrease of correlation with increase in the difference between the flight paths of the two photons.

Disagreement with the results of Faraci et al., agreement with the predictions of quantum theory, was found by Wilson, Lowe, and Butt (1976). They used a ^{64}Cu source and were able to vary the separation between photon source and polarizers by as much as 2.5 m , and the difference in separation by as much as 1 m , as compared to a 12 cm coherence length for the annihilation photons. They found no dependence of polarization correlation upon either separation.

Correlation of spins in low-energy (p, p) scattering has been observed by Lamehi-Rachti and Mittig (1976). Departures from Rutherford scattering
arise at low energies almost exclusively from the interaction of protons in a state of zero orbital angular momentum. That state is symmetric in proton coordinates. In order to satisfy the Pauli exclusion principle, it must be antisymmetric in proton spins; that is, it must possess total spin zero. Such a state gives rise to a maximal anticorrelation of the spin directions of the two particles. The measurements, as discussed by the observers and by Pipkin (1978), indicate that the hypothesis of agreement with quantum theory, disagreement with the Bell inequality, has only 7 chances in 10^4 to be wrong. The experiment was not unambiguous because the efficiency of the analyzers of polarization was low.

Correlaion of ine polarization of the photons emitted in a 2 -photon atomic cascade was investigated-to discriminate between quantum theory and Bell's inequality-by Kocher and Commins, 1967; Freedman and Clauser, 1972; Holt, 1973 (still unpublished; the only such experiment to disagree with quantum theory); Freedman and Holt, 1975; Clauser, 1976; Fry and Thompson, 1976 (III. 8 in this book); and Aspect, Grangier, and Roger (1981). An extensive review has been given by Pipkin (1978). In the experiment of Aspect, Grangier, and Roger, the relevant quantity δ,
is found to be $(5.72 \pm 0.43) \times 10^{-2}$, confirmed predictions of quantum violating by more than 13 standard deviations the condition $\delta \leq 0$ required by Freedman's transcription of the Bell inequality, but agreeing with the prediction of quantum theory, $\delta = (5.8 \pm 0.2) \times 10^{-2}$. Moreover, these investigators report, "moving each polarizer up to 6.5 m from the source, that is, to four coherence lengths of the wave packet associated with the lifetime of the intermediate state of the cascade (5 ns), we observed no change in the results." These experiments provide the clearest evidence to date for that violation of the Bell inequality that is predicted by quantum theory.

A "pilot-wave theory" or "theory of the double solution," proposed by de Broglic (1928), can be regarded as a first attempt to cast quantum theory in a deterministic mold, and thus achieve the goal of the modern-day "hidden variable" theories. According to de Broglie, the usual wave function ψ is to play a twofold role: apart from being a "probability wave" it is also to represent and determine the trajectory of the particle as a singular solution of the wave equation. Pauli (1928a) objected to de Broglie's ideas. He showed in a specific example that the motion of the singularity-particle will take place in a many-dimensional, and hence fictitious, configuration space.

Exploration of any hidden-variable approach to quantum theory was abandoned for many years after von Neumann (1932) published his muchdiscussed proof, later reformulated by Jauch and Piron (1963), that hidden variables of a rather restricted class directly contradict the experimentally

confirm theory.
Theories of hidien variabies were resuscitated by Bohm (1952a,b), first to point out that von Neumann's theorem did not have the generality commonly attributed to it. Bell (1966) identified the specific assumption of von Neumann that was not satisfied by so-called "realistic hidden variable theories."

The history and status of theories of hidden variables are reviewed by Belinfante (1973), Jammer (1974), and Pipkin (1978). Apart from the papers of Bohm and Bell included in the present collection there is a wide-ranging literature, not all of it free from speculation, on hidden variables. A few points of entily are provided by the papers of Bohm and Aharonov, 1957, 1960; Bub. 1969; Bohm and Bub, 1966a,b; Bohm and Vigier, 1954; Vigier, 1951, 1956; and Ridijk, 1971.
An inequality, an upper bound on the strength of correlations of polarization which can be allowed by a deterministic and local theory of hidden variables, was derived by Bell (1964) in the course of reexamining the arguments of Einstein, Podolsky, and Rosen (1935). Extensions of Bell's inequality have been given by Bell, 1971a; Clauser and Horne, 1974; McGuire and Fry, 1973; and Garuci and Selleri, 1976.

The so-called "non-locality" of quantum theory as it shows in the Einstein-Podolsky-Rosen and other experiments is discussed in some detail by d'Espagnat, 1976, part 3, and 1979; Bohm and Hiley, 1975, 1976; and Hiley, 1977; and in other papers too numerous to cite. Several interesting papers
of John S. Bell consider the bearing of so-called "non-locality" on what shall be understood by the term "reality." Bell (1976) is "particularly concerned with local "beables," those which (unlike, for example, the total energy) can be assigned to some bounded spacetime region." He formulates one concept of "local causality," and shows that "ordinary relativistic quantum field theory is not locally causal in this sense." Rell (1980a), on "BertImann's socks and the nature of reality," presents the EPR experiment in a particularly vivid form, and outiines four aiternative ways to come to terms with its implications for "reality." In particular he discusses the idea that the settings of the polarization analyzers (in Bohm's version of the EPR experiment) might not be independent in the sense assumed by apparently free-willed experimental physicists, and adds, "But this way of arranging quantum mechanical correlations would be even more mindboggling than one in which causal chains go faster than light. Apparently separate parts of the world would bc deeply and conspiratorially entangled, and our apparent free will would be entangled with them." Bell (1980b) defends the de Broglie-Bohm version of quantum theory "as sharp where the usual one is fuzzy, and general where the usual one is special" and illustrates this view by analyzing the delayedchoice double-slit experiment. Henry P. Stapp (1972, 1981) advocates a "psychophysical theory" in which "the physical world described by the laws of physics is a structure of tendencies in the world of mind."
"Delayed choice experiments" were
prefigured by Einstein, Tolman, and Podolsky (1931, reprinted here as 1.7), as well as by Bollr's solitary and pregnant sentence (1949, p. 230), "... it . can make no difference, as regards observable effects obtainable by a definite experimental arrangement, whether our plans for constructing or handling the instruments are fixed beforehand or whether we prefer to postpone the completion of our planning until a later moment when the particle is already on its way from one instrument to another." They were foreshadowed in an analysis of the uncertainty principle, as it shows up in the operation of an electron microscope, done by eighteen-year-old Karl Friedrich von Weizscker (1931) at the instance of Heisenberg. On page 128 of this paper appears this sentence (in our translation), "Physically one would reason in this case [atom not in the image plane but at the focal distance] that a photonn absorbed at the focal distance must, already before it went through the lens, have become equivalent to a plane wave whose direction of propagation can be calculated from the position of the absorbing atom." The general

concept of delayed-choice experiments was formulated, and seven types of such experiments were spelled out, in Wheeler (1978). Scully and Drhl (1982) "propose and analyze an experiment designed to probe the extent to which information accessible to an observerand the 'eraser' of this informationaffect measured results." They point out that their new experiment, too, lets itself be operated in the delayed-choice mode.

Would a world be conceivable in
which there is no quantum indeterminism? Peres and Zurek (1982) investigate conceivable alternatives and conclude that "Theories where the observed world is deterministic but the observer is not (whatever the reason for that) lead to Bell's nonseparability theorem. If, on the other hand, the observer too is deterministic, the theory is not verifiable. It follows that quantum theory must be the logically preferred option. Its inability to completely describe the measurement process is not a flaw of the theory but a logical necessity and is analogous to Gödel's undecidability theorem."

"Stochastic quantum mechanics" is a name often given to the view that (1) the Schrödinger equation is essentially diffusion equation, though an equation for the diffusion of probability amplitude rather than probability density itself; and (2) that this diffusion is driven by a force arising from other dynamical entities, that is, from a special class of hidden variables: random impacts of particles postulated ad hoc, fluctuating fields, electromagnetic or otherwise, etc.

This outlook was first introduced by Frth (1933) and is expounded at length in Fnyes (1952). In their work quantum mechanics is described as a "timesymmetric stochastic process," with little said about the origin of the random external force. In contrast, Kalitsin(1953), inspired by Einstein and Hopf (1910) and by Einstein and Stern (1913), likewise takes the mechanics of the electron to be classical at bottom, but views the fluctuating force on it that makes it behave "quantum mechanically" as originating from the fluctuat-
ing electromagnetic field of the vacuum. Well though this treatment reproduces the ground state of the harmonic oscillator, it fails for other systems. (i) It predicts that the electron of the hydrogen atom, originally in its ground state, will gain energy from the vacuum fluctuations. (2) When system breaks into two parts, as in the Einstein-Podolsky-Rosen experiment, the fluctuations at the location of the one system and the other would have to have a quite artificial correlation to reproduce the well-tested predictions of standard quantum mechanics. Boyer (1980b) surveys "stochastic electrodynamics."

A bibliography of over 200 papers on "stochastic quantum mechanics" has been prepared by Robert Hobart of Middle Georgia College, Cochran, Georgia. We are most indebted to him for making it available to us. Space iimitations have made it impossible for us to include more than an arbitrary but representative sampling of the literature: Bergia, Lugli, and Zamboni, 1980; Boyer, 1968, 1974, 1975, 1980a,b; Claverie and Diner, 1977; Comisar, 1965; Davidson, 1979; De La Pea, 1969, 1977; Einstein and Hopf, 1910; Einstein and Stern, 1913; Fnyes, 1952; Frth, 1933; Kalitsin, 1953; Kracklauer, 1974; Marshall, 1965; Nelson, 1966; Santos, 1979; Vigier, 1979. The subject of each paper is sufficiently indicated in most cases by its title as listed in the bibliography at the end of this book.

29.10.3 IV. Field Measurements

The paper of Landau and Peierls (1931, reprinted here as IV.1) stimulated Bohr
and Rosenfeld (1933, reprinted here as analyzing implications of the Maxwell IV.2; and 1950, reprinted here as IV.3) demon. Szilard's pathbreaking paper to do a thoroughgoing analysis of the (1929, here V.1) has led to an extensive measurability of electromagnetic field quantities. Stages in the evolution of in the evolution of scribe deCor by Rosenfeld (1955, 1967).

Corinaldesi (1951), pursuing a line of development opened up by Heisenberg twenty years earlier, analyzes charge fluctuations in quantum electrodynamics.

Byce DeWitt (1962, 1965) extends to the dynamics of geometry considerations on measurability analogous to those worked out by Bohr and Rosenfeld for the electromagnetic field. Salecker and Wigner (1958) show that there is one way of measuring geometry by use of light rays and test particles which fails far short of the accuracy expected from the considerations of DeWitt. Bohr and Rosenfeld had initially encountered a similar difficulty when they were trying to find an apparatus that would measure with the accuracy allowed by theory. In the end, however, they found that it was more reasonable to improve the apparatus than to question the theory.

29.10.4 VI. Irreversibility and Quantum Theory

Maxwell's demon "was conceived in discussions among Maxwell, Tate, and Thomson; he was first described in a letter from Maxwell to Tate in 1867, and publicly introduced in Maxwell's Theory of Heat (1871)," according to Brush (1966), who also reprints papers of Thomson (1874) and Poincar (1893) literature, one of the more significant treatises in which is Brillouin (1962).

An attempt to define thermodynamic entropy in terms of information content has been made by Jaynes (1957a,b, 1979). Whether his work can serve as a foundation for statistical mechanics remains a subject of controversy (Friedman and Shimony, 1971; Dias and Shimony, 1981). Szilard's paper has been criticized by Jauch and Baron (1972) for suggesting that the connection between entropy and information is straightforward. They have also criticized Szilard's discussion of the "one-particle-gas" model on physical grounds.

John von Neumann's 1932 formulation of the quantum theory of measurement has been critically discussed by Feyerabend (1957), Margenau (1963), Sneed (1966), and Furry (1966) as both too idealized and too restrictive.

Ergodicity was a central topic of classical mechanics from early days. It was the subject of a paper by twenty-two-year-old Enrico Fermi (1901-1954; Fermi, 1923). It is the focus of numerous treatises: Hopf (1937), Khinchin (1957), Jacobs (1962-1963), Billingsley (1965), Rohlin (1967), Arnold and Avez (1968), Moser (1973), Ornstein (1974), Sinai (1976), and Cornfeld, Fomin, and Sinai (1981). It took time to see how to extend these considerations to the new framework of quantum theory. Einstein (1917b) discussed the rule of Bohr and Sommerfeld for quantization in the case when the Hamilton-Jacobi equation is not separable, and showed
that if tori exist in phase space, it is von Neumann (1929), Pauli and Fierz possible to define action and angle (1937), Krylov (1979), and van Hove variables. Percival (1973) reviews the literature of classical mechanics which shows that "bound systems which have an analytic Hamiltonian, and which are sufficiently close to being separable, have a significant fraction of their phase space full of trajectories which behave very much like those of separable systems." Associated with such "regular" regions of phase space, Percival shows hy semiclassical methods, is a quantum energy spectrum with "regular" properties; but he shows that there is another part of the spectrum, an "irregular part," with strongly contrasting properties. McDonald and Kaufmann (1979) and Casati, Valz-Gris, and Guarnieri (1980) present numerical work on irregular spectra. Korsch and Berry (1981) use the Wigner phase-space density function to analyze what happens in the course of time to a distribution initially confined to a wellcircumscribed region of phase space. In the beginning it spreads out much as expected from classical mechanics. Classically, however, the distribution, for the case of a non-integrable Hamiltonian, develops an intricate structure of whorls and tendrils. Other workers had already pointed out that these tendrils can no longer evolve according to classical expectations when their dimensions grow so small as not even to include a single quantum cell in phase space. Korsch and Berry illustrate this result by numerical computations.

General ergodic properties of quantum systems, discussed by van Hove (1959, reprinted here as V.3) have also been investigated by, among others,

(1955, 1957). For a penetrating discussion of these prove additional refe

The relationship between "quantum ergodicity" and so-called "collapse of the wavepacket" proposed by Daneri, Loinger, and Prosperi (1962, reprinted here as V.4; also 1966 and Prosperi, 1967) has been endorsed by Rosenfeld (1965, 1968b), criticized by Jauch, Wigner, and Yanase (1967) and Bub (1968), and defended by Loinger (1968). Additional considerations on ergodicity fluctuations and entropy as they relate to quantum theory will be found in Pauli (1928b); Kemble (1939a,b); Vonsovsky (1946); Stueckelberg (1952); Groenewold (1952); Kiein (1952, 1956); Van Kampen (1954, 1958); Fierz (1955); Jancel (1955); Gamba (1955); Farinelli and Gamba (1956); Farquhar and Landsberg (1957); Ludwig (1958a,b); Prosperi and Scotti (1959, 1960); Wannier (1965).

Further discussion of time reversal (Aharonov, Bergmann, and Lebowitz, 1964, reprinted here as V.5) and its relevance to the quantum theory of measurement can be found in Belinfante (1975). See also Rankin (1965).

The Lyapounov superoperator formalism mentioned by Misra, Prigogine, and Courbage (1979a, reprinted here as V.6) has been described in much greater detail by Prigogine, George, Henin, and Rosenfeld (1973), and by Misra, Prigogine, and Courbage (1979b) and applied to problems of the quantum theory of measurement by George, Prigogine, and Rosenfeld (1972).

The relation between irreversibility,
amplification and "reduction of the wavepacket" has been a subject of many papers. For example, Green (1958) has stressed metastability of the initial state of the measuring apparatus. In his model the detector consists of two sets of oscillators kept at different temperatures, coupled by a quantum system, the wave function of which is to be "collapsed." A critical assessment of Green's paper has been given by Furry (1966). Hepp (1972) has argued that the generation of probabilities from probability amplitudes can take place if the apparatus is an infinite system. Though Hepp thus concludes that in a certain mathematical limit "rigorous reduction of the wavepacket" can be obtained, Bell (1975) has shown that at least in one of the models investigated by Hepp, such reduction does not take place. The non-reduction of the wavepacket becomes particularly apparent in the Heisenberg picture. Haake and Weidlich (1968) have argued that the reduction of the wavepacket can be achieved if the apparatus possesses "channel structure." They have investigated in detail a particular model, one where the "apparatus" is a field mode. More on this topic will be found in Weidlich (1967) and Weidlich and Haake (1969). Machida and Namiki (1980a,b) stress that any reasonable model of a macroscopic apparatus must subsume a large number of distinct Hilbert spaces. Their reasoning has been given a detailed mathematical development by Araki (1980) in terms of continuous superselection rules. Zurek (1981, 1982b) has argued that it is the
coupling between the Hilbert space of the apparatus pointer and the rest of the apparatus which is responsible for the effective superselection rules. According to this reasoning, the pointer of the apparatus cannot be regarded as an isolated system.

The thermodynamics of black holes (Bekenstein, 1973, 1974, 1975: Hawking. 1974, 1975) has suggested to some that irreversibility and noncausality may be inherent in the laws of nature (Hawking, 1976). Penrose (1973) proposes that such a finding might allow one to understand evolution from pure states to mixtures and, consequently, the process of measurement itself, in a completely new way.

For a long time it was thought that one could make a simple-minded appilcation of the considerations of Szilard in the theory of computers, and that each stage in the computation would require the dissipation of an energy of the order of magnitude of kT. By 1961, however, this doctrine was no longer beyond question (Landauer, 1961); and twelve years later, Bennett (1973) in an epoch-making paper, proved that a computation can, in principle, be operated as close to reversibility as desired. In the words of Landauer, the process is not "lossless, but only as reversible as automobiles or locomotives which can back up along their path. We also assume

that the frictional forces are proportional to velocity and thus, the accompanying energy losses, per logic step, can be made as small as desired, by sufficiently slow computation." Landauer (1981a) comments on
the implications of Szilard's work: "It taught us that measurement requires energy expenditure. But it does not seem to be adequately recognized that coupling a meter to an object to be measured, and letting the object thus influence the meter, does not require dissipation. The dissipation arises from the need to reset the meter after subsequent decoupling, in order to prepare the meter for further use. Again it is the destruction of information which is associated with the real need for energy dissipation. This relationship to information destruction has been emphasized only in our own field of computation, and not equally in the related analyses of the measurement process and of channel capacity requirements."

Distinguishability is the first requirement for measurement. Measurements in general, and measurements at the quantum level in particular, deal with information, often information of the "yes, no" type rather than the "how much" type. How much information of the "yes, no" type does one need to distinguish two nearby values of the angle of polarization of a beam of photons? And how should the probability of a yes or no count depend upon the angle of polarization to give-if nature were in the mood to give-the maximum number of distinguishable directions of polarization? Just the way nature says it does, according to contributions of Wootters (1980, 1981), who also goes on to show that "distance in Hilbert space measures distinguishability." This result raises the still un-
answered question whether all of quantum theory can be derived out of appropriate information-theoretic considerations.

That probability amplitudes are complex numbers, not reals or quaternions, has been connected by Stueckelberg (1960) with the principle of complementarity or indeterminism; and some of the extensive subsequent discussion of these issues is summarized in Jammer (1974, pp. 358-359).

This question about the ties between quantum theory and information theory leads to interest in two other intellectual partners of information theory, memory theory and undecidability theory. Out of the vast literature on memory theory, it may be appropriate to cite as representative contributions Ovenden and Roy (1973) and Pearl and Crolotte (1980). As regards undecidability, Chaitin (1975, 1981) notes that "Gödel's theorem (**1931**; see also Nagel and Newman, 1958; and Hofstadter, 1979) may be demonstrated using arguments having an information-theoretic flavor. In such an approach it is possible to argue that if a theorem contains more information than a given set of axioms, then it is impossible for the theorem to be derived from the axioms. In contrast with the traditional proof based on the paradox of the liar, this new viewpoint suggests that the incompleteness phenomenon discovered by Gödel is natural and widespread rather than pathological and unusual."

Even further from any immediately obvious tie to quantum theory, but also an incentive to think about the deeper
meaning of quantum theory, is the by Aharonov and Bohm (1961, VI.4), Austrian theory of capital (von Hayek, 1948, 1975; von Mises, 1966) as discussed in this connection by Tipler (1981). Tipler considers Friedrich von Hayek's definition of capital (an extension of that originally given by Eugen von Böhm-Bawerk) as analogous to the Feynman sum over histories, but more complex in depending in general on all the other histories.

29.10.5 Vi.accuracy of Measurements: Quantum Limitations

To measure the direction of the spin of a free electron is impossible, as Niels Bohr explained, Mott and Massey (1965, VII.) demonstrate, and Pauli (1932) illustrates by numerous examples; but for a bound electron the direction of the spin can be measured. Experiments of the Stern-

Gerlach type measure, for example, the direction of the spin of the valence electron of a neutral silver atom. More recently, the direction of the spin has been measured for an otherwise free electron trapped in a manmade mixture of electric and magnetic fields (Van Dyck, Ekstrom, and Dehmelt, 1976; Dehmelt, 1981; Van Dyck, Schwinberg, and Dehmelt, 1981).

Uncertainties of quantum origin arise in the typical Stern-Gerlach experiment when the measuring apparatus has a finite size, as elucidated in an extensive literature summarized by Wigner (1976, II.2), Araki and Yanase (1960, VI.2), and Yanase (1961, VI.3).

The principle of indeterminism as applied to time and energy, analyzed
has been discussed in additional contexts by Ailicock (1969a, b, c), who also gives extensive citations of the literature (1969a). Wigner (1972) works out the wave function that minimizes the product of the uncertainties in time and in energy.

All kinds of observing devices and amplifiers are affected by Brownian motion, as spelled out in a charming review article by Barncs and Silverman (1934). See Wax, ed. (1954) for a collection of papers on the theory of Brownian motion. A brief and elementary review of the subject of amplifiers will be found in Halkias and Alley (1977). A more advanced discussion can be found in Caves (1982b).

More on the uncertainty principle as it affects the operation of the ideal amplifier, the subject of two contributions reprinted here (Heffiner, 1962, VI.5, and Haus and Mullen, 1962, VI.6), will be found in the book of Pierce and Posner (1980, pp. 285-292), the book edited by Townes (1960), and in articles of Helstrom (1976) and Serber and Townes (1960).

The capacity of a communication channel (Shannon and Weaver, 1949; Pierce, 1981a) is analyzed as it depends on quantum limitations in the paper of Pierce (1978, VI.7) reprinted here.

A computer has some similarity in principle to an information channel. The process of computation, far from requiring a minimum energy of the order of kT per logic step, is in principle a reversible process, a fascinating conclusion proved by Bennett (1973, 1982).

On the basis of this result, Pierce (1981b), in an unpublished letter, draws up the following assessment:
(1) "Need it take energy to compute? Not in the following sense: A reversible finite state machine can act as a computer. In principle it can go from the initial condition to the final condition and back again without any net loss of energy.
(2) "What about (1) and information theory? As (i) is stated, nothing. If we know the data, program and machine, in principle we know the 'answer'. There is no uncertainty and hence there is no information involved in the operation of the reversible computer.
(3) "What about getting output from the computer of (1)? If we don't know the state of the computer output device, which is a part of the reversible finitestate computer, we can find the state of this output device only through an expenditure of kT joules per nat.
(4) "What about inputting to the reversible computer? If we know the state, this costs us nothing. See (5) below.
(5) "What about 'writing on a tape'? Ideally, if we know the initial state of the tape, this costs us nothing. Think of the tape as a lot of frictionlessly hinged bars that can lie left or right on a flat surface. If we know that a bar lies left. in principle we can raise it to vertical and lower it to right without loss of energy.*

- "But we might need a different specialpurpose machine for each initial and/or output state."
  (6) "If we don't know the state, what will writing cost? If we know nothing at all about the state it will cost kT joules per nat to find the state and nothing to write thereafter.*
  (7) "What about 'duplicating a tape'? It costs nothing if we know the states of both tapes. If we don't know anything about the state of one tape it costs kT joules per nat to find it.*

(8) "What about writing into our idealized computer? Ideally, it costs nothing if we know the state. If we don't know the state we can learn the state before we can write in for nothing at a cost of kT joules per nat. How much is this in total? That depends both on the complexity of the computer and on how litite or how much we do know about its state."

Landauer (1981a,b) notes that "the energies required by channel capacity considerations represent energy dissipation only if the message is destroyed at the receiving end and a computer need not do that. Consider, for example, a high density reel of storage tape sent physically through space, at high velocity... [constituting] transmission of information [with a] required dissipation [of] at most a few kT." Further discussion will be found in Louisell (1964).

How much mass-energy does it take to dispose of a bit of information? How much is the minimum mass increment experienced by a black hole in the process? This question is considered in the framework of quantum theory by Bekenstein (1981) and-with non-identical conclusions-by Unruh and Wald (1982) and by Deutsch (1982).

One acquires information with high effectiveness, without violating the uncertainty principle that connects frequency and time, by use of "chirp radar," a scheme of great consequence for hats and men (Griffin, 1950, 1958; Klauder, Price, Darlington, and Albersheim, 1960; Farnett et al., 1970; Casasent, 1978; Leith, 1978). See also Cutrona (1970) and Jensen et al. (1977) for radar in a broader context.

To count individual atoms is to approach one quantum limit to the measuring process. This feat has been accomplished by Hurst, Payne, Kramer. and Young (1979) and their Oak Ridge colleagues, surely with great consequences for the future of detecting and measuring devices of many kinds.

The idea of quantum nondemolition measurements, also pregnant with incalculable consequences for the future of measuring devices, reviewed here in Braginsky, Vorontsov, and Thone (1980, VI.8), is also the subject of a rapidly increasing and instructive literature (Braginsky and Manukin, 1977; Caves, Thoine, Drevei, Sandberg, and Zimmermann, 1980; Braginsky and Viatchanin, 1981; and Caves, 1982).

A superfluid helium interferometer is proposed by Chiao (1982) as a detector of the Lense-Thirring effect and of gravitational radiation.

Part XI
Appendix

A Introduction

A.1 Literature

A.1.1 Main Literature

Основная литература

Нельсон Чанг Квантовые вычисления и квантовая информация
Большая подробная книга, которую буду периодически смотреть, а когда минимальный уровень будет, может, отдельные месяцы и буду изучать.

Teiko Heinosaari, Mário Ziman, The Mathematical Language of Quantum Theory
тоже говорят, что хорошая книга.

А. Китаев, А.Шень, М. Вялый К53 Классические и квантовые вычисления. - М.: МЦНМО, ЧеРо, 1999. - 192 с. ISBN 5-900916-35-9
Выглядит как прекрасное введение в предмет, с нее скорее всего и начну, не такая большая и многое там написано!

Books With Many Solved Problems

Вводная, обзорная

https://www.youtube.com/watch?v=xjlGL4Mvq7A&ab_channel=Qiskit
Милое, обзорное видео для обзора истории.

Основная методическая

Лекции и презентации Филиппова https://mipt.ru/science/labs/QIT-lab/for-students.php
Отличный материала для начала, лучше - не знаю.

Холево А.С. Квантовые системы, каналы, информация. М.: МЦНМО, 2010.
Филиппов рекомемндует, значит, она тоже хорошая. Скорее всего после минимального уровня выгружу ее всю! гуглится. https://www.mccme.ru/free-books/holevo-quantum.pdf

Основная профессиональная

А. С. Холево, Квантовая вероятность и квантовая статистика, Итоги науки и техн. Сер. Соврем. пробл. мат. Фундам. направления, 1991, том 83, 5–132
130 страниц очень содержательной теории, скорее всего по этой книге многие и учатся. В 1ю часть добавил, мне показалось, что книга очень очень содержательная.

A.1.2 Extra Literature

Дополнительная методическая

Нильсен М., Чанг И. Квантовые вычисления и квантовая информация. М.: Мир, 2009.
3. Холево А.С. Математические основы квантовой информатики. М.: МИАН, 2018.
Филиппов рекомендует.

4. Белоусов Ю.М., Манько В.И. Матрица плотности. Представления и применения в статистической механике. Ч. 1. М.: МФТИ, 2004; Ч. 2. М.: МФТИ, 2005.
Филиппов рекомендует.

5. Стиб В.-Х., Харди Й. Задачи и их решения в квантовых вычислениях и квантовой теории информации. М., Ижевск: НИЦ «Регулярная и хаотическая динамика», 2007.
Филиппов рекомендует.

6. Бройер Х.-П., Петруччионе Ф. Теория открытых квантовых систем. М., Ижевск: НИЦ «Регулярная и хаотическая динамика», 2010.
Филиппов рекомендует.

7. Кашурников В.А., Красавин А.В. Численные методы квантовой статистики. М.: Физматлит, 2010.
Филиппов рекомендует.

Статьи о разных явлениях

[1] Aharonov, Yakir and Albert, David Z. and Vaidman, Lev
Оказывается, можно измерить спин частицы раный 100, если он на самом деле равен 1/2. удивительно, мб за 2 дня это бы я и понял, но не до этого. Потом впишу в теорию.

Дополнительная по теории

[2] Aharonov, Yakir. and Rohrlich, Daniel Quantum paradoxes quantum theory for the perplexed
Книга от профессионалов, во многом поулярная вроде. В открытом доступе нет, в библиотеку нужно идти. Вроде много очень интересных тем обсуждается, по идее многое можно очень фундаментального понять по ней.

В помощь

Статьи о теоретических методах

О приложениях

A.2 Puzzles for Different Cases

Обсудим в порядке интересности задачки и вопросы

A.2.1 Puzzles in Everyday life

Каковы фундаментальные принципы квантовых вычислений и квантовой информации?

(см. нельсон чанг)

Как фундаментальные принципы квантовых вычислений развивались?

(см. нельсон чанг)

Где фундаментальные принципы квантовых вычислений можно применить?

(см. нельсон чанг)

A.2.2 General Fundamental Topics to Discuss

(??? see articles about them for now)

B Mathematics, Physics, Programming

(потом укажу, где что нужно. заготовки по Нильсону Чангу)

B.0.1 Linear Algebra

Частичное транспонирование

$$X : \mathcal{H}^{AB} \to \mathcal{H}^{AB}, \quad X^{\Gamma} \equiv X^{\top_B} \equiv \sum_{i,j=1}^{d_B} I \otimes |j\rangle\langle i| \cdot X \cdot I \otimes |j\rangle\langle i|$$

$$X : \mathcal{H}^{AB} \to \mathcal{H}^{AB}, \quad X^{\urcorner} \equiv X^{\top} A \equiv \sum_{i,j=1}^{d_A} |j\rangle\langle i| \otimes I \cdot X \cdot |j\rangle\langle i| \otimes I$$

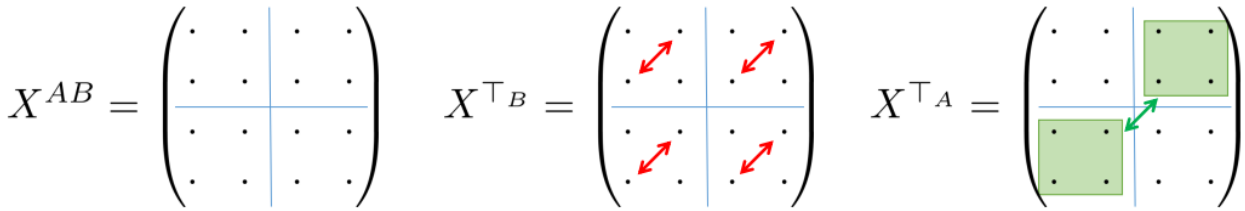


Figure B.1: Частичное транспонирование

(??? примеры в случае больших размерностей???)

Некоторые свойства следов

$\mathrm{tr}\left[X^A\right] = \sum\limits_k \left\langle k^A \middle| X^A \middle| k^A \right\rangle$ - это число

$\mathrm{tr}\left[X^B\right] = \sum\limits_j \left\langle j^B \middle| X^B \middle| j^B \right\rangle$ - это число

$\mathrm{tr}\left[X^{AB}\right] = \sum\limits_{k,j} \left\langle k^A \middle| \otimes \left\langle j^B \middle| \cdot X^{AB} \cdot \middle| k^A \right\rangle \otimes \middle| j^B \right\rangle$ - это число

(пример бы потом про это написать ниже...)

$\mathrm{tr}_B\left[X^{AB}\right] = \sum\limits_j I^A \otimes \left\langle j^B \middle| \cdot X^{AB} \cdot I^A \otimes \middle| j^B \right\rangle$ - оператор, действующий в H^A.

(пример бы потом про это написать ниже...)

$\mathrm{tr}_A\left[X^{AB}\right] = \sum\limits_k \left\langle k^A \middle| \otimes I^B \cdot X^{AB} \cdot \middle| k^A \right\rangle \otimes I^B$ - оператор, действующий в H^A.

(?? примеры)

Под ним можно переставлять местами операторы (?)
Сумму можно выносить из-под следа
(тут примеры, как это используем, на самом деле достаточно часто)

B.0.2 NCh.1: Notes on basic probability theory

This appendix collects some elementary definitions and results about probability theory. It is assumed that the reader already has some familiarity with this material. The reader who is not familiar with any of the results should take time out to prove them, as indicated in the exercises.

The basic notion of probability theory is that of a random variable. A random variable X may take one of a number of values, x, with probabilities $p(X = x)$. We use upper case to denote the random variable, and x to denote the values that random variable may take. We often use the notation $p(x)$ instead of $p(X = x)$, leaving the ' $X =$ ' implicit. In this book we shall only be concerned with random variables which take their value from a finite set of values, and we always assume that this is the case. Occasionally it is convenient to consider random variables whose values are vectors taking values, for example, in the set $(i, j), i = 1, \ldots, m_1, j = 1, \ldots, m_2$.

The conditional probability that $Y = y$ given that $X = x$ is defined by

$$p(Y = y \mid X = x) \equiv \frac{p(X = x, Y = y)}{p(X = x)}, \tag{A1.1}$$

where $p(X = x, Y = y)$ is the probability that $X = x$ and $Y = y$. When $p(X = x) = 0$ we make the convention that $p(Y = y \mid X = x) = 0$. We often use the notation $p(y \mid x)$ leaving the ' $Y =$ ' and ' $X =$ ' implicit. Random variables X and Y are said to be independent if $p(X = x, Y = y) = p(X = x)p(Y = y)$ for all x and y. Note that when X and Y are independent, it follows that $p(y \mid x) = p(y)$ for all x and y.

Bayes' rule relates the conditional probabilities for Y given X to those for X given Y,

$$p(x \mid y) = p(y \mid x)\frac{p(x)}{p(y)}. \tag{A1.2}$$

The probability $p(y)$ appearing in this expression is often re-expressed using the law of total probability discussed below.

Exercise A1.1: Prove Bayes' rule.

One of the most important and frequently used results in probability theory is the law of total probability. It states that if X and Y are two random variables, then the probabilities for Y can be expressed in terms of the probabilities for X, and the conditional probabilities for Y given X,

$$p(y) = \sum_x p(y \mid x)p(x), \tag{A1.3}$$

where the sum is over all values x that X can take.

Exercise A1.2: Prove the law of total probability.

The expectation, average, or mean of a random variable X is defined by

$$\mathbf{E}(X) \equiv \sum_x p(x)x \tag{A1.4}$$

where the sum is over all values x which the random variable X can take.

Exercise A1.3: Prove that there exists a value of $x \geq \mathbf{E}(X)$ such that $p(x) > 0$.

Exercise A1.4: Prove that $\mathbf{E}(X)$ is linear in X.

Exercise A1.5: Prove that for independent random variables X and Y, $\mathbf{E}(XY) = \mathbf{E}(X)\mathbf{E}(Y)$.

The variance of a random variable X is defined by the expression

$$\mathrm{var}(X) \equiv \mathbf{E}\left[(X - \mathbf{E}(X))^2\right] = \mathbf{E}\left(X^2\right) - \mathbf{E}(X)^2. \tag{A1.5}$$

The standard deviation, $\Delta(X) \equiv \sqrt{\mathrm{var}(X)}$, is a measure of the spread of a random variable about the average. Chebyshev's inequality quantifies more precisely in what sense the standard deviation is a measure of the spread of values a random variable may take. It states that for any $\lambda > 0$ and random variable X with finite variance,

$$p(|X - \mathbf{E}(X)| \geq \lambda \Delta(X)) \leq \frac{1}{\lambda^2} \tag{A1.6}$$

Thus, the probability of being more than λ standard deviations away from the mean gets small as λ goes to infinity.

Exercise A1.6: Prove Chebyshev's inequality.

The main text of the book contains many other results in probability theory, including the Chernoff bound on page 154, Fano's inequality on page 536, and the law of large numbers on page 541.

History and further reading

Probability theory enjoys a surfeit of superb texts. We especially recommend the text of Grimmett and Stirzaker [GS92] as an excellent introduction to many basic ideas in the theory of probability and stochastic processes. From a more purely mathematical point of view, Williams [Wi191] is a superb introduction to the modern theory of probability, with an emphasis on the beautiful theory of martingales. Finally, the classic two-volume text of Feller [Fel68a, Fel68b] is an excellent indepth introduction to the ideas of probability theory.

B.0.3 NCh.2: Group theory

The mathematical theory of groups is useful at several points in the study of quantum computation and quantum information. The generalization of the order-finding, factoring, and period finding algorithms in Chapter 5 is based on the hidden subgroup problem; the stabilizer formalism for quantum error-correction in Chapter 10 is based on some elementary group theory. The number theory described in Appendix 4 uses the properties of the group $\mathbf{Z}_n^*$. And, implicitly, the quantum circuits used throughout the book are an example of the use of Lie groups. In this appendix we review some basic material on group theory. We summarize many of the fundamental concepts and provide important definitions, but do not attempt to explain very much, as group theory is a vast subject!

A2.1 Basic definitions

A group $(G, \cdot)$ is a non-empty set G with a binary group multiplication operation '$\cdot$', with the following properties: (closure) $g_1 \cdot g_2 \in G$ for all $g_1, g_2 \in G$; (associativity) $(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$, for all $g_1, g_2, g_3 \in G$; (identity) there exists $e \in G$ such that $\forall g \in G, g \cdot e = e \cdot g = g$; (inverses) for all $g \in G$, there exists $g^{-1} \in G$ such that $g \cdot g^{-1} = e$ and $g^{-1} \cdot g = e$. We often leave out $\cdot$ and write $g_1 \cdot g_2$ as simply $g_1 g_2$. We also often refer to the group G without referring explicitly to its multiplication operation, but it must be defined.

A group G is finite if the number of elements in G is finite. The order of a finite group G is the number of elements it contains, denoted as $|G|$. A group G is said to be Abelian if $g_1 g_2 = g_2 g_1$ for all $g_1, g_2 \in G$. A simple example of a finite Abelian group is the additive group $\mathbf{Z}_n$ of integers modulo n, with 'multiplication' operation the operation of modular addition. It is easily checked that this operation satisfies the closure and associativity axioms; there is an

identity element, 0 , since $x + 0 = x (\mathrm{mod} n)$ for all x, and every $x \in G$ has an inverse, $n - x$, since $x + (n - x) = 0 (\mathrm{mod} n)$.

The order of an element $g \in G$ is the smallest positive integer r such that g^r (g multiplied with itself r times) equals the identity element e.

A subgroup H of G is a subset of G which forms a group under the same group multiplication operation as G.

Theorem A2.1: (Lagrange's theorem) If H is a subgroup of a finite group G then $|H|$ divides $|G|$.

Exercise A2.1: Prove that for any element g of a finite group, there always exists a positive integer r such that $g^r = e$. That is, every element of such a group has an order.

Exercise A2.2: Prove Lagrange's theorem.

Exercise A2.3: Show that the order of an element $g \in G$ divides $|G|$.

If g_1 and g_2 are elements of G, then the conjugate of g_2 with respect to g_1 is the element $g_1^{-1} g_2 g_1$. If H is subgroup of G, then it is known as a normal subgroup if $g^{-1} H g = H$ for all $g \in G$. The conjugacy class G_x of an element x in a group G is defined by $G_x \equiv \{g^{-1} x g \mid g \in G\}$.

Exercise A2.4: Show that if $y \in G_x$ then $G_y = G_x$.

Exercise A2.5: Show that if x is an element of an Abelian group G then $G_x = \{x\}$.

An interesting example of a group which is not Abelian is the Pauli group on n qubits. For a single qubit, the Pauli group is defined to consist of all the Pauli matrices, with multiplicative factors $\pm 1, \pm i$ allowed by the definition:

$$G_1 \equiv \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}. \tag{A2.1}$$

This set of matrices forms a group under the operation of matrix multiplication. You might wonder why we don't omit the multiplicative factors ± 1 and $\pm i$; the reason these are included is to ensure that G_1 is closed under multiplication, and thus forms a legitimate group. The general Pauli group on n qubits is defined to consist of all n-fold tensor products of Pauli matrices, and again we allow multiplicative factors of $\pm 1, \pm i$.

A2.1.1 Generators

The study of groups is often greatly simplified by the use of a set of group generators for the group being studied. A set of elements $g_1, \ldots, g_l$ in a group G is said to generate the group G if every element of G can be written as a product of (possibly repeated) elements from the list $g_1, \ldots, g_l$, and we write $G = \langle g_1, \ldots, g_l \rangle$. For example, $G_1 = \langle X, Z, iI \rangle$, since every element in G can be written as a product of X, Z and iI. On the other hand, $\langle X \rangle = \{I, X\}$, a subgroup of G_1, since not every element of G_1 can be written as a power of X. The notation $\langle \cdots \rangle$ which we use for group generators may potentially be confused with the notation for observable averages introduced in Section 2.2.5 (page 87); however, in practice it is always clear from context how the notation is being used.

The great advantage of using generators to describe groups is that they provide a compact means of describing the group. Suppose G has size $|G|$. Then it is pretty easy to show that there is a set of $\log(|G|)$ generators generating G. To see this, suppose $g_1, \ldots, g_l$ is a set of elements in a group G, and g is not an element of $\langle g_1, \ldots, g_l \rangle$. Let $f \in \langle g_1, \ldots, g_l \rangle$. Then $fg \notin \langle g_1, \ldots, g_l \rangle$, since if it were then we would have $g = f^{-1} fg \in \langle g_1, \ldots, g_l \rangle$, which we know is false by assumption. Thus for each element $f \in \langle g_1, \ldots, g_l \rangle$ there is an element fg which is in $\langle g_1, \ldots, g_l, g \rangle$ but not in $\langle g_1, \ldots, g_l \rangle$. Thus adding the generator g to $\langle g_1, \ldots, g_l \rangle$ doubles (or more) the size of the group being generated, from which we conclude that G must have a set of generators containing at most $\log(|G|)$ elements.

A2.1.2 Cyclic groups

A cyclic group G possesses an element a such that any element $g \in G$ can be expressed as a^n for some integer n. a is known as a generator of G, and we write $G = \langle a \rangle$. A cyclic subgroup H generated by $g \in G$ is the group formed by $\{e, g, g^2, \ldots, g^{r-1}\}$, where r is the order of g. That is, $H = \langle g \rangle$.

Exercise A2.6: Show that any group of prime order is cyclic.
Exercise A2.7: Show that every subgroup of a cyclic group is cyclic.
Exercise A2.8: Show that if $g \in G$ has finite order r, then $g^m = g^n$ if and only if $m = n (\mathrm{mod}\, r)$.

A2.1.3 Cosets

For H a subgroup of G, the left coset of H in G determined by $g \in G$ is the set $gH \equiv \{gh \mid h \in H\}$. The right coset is defined similarly. Often whether a coset is a 'left' or 'right' coset is implied by context. In the case of a group like $\mathbf{Z}_n$ where the group operation is addition it is conventional to write cosets of a subgroup H in the form $g + H$, for $g \in \mathbf{Z}_n$. Elements of a particular coset gH are known as coset representatives of that coset.

Exercise A2.9: Cosets define an equivalence relation between elements. Show that $g_1, g_2 \in G$ are in the same coset of H in G if and only if there exists some $h \in H$ such that $g_2 = g_1 h$.

Exercise A2.10: How many cosets of H are there in G ?

A2.2 Representations

Let M_n be the set of $n \times n$ complex matrices. A matrix group is a set of matrices in M_n which satisfy the properties of a group under matrix multiplication. We shall denote the identity element in such groups as I. A representation ρ of a group G may be defined as a function which maps G to a matrix group, preserving group multiplication. Specifically, $g \in G$ is mapped to $\rho(g) \in M_n$, such that $g_1 g_2 = g_3$ implies $\rho(g_1)\,\rho(g_2) = \rho(g_3)$. If the map is many to one, it is known as a homomorphism; if it is one to one, then the map is an isomorphism. A representation ρ which maps into M_n has dimension $d_\rho = n$. The representations we have defined are also referred to as being matrix representations; there are more general ones, but these are sufficient for our purposes. For the remainder of this appendix all the groups G which we deal with should be taken to be finite groups.

A2.2.1 Equivalence and reducibility

Two important concepts about representations are equivalence and reducibility. The character of a matrix group $G \subset M_n$ is a function on the group defined by $\chi(g) = \mathrm{tr}(g)$, for $g \in G$, where $\mathrm{tr}(\cdot)$ is the usual trace function on matrices. It has the following properties: (1) $\chi(I) = n$, (2) $|\chi(g)| \leq n$, (3) $|\chi(g)| = n$ implies $g = e^{i\theta} I$, (4) χ is constant on any given conjugacy class of G, (5) $\chi(g^{-1}) = \chi^*(g)$, and (6) $\chi(g)$ is an algebraic number for all g. Two matrix groups are said to be equivalent if they are isomorphic, and corresponding elements under the isomorphism have the same character.

Exercise A2.11: (Characters) Prove the properties of characters given above.
Exercise A2.12: (Unitary matrix groups) A unitary matrix group is comprised solely of unitary matrices (those which satisfy $U^\dagger U = I$). Show that every matrix group is equivalent to a unitary matrix group. If a representation of a group
consists entirely of unitary matrices, we may refer to it as being a unitary representation.

A matrix group G in M_n is said to be completely reducible if it is equivalent to another matrix group H which is of block diagonal form, that is all elements $m \in H$ are of the form $\mathrm{diag}\,(m_1, m_2)$, for some $m_1 \in M_{n_1}$ and $m_2 \in M_{n_2}$. If no such equivalence exists, then the matrix group is irreducible. The following is a useful property of irreducible matrix groups:

Lemma A2.2: (Schur's lemma) Let $G \subset M_n$ and $H \subset M_k$ be two matrix groups of the same order, $|G| = |H|$. If there exists a k by n matrix S such that $Sg_i = h_i S$ for some ordering of all elements $g_i \in G$ and $h_i \in H$, then either S is the zero matrix, or $n = k$ and S is a square nonsingular matrix.

Exercise A2.13: Show that every irreducible Abelian matrix group is one dimensional.
Exercise A2.14: Prove that if ρ is an irreducible representation of G, then $|G|/d_\rho$ is an integer.

The following theorem connects irreducibility with characters:
Theorem A2.3: A matrix group G is irreducible if and only if

$$\frac{1}{|G|}\sum_{g\in G}|\chi(g)|^2 = 1 \tag{A2.2}$$

A2.2.2 Orthogonality

The key theorem of representation theory is the following:

Theorem A2.4: (Fundamental theorem) Every group G has exactly r inequivalent irreducible representations, where r is the number of conjugacy classes of G. And if $\rho^p \in M_{d_\rho}$ and ρ^q are any two of these, then the matrix elements satisfy the orthogonality relations

$$\sum_{g\in G}\left[\rho^p(g)\right]^{-1}_{ij}\left[\rho^q(g)\right]_{kl} = \frac{|G|}{d_\rho}\delta_{il}\delta_{jk}\delta_{pq} \tag{A2.3}$$

where $\delta_{pq} = 1$ if $\rho^p = \rho^q$ and is zero otherwise.

Exercise A2.15: Using the Fundamental Theorem, prove that characters are orthogonal, that is:

$$\sum_{i=1}^{r} r_i \left(\chi_i^p\right)^* \chi_i^q = |G|\delta_{pq} \quad \text{and} \quad \sum_{p=1}^{r}\left(\chi_i^p\right)^*\chi_j^p = \frac{|G|}{r_i}\delta_{ij}, \tag{A2.4}$$

where p, q, and δ_{pq} have the same meaning as in the theorem, and χ_i^p is the value the character of the p th irreducible representation takes on the i th conjugacy class of G, and r_i is the size of the i th conjugacy class.

Exercise A2.16: S_3 is the group of permutations of three elements. Suppose we order these as mapping 123 to: $123; 231; 312; 213; 132$, and 321 , respectively. Show that
there exist two one-dimensional irreducible representations of S_3, one of which is trivial, and the other of which is $1, 1, 1, -1, -1, -1$, corresponding in order to the six permutations given earlier. Also show that there exists a two-dimensional irreducible representation, with the matrices

$$\begin{array}{lll} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, & \frac{1}{2}\begin{bmatrix} -1 & -\sqrt{3} \\ \sqrt{3} & -1 \end{bmatrix}, & \frac{1}{2}\begin{bmatrix} -1 & \sqrt{3} \\ -\sqrt{3} & -1 \end{bmatrix}, \\ \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, & \frac{1}{2}\begin{bmatrix} 1 & \sqrt{3} \\ \sqrt{3} & -1 \end{bmatrix}, & \frac{1}{2}\begin{bmatrix} 1 & -\sqrt{3} \\ -\sqrt{3} & -1 \end{bmatrix}. \end{array} \tag{A2.5}$$

Verify that the representations are orthogonal.

A2.2.3 The regular representation

The number 1 is a valid one-dimensional matrix representation of any group. However, it is trivial. A representation is faithful if the matrix group of the representation is isomorphic to the original group. The regular representation is a faithful representation which exists for any group, and is constructed in the following manner. Let $\vec{v} = \left[g_1, g_2, \ldots, g_{|G|}\right]^T$ be a column vector of elements from G. Multiplying each element of $\vec{v}$ by an element $g \in G$ permutes the

entries of the vector; this permutation can be represented by a $|G| \times |G|$ matrix acting by matrix multiplication on $\vec{v}$. The $|G|$ such matrices corresponding to the possible different permutations form a faithful representation of G, under matrix multiplication.

Exercise A2.17: Prove that the regular representation is faithful.

Exercise A2.18: Show that the character of the regular representation is zero except on the representation of the identity element, for which $\chi(I) = |G|$.

The decomposition of arbitrary representations into tensor sums of irreducible representations obeys the following theorem:

Theorem A2.5: If ρ is an arbitrary representation of G with character χ, and ρ^p are the inequivalent irreducible representations of G with characters χ^p, then $\rho = \oplus_p c_p \rho^p$, where $\oplus$ denotes a direct sum, and c_p are the numbers determined by

$$c_p = \frac{1}{|G|} \sum_{i=1}^{r} r_i \left(\chi_i^p\right)^* \chi_i. \tag{A2.6}$$

Exercise A2.19: Use Theorem A2.5 to show that the regular representation contains d_{ρ^p} instances of each irreducible representation ρ^p. Thus, if R denotes the regular representation, and $\hat{G}$ denotes the set of all inequivalent irreducible representations, then

$$\chi_i^R = \sum_{\rho \in \hat{G}} d_\rho \chi_i^\rho. \tag{A2.7}$$

Exercise A2.20: The character of the regular representation is zero except for the conjugacy class i containing e, the identity element in G. Show, therefore, that

$$\sum_{\rho \in \hat{G}} d_\rho \chi^\rho(g) = N \delta_{ge} \tag{A2.8}$$

Exercise A2.21: Show that $\sum_{\rho \in \hat{G}} d_\rho^2 = |G|$.

A2.3 Fourier transforms

Let G be a finite group of order N, and f be a function which maps group elements to complex numbers. For an irreducible representation ρ of G, of dimension d_ρ, we define the Fourier transform of f to be $\hat{f}$,

$$\hat{f}(\rho) \equiv \sqrt{\frac{d_\rho}{N}} \sum_{g \in G} f(g) \rho(g) \tag{A2.9}$$

Note that for ρ a matrix representation, $\hat{f}(\rho)$ maps matrices to matrices. Let $\hat{G}$ be a complete set of inequivalent irreducible representations of G. We define the inverse Fourier transform of $\hat{f}$ to be

$$f(g) = \frac{1}{\sqrt{N}} \sum_{\rho \in \hat{G}} \sqrt{d_\rho} \operatorname{tr}\left(\hat{f}(\rho) \rho\left(g^{-1}\right)\right) \tag{A2.10}$$

Because $\sum_\rho d_\rho^2 = N$, f and $\hat{f}$ can both be expressed as vectors of complex numbers of length N. Note that the coefficients in the above equations have been chosen such that if $\hat{G}$ consists of unitary representations, then the Fourier transformations are unitary.

The above definitions can be understood by substituting (A2.9) into (A2.10) to obtain

$$f(g) = \frac{1}{N} \sum_{\rho \in \hat{G}} \sum_{g' \in G} d_\rho f\left(g'\right) \operatorname{tr}\left(\rho\left(g'\right) \rho\left(g^{-1}\right)\right) \tag{A2.11}$$

$$= \frac{1}{N} \sum_{\rho \in \hat{G}} \sum_{g' \in G} d_\rho f\left(g'\right) \operatorname{tr}\left(\rho\left(g' g^{-1}\right)\right) \tag{A2.12}$$

$$= \frac{1}{N} \sum_{g' \in G} f\left(g'\right) \sum_{\rho \in \hat{G}} d_\rho \chi^\rho\left(g' g^{-1}\right). \tag{A2.13}$$

Using (A2.8), we may simplify (A2.13) to

$$f(g) = \sum_{g' \in G} f\left(g'\right) \delta_{g' g} \tag{A2.14}$$

as desired.

Exercise A2.22: Substitute (A2.10) into (A2.9) and prove that $\hat{f}(\rho)$ is obtained.

Exercise A2.23: Let us represent an Abelian group G by $g \in [0, N-1]$, with addition as the group operation, and define $\rho_h(g) = \exp[-2\pi i g h/N]$ as the h representation of g. This representation is one-dimensional, so $d_\rho = 1$. Show that the Fourier transform relations for G are

$$\hat{f}(h) = \frac{1}{\sqrt{N}} \sum_{g=0}^{N-1} f(g) e^{-2\pi i g h/N} \quad \text{and} \quad f(h) = \frac{1}{\sqrt{N}} \sum_{g=0}^{N-1} \hat{f}(g) e^{2\pi i h g/N} \tag{A2.15}$$

Exercise A2.24: Using the results of Exercise A2.16, construct the Fourier transform over S_3 and express it as a 6×6 unitary matrix.

History and further reading

There are many outstanding texts on group theory, and virtually any book on algebra has a section devoted to the theory of groups. The discussion here borrowed much notation from the text on finite groups by Lomont [Lom87] . Hammermesh is a standard reference for group theory in physics [Ham89]. Discussions of Fourier transforms over groups are not so common. Diaconis and Rockmore have written a good article on the efficient computation of Fourier transforms over groups [DR90]; many of their results are also reviewed in Fässler and Stiefel [FS92]. Beth independently discovered the fast Fourier transform over groups[Bet84], as did Clausen[Cla89].

B.0.4 NCh.3: The Solovay-Kitaev theorem

In Chapter 4 we showed that an arbitrary unitary operation U may be implemented on a quantum computer using a circuit consisting of single qubit and controlled-NOT gates. Such universality results are important because they ensure the equivalence of apparently different models of quantum computation. For example, the universality results ensure that a quantum computer programmer may design quantum circuits containing gates which have four input and output qubits, confident that such gates can be simulated by a constant number of controlled-NOT and single qubit unitary gates.

An unsatisfactory aspect of the universality of controlled-NOT and single qubit unitary gates is that the single qubit gates form a continuum, while the methods for fault-tolerant quantum computation described in Chapter 10 work only for a discrete set of gates. Fortunately, also in Chapter 4 we saw that any single qubit gate may be approximated to arbitrary accuracy using a finite set of gates, such as the controlled-not gate, Hadamard gate H, phase gate S, and $\pi/8$

gate. We also gave a heuristic argument that approximating the chosen single qubit gate to an accuracy ϵ required only $\Theta(1/\epsilon)$ gates chosen from the finite set. Furthermore, in Chapter 10 we showed that the controlled-not, Hadamard, phase and $\pi/8$ gates may be implemented in a fault-tolerant manner.

In this appendix we show that a much faster rate of convergence than $\Theta(1/\epsilon)$ may be achieved. The Solovay-Kitaev theorem shows that for any gate U on a single qubit, and given any $\epsilon > 0$, it is possible to approximate U to a precision ϵ using $\Theta\left(\log^c(1/\epsilon)\right)$ gates from a fixed finite set, where c is a small constant approximately equal to 2 . The best possible value for c isn't known yet, so we are going to explain the proof of the Solovay-Kitaev theorem for c approximately equal to 4 , and then in the end of appendix problems outline a method that may be used to reduce c down closer to 2 . We will also prove that c cannot be less than 1 ; determining the best possible value of c between 1 and 2 is an open problem!

To appreciate the importance of the Solovay-Kitaev theorem, imagine a quantum computer programmer designs an algorithm using $f(n)$ gates to solve a problem. Suppose the algorithm he or she comes up with uses many gates outside the usual fault-tolerant set of controlled-not, Hadamard, phase and $\pi/8$ gates. How many gates are required to implement the algorithm fault-tolerantly? If the tolerance to error for the entire algorithm is to be ϵ, then the individual gates must be accurate to a tolerance $\epsilon/f(n)$. By the heuristic argument of Chapter 4 it would take $\Theta(f(n)/\epsilon)$ gates in the fault-tolerant set to approximate each one of the gates used in the algorithm, for a total cost $\Theta\left(f(n)^2/\epsilon\right)$, a polynomial increase in the number of gates required by the algorithm. Using the SolovayKitaev theorem each gate in the algorithm can be simulated by $O\left(\log^c(f(n)/\epsilon)\right)$ gates in the fault-tolerant set, for a total cost $O\left(f(n)\log^c(f(n)/\epsilon)\right)$ for the fault-tolerant algorithm, which is only polylogarithmically more than for the original algorithm. For many
problems, such a polylogarithmic cost is quite acceptable, whereas the polynomial cost provided by the heuristic argument of Chapter 4 may be much less desirable.

To state the Solovay-Kitaev theorem more precisely, we need to define some notation and nomenclature. Recall that $SU(2)$ is the set of all single qubit unitary matrices with determinant equal to one. We restrict our attention to $SU(2)$, since all single qubit unitary gates may be written as the product of an element of $SU(2)$ with an unimportant global phase factor. Suppose $\mathcal{G}$ is a finite set of elements of $SU(2)$; $\mathcal{G}$ plays the role of the finite set of elementary gates our quantum computer programmer is using to simulate all the other gates. For the sake of concreteness, think of $\mathcal{G}$ as containing the fault-tolerant set H, S, and T, with appropriate global phases added to ensure the determinants are all equal to one. We suppose for the sake of convenience that $\mathcal{G}$ contains its own inverses, that is, if $U \in \mathcal{G}$, then $U^\dagger \in \mathcal{G}$. In the case of the fault-tolerant set, that means adding $S^\dagger = S^3$ and $T^\dagger = T^7$ to the set, which fortunately can be expressed in terms of gates already in the set. A word of length l from $\mathcal{G}$ is a product $g_1 g_2 \ldots g_l \in SU(2)$, where $g_i \in \mathcal{G}$ for each i. We define $\mathcal{G}_l$ to be the set of all words of length at most l, and $\langle \mathcal{G} \rangle$ to be the set of all words of finite length.

We need some notion of distance to quantify what we mean by an approximation to a unitary matrix. The exact measure used is not all that important. It is convenient for our purposes to use the trace distance studied in Chapter 9, $D(U, V) \equiv \mathrm{tr}\,|U - V|$, where $|X| \equiv \sqrt{X^\dagger X}$ is the positive square root of $X^\dagger X$. Actually, this definition differs by a factor 2 from the definition used in Chapter 9; the reason for using a different normalization is that it makes geometric visualization of the proof of the Solovay-Kitaev theorem easier, as we shall see (it will also be helpful to think of elements in $SU(2)$ as being points in space). A subset S of $SU(2)$ is said to be dense in $SU(2)$ if for any element U of $SU(2)$ and $\epsilon > 0$ there is an element $s \in S$ such that $D(s, U) < \epsilon$. Suppose S and W are subsets of $SU(2)$. Then S is said to form an ϵ-net for W, where $\epsilon > 0$, if every point in W is within a distance ϵ of some point in S. Our interest is in how fast $\mathcal{G}_l$ 'fills up' $SU(2)$ as l is increased. That is, for how small an ϵ is $\mathcal{G}_l$ an ϵ-net for $SU(2)$

? The Solovay-Kitaev theorem says that ϵ gets small very quickly indeed as l is increased.

Exercise A3.1: In Chapter 4 we made use of the distance measure $E(U,V) = \max_{|\psi\rangle} \|(U-V)|\psi\rangle\|$, where the maximum is over all pure states $|\psi\rangle$. Show that when U and V are single qubit rotations, $U = R_{\hat{m}}(\theta), V = R_{\hat{n}}(\varphi)$, $D(U,V) = 2E(U,V)$, and thus it does not matter whether we use the trace distance or the measure $E(\cdot,\cdot)$ for the Solovay-Kitaev theorem.

Theorem A3.1: (Solovay-Kitaev theorem) Let $\mathcal{G}$ be a finite set of elements in $SU(2)$ containing its own inverses, such that $\langle \mathcal{G} \rangle$ is dense in $SU(2)$. Let $\epsilon > 0$ be given. Then $\mathcal{G}_l$ is an ϵ-net in $SU(2)$ for $l = O\left(\log^c(1/\epsilon)\right)$, where $c \approx 4$.

As already noted, the best possible value of c is somewhat lower than 4 , but it is convenient to give the proof for this particular case. In Problem 3.1 we explain how modifications of the proof can be used to lower c. The first part of the proof is to show that the points of $\mathcal{G}_l$ get very dense in a small neighbourhood of the identity matrix I as l is increased, a conclusion encapsulated in the following lemma. To state the lemma, we define S_ϵ to be the set of all points U in $SU(2)$ such that $D(U,I) \leq \epsilon$.

Lemma A3.2: Let $\mathcal{G}$ be a finite set of elements in $SU(2)$ containing its own inverses, and such that $\langle \mathcal{G} \rangle$ is dense in $SU(2)$. There exists a universal constant ϵ_0 independent of $\mathcal{G}$, such that for any $\epsilon \leq \epsilon_0$, if $\mathcal{G}_l$ is an ϵ^2-net for S_ϵ, then $\mathcal{G}_{5l}$ is a $C\epsilon^3$-net for $S_{\sqrt{C}\epsilon^{3/2}}$, for some constant C.

We prove Lemma A3.2 shortly, but first let's see how it implies the Solovay-Kitaev theorem. There are two steps to the proof. The first step is to apply Lemma A3.2 iteratively to show that the neighbourhood of the origin fills in very quickly as the word length l is increased. Since $\mathcal{G}$ is dense in $SU(2)$ we can find an l_0 such that $\mathcal{G}_{l_0}$ is an ϵ_0^2-net for SU(2), and thus also for S_{ϵ_0}. Applying Lemma A3.2 with $\epsilon = \epsilon_0$ and $l = l_0$ implies that $\mathcal{G}_{5l_0}$ is a $C\epsilon_0^3$-net for $S_{\sqrt{C}\epsilon_0^{3/2}}$. Applying Lemma A3.2 again with $\epsilon = \sqrt{C}\epsilon_0^{3/2}$ and $l = 5l_0$ implies that $\mathcal{G}_{5^2 l_0}$ is a $C\left(\sqrt{C}\epsilon_0^{3/2}\right)^3$-net for $S_{\sqrt{C}\left(\sqrt{C}\epsilon_0^{3/2}\right)^{3/2}}$. Iterating this procedure k times, we find that $\mathcal{G}_{5^k l_0}$ is an $\epsilon(k)^2$-net for $S_{\epsilon(k)}$, where

$$\epsilon(k) = \frac{(C\epsilon_0)^{(3/2)^k}}{C} \tag{A3.1}$$

Without loss of generality we may suppose ϵ_0 has been chosen such that $C\epsilon_0 < 1$, and therefore $\epsilon(k)$ gets small very fast as k increases. It will also be useful to note that, provided ϵ_0 is chosen small enough, $\epsilon(k)^2 < \epsilon(k+1)$.

The second step is to let U be any element of $SU(2)$ and use the translation idea illustrated in Figure A3.1 to approximate U using products of elements of $\mathcal{G}$. Let $U_0 \in \mathcal{G}_{l_0}$ be an $\epsilon(0)^2$-approximation to U. Now define V so that $VU_0 = U$, that is, $V \equiv UU_0^\dagger$. Thus $D(V,I) = \operatorname{tr}|V-I| = \operatorname{tr}\left|(U-U_0)U_0^\dagger\right| = \operatorname{tr}|U-U_0| < \epsilon(0)^2 < \epsilon(1)$. From the iterated application of Lemma A3.2 discussed above, we can find $U_1 \in \mathcal{G}_{5l_0}$ which is an $\epsilon(1)^2$-approximation to V. It follows that U_1U_0 is an $\epsilon(1)^2$-approximation to U. Now define V' so that $V'U_1U_0 = U$, that is, $V' \equiv UU_0^\dagger U_1^\dagger$. Thus $D(V',I) = \operatorname{tr}|V-I| = \operatorname{tr}\left|(U-U_1U_0)U_0^\dagger U_1^\dagger\right| = \operatorname{tr}|U-U_1U_0| / < \epsilon(1)^2 < \epsilon(2)$. It follows from the iterated application of Lemma A3.2 that we can find $U_2 \in \mathcal{G}_{5^2 l_0}$ which is an $\epsilon(2)^2$-approximation to V', and thus $U_2U_1U_0$ is an $\epsilon(2)^2$-approximation to U. Continuing in this way we construct $U_k \in \mathcal{G}_{5^k l_0}$ so that $U_kU_{k-1}\ldots U_0$ is an $\epsilon(k)^2$-approximation to U.

Putting it all together, a sequence of $l_0 + 5l_0 + \cdots + 5^k l_0 < \frac{5}{4}5^k l_0$ gates can be used to approximate any unitary gate U to an accuracy $\epsilon(k)^2$. To approximate to some desired accuracy ϵ, we therefore must choose k such that

$$\epsilon(k)^2 < \epsilon. \tag{A3.2}$$

Substituting (A3.1) this can be restated as

$$\left(\frac{3}{2}\right)^k < \frac{\log\left(1/C^2\epsilon\right)}{2\log\left(1/C\epsilon_0\right)} \tag{A3.3}$$

It follows that the number of gates required to approximate to within ϵ satisfies ($c = \log 5/\log(3/2) \approx 4$)

$$\text{number of gates } < \frac{5}{4}5^k l_0 = \frac{5}{4}\left(\frac{3}{2}\right)^{kc} l_0 < \frac{5}{4}\left(\frac{\log\left(1/C^2\epsilon\right)}{2\log\left(1/C\epsilon_0\right)}\right)^c l_0. \tag{A3.4}$$

That is, the number of gates required to approximate to within ϵ is $O\left(\log^c(1/\epsilon)\right)$, completing the proof of the Solovay-Kitaev theorem.

The proof of Lemma A3.2 uses a few elementary facts about multiplication of elements

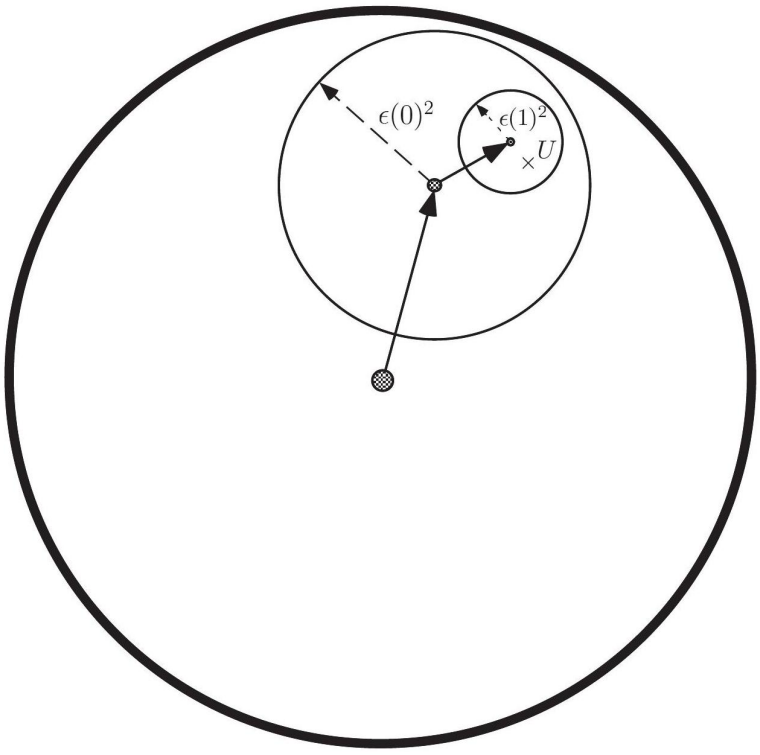


Figure A3.1. The translation step used in the proof of the Solovay-Kitaev theorem. To approximate an arbitrary single qubit gate we first approximate to within a distance $\epsilon(0)^2$ using l_0 gates from $\mathcal{G}$. Then we improve the approximation by adding $5l_0$ more gates, for a total accuracy better than $\epsilon(1)^2$, and continue on in this way, quickly converging to U.}

of $SU(2)$, which we now recall. The key idea of the lemma is to work in the neighborhood of the identity, which greatly simplifies the rather complicated operation of multiplication in $SU(2)$. More precisely, suppose U and V are elements of $SU(2)$, and define the group commutator of U and V by

$$[U, V]_{\text{gp}} \equiv UVU^\dagger V^\dagger. \tag{A3.5}$$

Suppose U and V are both close to the identity, so that they may be written $U = e^{-iA}$ and $V = e^{-iB}$, where A and B are Hermitian matrices such that $\text{tr}\,|A|, \text{tr}\,|B| \leq \epsilon$ for some small ϵ. Expanding $e^{\pm iA}$ and $e^{\pm iB}$ to terms quadratic in A and B gives

$$D\left([U,V]_{\rm gp}, e^{-[A,B]}\right) = O\left(\epsilon^3\right), \tag{A3.6}$$

where $[A,B] = AB - BA$ is the usual commutator for matrices (in fact, the commutator for the Lie algebra of $SU(2)$). Thus, in the neighborhood of the identity we can study the group commutator by studying instead the much simpler matrix commutator.

Indeed, for qubits the matrix commutator has an especially nice form. An arbitrary element of $SU(2)$ may be written $U = u(\vec{a}) \equiv \exp(-i\vec{a}\cdot\vec{\sigma}/2)$ for some real vector $\vec{a}$. Similarly $V = u(\vec{b}) = \exp\left(-i\vec{b}\cdot\vec{\sigma}/2\right)$ for some real vector $\vec{b}$. Recalling from Exercise 2.40 that

$$[\vec{a}\cdot\sigma, \vec{b}\cdot\sigma] = 2i(\vec{a}\times\vec{b})\cdot\vec{\sigma} \tag{A3.7}$$

we see from (A3.6) that

$$D\left([U,V]_{\rm gp}, u(\vec{a}\times\vec{b})\right) = O\left(\epsilon^3\right). \tag{A3.8}$$

The basic idea of the proof of Lemma A3.2 is now easy to understand. The details, most of which relate to approximation issues, are filled in below for completeness; for now we just give the main idea, as illustrated in Figure A3.2. Suppose we wish to approximate some element $U = u(\vec{x})$ in S_{ϵ^2}. You will see in Exercise A3.4 that trace distances like $D(U,I)$ are equal (up to small corrections) to the Euclidean distance $\|\vec{x}\|$, so to a good approximation $\|\vec{x}\| \leq \epsilon^2$. We can always choose $\vec{y}$ and $\vec{z}$ of length at most ϵ, such that $\vec{x} = \vec{y}\times\vec{z}$. Pick $\vec{y}_0$ and $\vec{z}_0$ such that $u(\vec{y}_0)$ and $u(\vec{z}_0)$ are elements of $\mathcal{G}_l$ that ϵ^2-approximate $u(\vec{y})$ and $u(\vec{z})$, respectively. Applying (A3.6) to the commutator $[u(\vec{y}_0), u(\vec{z}_0)]_{\rm gp}$ we get an $O(\epsilon^3)$-approximation to U. This gives a $O(\epsilon^3)$-net for S_{ϵ^2}; to finish the proof of the lemma we apply a translation step like that in the main part of the proof of the Solovay-Kitaev theorem, obtaining in $5l$ gates an $O(\epsilon^3)$-approximation to any element of $S_{O\left(\epsilon^{3/2}\right)}$.

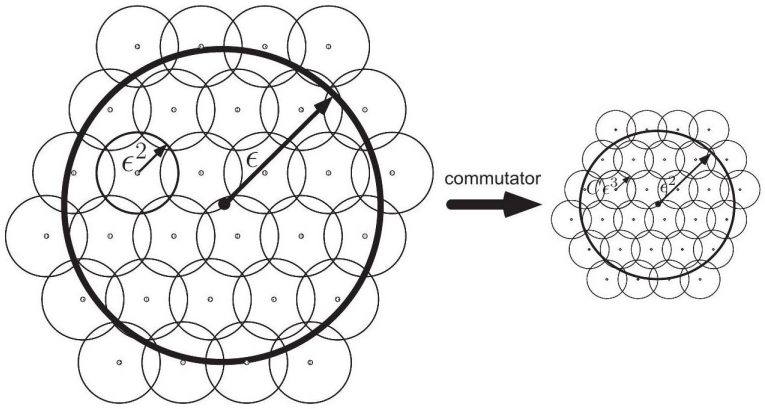


Figure A3.2. The main idea in the proof of Lemma A3.2. Taking group commutators of elements \$U_{1
\$ and U_2 in S_ϵ fills in S_{ϵ^2} much more densely. Note that the density of circles appearing on the right hand side ought to be much higher than is shown, as there should be one for each pair of circles on the left; the lower density is merely for clarity. The proof of the lemma is completed by applying a translation step (not shown) to get good approximations to any element of $S_{\sqrt{3}\epsilon^{3/2}}$.}

Exercise A3.2: Suppose A and B are Hermitian matrices such that $\mathrm{tr}\,|A|, \mathrm{tr}\,|B| \leq \epsilon$. Prove that for all sufficiently small ϵ,

$$D\left(\left[e^{-iA}, e^{-iB}\right]_{\text{gp}}, e^{-[A,B]}\right) \leq d\epsilon^3, \tag{A3.9}$$

for some constant d, establishing Equation (A3.6). (Comment: for practical purposes it may be interesting to obtain good bounds on d.)

Exercise A3.3: Let $\vec{x}$ and $\vec{y}$ be any two real vectors. Show that

$$D(u(\vec{x}), u(\vec{y})) = 2\sqrt{2}\sqrt{1 - \cos(x/2)\cos(y/2) - \sin(x/2)\sin(y/2)\hat{x}\cdot\hat{y}} \tag{A3.10}$$

where $x \equiv \|\vec{x}\|, y \equiv \|\vec{y}\|$, and $\hat{x}$ and $\hat{y}$ are unit vectors in the $\vec{x}$ and $\vec{y}$ directions, respectively.

Exercise A3.4: Show that in the case $\vec{y} = 0$ the formula for $D(u(\vec{x}), u(\vec{y}))$ reduces to

$$D(u(\vec{x}), I) = 4\sin\left|\frac{x}{4}\right| \tag{A3.11}$$

Exercise A3.5: Show that when $x, y \leq \epsilon$,

$$D(u(\vec{x}), u(\vec{y})) = \|\vec{x} - \vec{y}\| + O\left(\epsilon^3\right). \tag{A3.12}$$

Proof

(Lemma A3.2)

Suppose $\mathcal{G}_l$ is an ϵ^2-net in S_ϵ. The first step of the proof is to show that $[\mathcal{G}_l, \mathcal{G}_l]_{\text{gp}}$ is a $C\epsilon^3$-net for S_{ϵ^2} and some constant C.

Let $U \in S_{\epsilon^2}$ and pick $\vec{x}$ such that $U = u(\vec{x})$. By Exercise A3.4 it follows that $x \leq \epsilon^2 + O(\epsilon^6)$. Choose any pair of vectors $\vec{y}$ and $\vec{z}$ of length at most $\epsilon + O(\epsilon^5)$ such that $\vec{x} = \vec{y} \times \vec{z}$.$\mathcal{G}_l$ is an ϵ^2-net for S_ϵ, so choose U_1 and U_2 in $\mathcal{G}_l \cap S_\epsilon$ such that

$$D\left(U_1, u(\vec{y})\right) < \epsilon^2 + O\left(\epsilon^5\right) \tag{A3.13}$$

$$D\left(U_2, u(\vec{z})\right) < \epsilon^2 + O\left(\epsilon^5\right) \tag{A3.14}$$

and let $\vec{y}_0$ and $\vec{z}_0$ be chosen such that $U_1 = u(\vec{y}_0)$ and $U_2 = u(\vec{z}_0)$. By Exercise A3.4 it follows that $y_0, z_0 \leq \epsilon + O(\epsilon^3)$. Our goal is to show that $D\left(U, [U_1, U_2]_{\text{gp}}\right)$ is smaller than $C\epsilon^3$. To do this, we use the triangle inequality,

$$D\left(U, [U_1, U_2]_{\text{gp}}\right) \leq D\left(U, u\left(\vec{y}_0 \times \vec{z}_0\right)\right) + D\left(u\left(\vec{y}_0 \times \vec{z}_0\right), [U_1, U_2]_{\text{gp}}\right). \tag{A3.15}$$

The second term is at most $d'\epsilon^3$, by Exercise A3.2, where d' is a constant slightly larger than d because of the possible contribution due to the fact that $y_0, z_0 < \epsilon + O(\epsilon^3)$, rather than $y_0, z_0 < \epsilon$. Substituting $U = u(\vec{x})$, making use of Exercise A3.5, introducing an appropriate constant d'' and doing some elementary algebra gives

$$D\left(U, [U_1, U_2]_{\text{gp}}\right) \leq D\left(u(\vec{x}), u\left(\vec{y}_0 \times \vec{z}_0\right) + d'\epsilon^3\right. \tag{A3.16}$$

$$= \|\vec{x} - \vec{y}_0 \times \vec{z}_0\| + d''\epsilon^3 \tag{A3.17}$$

$$= \|\vec{y} \times \vec{z} - \vec{y}_0 \times \vec{z}_0\| + d''\epsilon^3 \tag{A3.18}$$

$$= \|[(\vec{y} - \vec{y}_0) + \vec{y}_0] \times [(\vec{z} - \vec{z}_0) + \vec{z}_0] - \vec{y}_0 \times \vec{z}_0\| + d''\epsilon^3 \tag{A3.19}$$

$$\leq (d'' + 2)\epsilon^3 + O\left(\epsilon^4\right) \tag{A3.20}$$

$$\leq C\epsilon^3 \tag{A3.21}$$

where C is an appropriately chosen constant.
The second step in the proof of the lemma is to apply a translation step like that used in the main part of the proof of the Solovay-Kitaev theorem. Specifically, given
$U \in S_{\sqrt{C\epsilon^3}}$, we can find V in $\mathcal{G}_l$ such that $D(U,V) \leq \epsilon^2$, and thus $UV^\dagger \in S_{\epsilon^2}$. Then find W_1 and W_2 in $\mathcal{G}_l$ such that $D\left([W_1,W_2]_{\rm gp}, UV^\dagger\right) \leq C\epsilon^3$, and therefore

$$D\left([W_1,W_2]_{\rm gp} V, U\right) \leq C\epsilon^3, \tag{A3.22}$$

which completes the proof. □

Exercise A3.6: Fixing the set $\mathcal{G}$ of elementary gates, describe an algorithm which, given a description of a single qubit unitary gate U and a desired accuracy $\epsilon > 0$, efficiently computes a sequence of gates from $\mathcal{G}$ that ϵ-approximates U.

The analysis in this appendix is rather crude, and a much tighter analysis can be made. One issue of especial interest is the best possible value of the exponent c in the $O\left(\log^c(1/\epsilon)\right)$ bound. It is not difficult to show that c can be no less than 1 . To see this, imagine we have a collection of N little balls, all of radius ϵ, in $SU(2)$. The volume of these balls scales like ϵ^d, for some unimportant constant d. Therefore, if the balls are to cover SU(2), N must be of size $\Omega\left(1/\epsilon^d\right)$. Suppose we consider all possible sequences $U_1 U_2 \ldots U_g$ consisting of g gates chosen from $\mathcal{G}$. Clearly such sequences can generate at most $|\mathcal{G}|^g$ distinct unitary operations. Thus we must have $|\mathcal{G}|^g = \Omega\left(1/\epsilon^d\right)$, which implies the desired lower bound on the number of gates,

$$g = \Omega\left(\log\left(\frac{1}{\epsilon}\right)\right). \tag{A3.23}$$

Problem 3.1: The following problem outlines a more elaborate construction that achieves an $O\left(\log^2(1/\epsilon)\log^c(\log(1/\epsilon))\right)$ bound on the number of gates required to approximate to within ϵ of a desired target, for any $c > 2$.
(1) Suppose $\mathcal{N}$ is a δ-net in S_ϵ, for $0 < \delta < \epsilon \leq \epsilon_0, \epsilon_0$ sufficiently small. Show that $[\mathcal{N},\mathcal{N}]_{\rm gp}$ is a $d\delta\epsilon$-net in S_{ϵ^2}, for some constant d.
(2) Suppose $\mathcal{G}_l$ is a δ-net in S_ϵ, for $0 < \delta < \epsilon \leq \epsilon_0$. Show that $\mathcal{G}_{4^k l}$ is a $d^k\delta\epsilon^{2^k-1}$-net in $S_{\epsilon^{2^k}}$.
(3) Suppose we define k by

$$k \equiv \left\lceil \log\left(\frac{\log(1/\epsilon)}{\log\left(1/\epsilon_0\right)}\right)\right\rceil, \tag{A3.24}$$

and suppose we can find l such that $\mathcal{G}_l$ is a δ_0-net for S_{ϵ_0}, where

$$d^k\delta_0 = \epsilon_0. \tag{A3.25}$$

Show that $\mathcal{G}_{4^k l}$ is an ϵ-net for $S_{\epsilon_0^k}$.
(4) Use the already-proved version of the Solovay-Kitaev theorem to show that choosing $l = O\left(k^c\right)$ suffices in the previous part of this problem, where $c = \log(5)/\log(3/2)$ is the constant appearing in the exponent in the already-proved version of the Solovay-Kitaev theorem.
(5) Combine the previous results to prove that $O\left(\log^2(1/\epsilon)\log^c(\log(1/\epsilon))\right)$ gates can be used to ϵ-approximate an arbitrary gate in $SU(2)$.
(6) Show that any $c > 2$ can appear in the conclusion of the previous result.

Problem 3.2: (Research) If it exists, find an approximation procedure asympoticially faster than the result found in the previous problem. Ideally, a procedure would (a) saturate the $\Omega(\log(1/\epsilon))$ lower bound on the number of gates required to perform the approximation, and (b) provide an efficient algorithm for constructing such approximating sequences of gates.

Problem 3.3: (Research) Fix a finite set of single qubit gates $\mathcal{G}$ which can be performed fault-tolerantly and which generate a set dense in the single qubit gates; say the $\pi/8$ gate and the Hadamard gate. Develop an elegant, efficient and reasonably tight method which,

given an arbitrary single qubit gate U and some $\epsilon > 0$, produces a sequence of gates from the fault-tolerant set giving an ϵ-approximation to U, up to global phase.

History and further reading

The results in this appendix were proved by Solovay in 1995 (unpublished manuscript), and independently by Kitaev, who gave an outline of the proof in [Kit97b]. In the same paper Kitaev observed that the result can be generalized to many Lie groups other than $SU(2)$; roughly speaking, the key fact about $SU(2)$ used in the proof was that $[\ S_\epsilon, S_\epsilon]_{\rm gp} \supseteq S_{\Omega(\epsilon^2)}$, and other Lie groups for which this fact holds also obey some version of the Solovay-Kitaev theorem. The Solovay-Kitaev theorem is true, for example, for the Lie group $SU(d)$ of d by d unitary matrices with unit determinant. After hearing of this result, Solovay subsequently generalized his proof in a similar fashion. Our presentation has benefited substantially from a 1999 lecture of Freedman, and by discussions with Freedman, Kitaev and Solovay.

B.0.5 NCh.4: Number theory

Understanding some elementary number theory is necessary if we are to understand cryptosystems and how quantum computers can be used to break them. In this appendix we review some basic facts about number theory.

A4.1 Fundamentals

Let's start off by agreeing about a few conventions for nomenclature and notation. The set of integers is the set $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$, denoted $\mathbf{Z}$. We may occasionally refer to the natural numbers, meaning non-negative integers, but more often we'll say nonnegative integer or positive integer, in order to make the distinction between the case when zero is included, and when zero is not included.

Suppose n is an integer. An integer d divides n (written $d \mid n$) if there exists an integer k such that $n = dk$. We say in this case that d is a factor or divisor of n. Notice that 1 and n are always factors of n. When d does not divide (is not a factor of) n we write $d \nmid n$. For example, $3 \mid 6$ and $3 \mid 18$, but $3 \nmid 5$ and $3 \nmid 7$.

Exercise A4.1: (Transitivity) Show that if $a \mid b$ and $b \mid c$ then $a \mid c$.

Exercise A4.2: Show that if $d \mid a$ and $d \mid b$ then d also divides linear combinations of a and $b, ax + by$, where x and y are integers.

Exercise A4.3: Suppose a and b are positive integers. Show that if $a \mid b$ then $a \leq b$. Conclude that if $a \mid b$ and $b \mid a$ then $a = b$.

A prime number is an integer greater than 1 which has only itself and 1 as factors. The first few prime numbers are $2, 3, 5, 7, 11, 13, 17, \ldots$. Perhaps the most important single fact about the positive integers is that they may be represented uniquely as a product of factors which are prime numbers. This result is given an appropriately impressive name, the fundamental theorem of arithmetic:

Theorem A4.1: (Fundamental theorem of arithmetic) Let a be any integer greater than 1 . Then a has a prime factorization of the form

$$a = p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n} \tag{A4.1}$$

where $p_1, \ldots, p_n$ are distinct prime numbers, and $a_1, \ldots, a_n$ are positive integers. Moreover, this prime factorization is unique, up to the order of the factors.

Proof

The reader who has never seen a proof of the fundamental theorem of arithmetic is strongly encouraged to attempt to supply it for themselves. Failing that, a proof may be found in any elementary number theory text; see the end of appendix 'History and further reading' for references. □

For small numbers it is easy to find the prime factorization by trial and error, for example $20 = 2^2 \cdot 5^1$. For large numbers no efficient algorithm is known to find the prime factorization on a classical computer, despite immense effort aimed at finding such an algorithm.

Exercise A4.4: Find the prime factorizations of 697 and 36300.

A4.2 Modular arithmetic and Euclid's algorithm

We're all thoroughly familiar with the techniques of ordinary arithmetic. Another type of arithmetic, modular arithmetic, is extremely useful in understanding the properties of numbers. We assume that you are familiar with the elementary ideas of modular arithmetic, and so will quickly breeze through the basic ideas and notation, before coming to more advanced theory.

Modular arithmetic can be thought of as the arithmetic of remainders. If we divide 18 by 7 we get the answer 2, with a remainder of 4 . More formally, given any positive integers x and n, x can be written (uniquely) in the form

$$x = kn + r, \tag{A4.2}$$

where k is a non-negative integer, the result of dividing x by n, and the remainder r lies in the range 0 to $n-1$, inclusive. Modular arithmetic is simply ordinary arithmetic in which we only pay attention to remainders. We use the notation $(\bmod n)$ to indicate that we are working in modular arithmetic. For instance, we write $2 = 5 = 8 = 11(\text{mod}3)$, because $2, 5, 8$ and 11 all have the same remainder (2) when divided by 3 . The appellation ' $(\text{mod}n)$ ' reminds us that we are working in modular arithmetic, with respect to the number n.

Addition, multiplication, and subtraction operations for modular arithmetic may all be defined in the obvious ways, but it is perhaps not so obvious how to define a division operation. To understand how this may be done we introduce another key concept from number theory, that of the greatest common divisor of two integers. The greatest common divisor of integers a and b is the largest integer which is a divisor of both a and b. We write this number as $\gcd(a, b)$. For example, the greatest common divisor of 18 and 12 is 6 . An easy way of seeing this is to enumerate the positive divisors of $18(1, 2, 3, 6, 9, 18)$ and $12(1, 2, 3, 4, 6, 12)$, and then pick out the largest common element in the two lists. This method is quite inefficient and impractical for large numbers. Fortunately, there is a much more efficient way of working out the greatest common divisor, a method known as Euclid's algorithm, whose explication occupies us for the next few pages.

Theorem A4.2: (Representation theorem for the gcd) The greatest common divisor of two integers a and b is the least positive integer that can be written in the form $ax + by$, where x and y are integers.

Proof

Let $s = ax + by$ be the smallest positive integer that can be written in this form. Since $\gcd(a, b)$ is a divisor of both a and b it is also a divisor of s. It follows that $\gcd(a, b) \leq s$. To complete the proof we demonstrate that $s \leq \gcd(a, b)$ by showing that s is a divisor of both a and b. The proof is by contradiction. Suppose s is not a divisor of a. Then $a = ks + r$, where the remainder r is in the range 1 to $s-1$. Rearranging this equation and using $s = ax + by$ we see that $r = a(1-kx)+b(-ky)$ is a positive integer that can be written as a linear combination

of a and b, and which is smaller than s. But this contradicts the definition of s as the smallest positive integer that can be written as a linear combination of a and b. We conclude that s must divide a. By symmetry s must also be a divisor of b, which completes the proof. □

Corollary A4.3: Suppose c divides both a and b. Then c divides $\gcd(a, b)$.

Proof

By Theorem A4.2, $\gcd(a, b) = ax + by$ for some integers x and y. Since c divides a and b it must also divide $ax + by$. □

When does a number, a, have a multiplicative inverse in modular arithmetic? That is, given a and n, when does there exist a b such that $ab = 1(\mathrm{mod} n)$? For example, note that $2 \cdot 3 = 1(\mathrm{mod} 5)$, so the number 2 has multiplicative inverse 3 in arithmetic modulo 5. On the other hand, trial and error shows that 2 has no multiplicative inverse modulo 4 . Finding multiplicative inverses in modular arithmetic turns out to be related to the gcd by the notion of co-primality: integers a and b are said to be co-prime if their greatest common divisor is 1 . For example, 14 and 9 are co-prime, since the positive divisors of 14 are $1, 2, 7$ and 14 , while 1,3 and 9 are the positive divisors of 9 . The following corollary characterizes the existence of multiplicative inverses in modular arithmetic using co-primality.

Corollary A4.4: Let n be an integer greater than 1 . An integer a has a multiplicative inverse modulo n if and only if $\gcd(a, n) = 1$, that is, a and n are co-prime.

Proof

Suppose a has a multiplicative inverse, which we denote a^{-1}, modulo n. Then $aa^{-1} = 1 + kn$ for some integer k, and thus $aa^{-1} + (-k)n = 1$. From Theorem A4.2 we conclude that $\gcd(a, n) = 1$. Conversely, if $\gcd(a, n) = 1$ then there must exist integers a^{-1} and b such that $aa^{-1} + bn = 1$, and therefore $aa^{-1} = 1(\mathrm{mod} n)$. □

Exercise A4.5: For p a prime prove that all integers in the range 1 to $p-1$ have multiplicative inverses modulo p. Which integers in the range 1 to $p^2 - 1$ do not have multiplicative inverses modulo p^2 ?

Exercise A4.6: Find the multiplicative inverse of 17 modulo 24.

Exercise A4.7: Find the multiplicative inverse of $n+1$ modulo n^2, where n is any integer greater than 1 .

Exercise A4.8: (Uniqueness of the inverse) Suppose b and b' are multiplicative inverses of a, modulo n. Prove that $b = b'(\mathrm{mod} n)$.

The next theorem is the key to Euclid's efficient algorithm for finding the greatest common divisor of two positive integers.

Theorem A4.5: Let a and b be integers, and let r be the remainder when a is divided by b. Then provided $r \neq 0$,

$$\gcd(a, b) = \gcd(b, r) \tag{A4.3}$$

Proof

We prove the equality by showing that each side divides the other. To prove that the left hand side divides the right note that $r = a - kb$ for some integer k. Since $\gcd(a, b)$ divides a, b and linear combinations of these it follows that $\gcd(a, b)$ divides r. By Corollary A4.3, $\gcd(a, b)$ divides $\gcd(b, r)$. To prove that the right hand side divides the left note that $\gcd(b, r)$ divides b, and since $a = r + kb$ is a linear combination of b and r it follows that $\gcd(b, r)$ also divides a. By Corollary A4.3, $\gcd(b, r)$ divides $\gcd(a, b)$.

Exercise A4.9: Explain how to find $\gcd(a, b)$ if the prime factorizations of a and b are known. Find the prime factorizations of 6825 and 1430 , and use them to compute $\gcd(6825, 1430)$

Euclid's algorithm for finding the greatest common divisor of positive integers a and b works as follows. First, order a and b so that $a > b$. Divide b into a, with result k_1 and remainder $r_1 : a = k_1 b + r_1$. By Theorem A4.5 $\gcd(a, b) = \gcd(b, r_1)$. Next, we perform a second division with b playing the role of a, and r_1 playing the role of $b : b = k_2 r_1 + r_2$. By Theorem A4.5 $\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2)$. Next, we perform a third division with r_1 playing the role of a and r_2 the role of $b : r_1 = k_3 r_2 + r_3$. By Theorem A4.5 $\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \gcd(r_2, r_3)$. We continue in this manner, each time dividing the most recent remainder by the second most recent remainder, obtaining a new result and remainder. The algorithm halts when we obtain a remainder that is zero, that is, $r_m = k_{m+1} r_{m+1}$ for some m. We have $\gcd(a, b) = \gcd(r_m, r_{m+1}) = r_{m+1}$, so the algorithm returns r_{m+1}.

As an example of the use of Euclid's algorithm we find $\gcd(6825, 1430)$:

$$6825 = 4 \times 1430 + 1105 \tag{A4.4}$$
$$1430 = 1 \times 1105 + 325 \tag{A4.5}$$
$$1105 = 3 \times 325 + 130 \tag{A4.6}$$
$$325 = 2 \times 130 + 65 \tag{A4.7}$$
$$130 = 2 \times 65 \tag{A4.8}$$

From this we see that $\gcd(6825, 1430) = 65$.

An adaptation of Euclid's algorithm may be used to efficiently find integers x and y such that $ax + by = \gcd(a, b)$. The first stage is to run through the steps of Euclid's algorithm, as before. The second stage begins at the second last line of the running of Euclid's algorithm, and involves successive substitution of the lines higher up in the algorithm as illustrated by the following example:

$$65 = 325 - 2 \times 130 \tag{A4.9}$$

$$= 325 - 2 \times (1105 - 3 \times 325) = -2 \times 1105 + 7 \times 325 \tag{A4.10}$$
$$= -2 \times 1105 + 7 \times (1430 - 1 \times 1105) = 7 \times 1430 - 9 \times 1105 \tag{A4.11}$$
$$= 7 \times 1430 - 9 \times (6825 - 4 \times 1430) = -9 \times 6825 + 37 \times 1430 \tag{A4.12}$$

That is, $65 = 6825 \times (-9) + 1430 \times 37$, which is the desired representation.

What resources are consumed by Euclid's algorithm? Suppose a and b may be represented as bit strings of at most L bits each. It is clear that none of the divisors k_i or remainders r_i can be more than L bits long, so we may assume that all computations are done in L bit arithmetic. The key observation to make in a resource analysis is that $r_{i+2} \leq r_i/2$. To prove this we consider two cases:

- $r_{i+1} \leq r_i/2$. It is clear that $r_{i+2} \leq r_{i+1}$ so we are done.
- $r_{i+1} > r_i/2$. In this case $r_i = 1 \times r_{i+1} + r_{i+2}$, so $r_{i+2} = r_i - r_{i+1} \leq r_i/2$.

Since $r_{i+2} \leq r_i/2$, it follows that the divide-and-remainder operation at the heart of Euclid's algorithm need be performed at most $2\lceil \log a \rceil = O(L)$ times. Each divide-andremainder operation requires $O(L^2)$ operations, so the total cost of Euclid's algorithm is $O(L^3)$. Finding x and y such that $ax + by = \gcd(a, b)$ incurs a minor additional cost: $O(L)$ substitutions are performed, at a cost of $O(L^2)$ per substitution to do the arithmetic involved, for a total resource cost of $O(L^3)$.

Euclid's algorithm may also be used to efficiently find multiplicative inverses in modular arithmetic. This is implicit in the proof of Corollary A4.4; we now make it explicit. Suppose a is co-prime to n, and we wish to find a^{-1}, modulo n. To do so, use Euclid's algorithm and the co-primality of a and n to find integers x and y such that

$$ax + ny = 1. \tag{A4.13}$$

Note then that $ax = (1 - ny) = 1(\mathrm{mod} n)$, that is, x is the multiplicative inverse of a, modulo n. Furthermore, this algorithm is computationally efficient, taking only $O\left(L^3\right)$ steps, where L is the length in bits of n.

Now that we know how to efficiently find inverses in modular arithmetic, it is only a short step to solve simple linear equations, such as

$$ax + b = c(\mathrm{mod} n). \tag{A4.14}$$

Suppose a and n are co-prime. Then using Euclid's algorithm we may efficiently find the multiplicative inverse a^{-1} of a, modulo n, and thus the solution to the previous equation,

$$x = a^{-1}(c - b)(\mathrm{mod} n). \tag{A4.15}$$

An important result known as the Chinese remainder theorem extends the range of equations we may solve much further, allowing us to efficiently solve systems of equations in modular arithmetic.

Theorem A4.6: (Chinese remainder theorem) Suppose $m_1, \ldots, m_n$ are positive integers such that any pair m_i and $m_j (i \neq j)$ are co-prime. Then the system of equations

$$x = a_1 \left(\mathrm{mod} m_1\right) \tag{A4.16}$$
$$x = a_2 \left(\mathrm{mod} m_2\right) \tag{A4.17}$$

$$x = a_n \left(\mathrm{mod} m_n\right) \tag{A4.18}$$

has a solution. Moreover, any two solutions to this system of equations are equal modulo $M \equiv m_1 m_2 \ldots m_n$.

Proof

The proof is to explicitly construct a solution to the system of equations. Define $M_i \equiv M/m_i$ and observe that m_i and M_i are co-prime. It follows that M_i has an inverse modulo m_i, which we denote N_i. Define $x \equiv \sum_i a_i M_i N_i$. To see that x is a solution to the system of equations, note that $M_i N_i = 1 \left(\mathrm{mod} m_i\right)$ and $M_i N_i = 0 \left(\mathrm{mod} m_j\right)$ when $i \neq j$, so $x = a_i \left(\mathrm{mod} m_i\right)$, which demonstrates the existence of a solution.

Suppose x and x' are both solutions to the system of equations. It follows that $x - x' = 0 \left(\mathrm{mod} m_i\right)$ for each i, and thus m_i divides $x - x'$ for each i. Since the m_i are co-prime, it follows that the product $M = m_1 \ldots m_n$ also divides $x - x'$, so $x = x' (\mathrm{mod} M)$, as we set out to show.

Euclid's algorithm and the Chinese remainder theorem are two of the signal triumphs of algorithmic number theory. How ironic then that they should play a role in the sequence of ideas leading up to the RSA cryptosystem, whose presumed security is based on the difficulty of performing certain algorithmic tasks in number theory. Nevertheless, this is indeed the case! We turn now to the number-theoretic background necessary to understand the RSA cryptosystem. The key ideas are a famous result of classical number theory, Fermat's little theorem - not to be confused with Fermat's last theorem - and a generalization of Fermat's little theorem due to Euler. The proof of Fermat's little theorem relies on the following elegant lemma.

Lemma A4.7: Suppose p is prime and k is an integer in the range 1 to $p-1$. Then p divides $\binom{p}{k}$.

Proof

Consider the identity

$$p(p-1)\cdots(p-k+1) = \binom{p}{k} k(k-1)\cdots 1. \tag{A4.19}$$

Since $k \geq 1$ the left hand side (and thus the right) is divisible by p. Since $k \leq p-1$ the term $k(k-1)\cdots 1$ is not divisible by p. It follows that $\binom{p}{k}$ must be divisible by p.

Theorem A4.8: (Fermat's little theorem) Suppose p is a prime, and a is any integer. Then $a^p = a(\mathrm{mod}p)$. If a is not divisible by p then $a^{p-1} = 1(\mathrm{mod}p)$.

Proof

The second part of the theorem follows from the first, since if a is not divisible by p then a has an inverse modulo p, so $a^{p-1} = a^{-1}a^p = a^{-1}a = 1(\mathrm{mod}p)$. We prove the first part of the theorem for positive a (the case of non-positive a follows easily) by induction on a. When $a = 1$ we have $a^p = 1 = a(\mathrm{mod}p)$, as required. Suppose the result holds true
for a, that is, $a^p = a(\mathrm{mod}p)$ and consider the case of $a+1$. By the binomial expansion,

$$(1+a)^p = \sum_{k=0}^{p} \binom{p}{k} a^k \tag{A4.20}$$

By Lemma A4.7, p divides $\binom{p}{k}$ whenever $1 \leq k \leq p-1$, so all terms except the first and last vanish from the sum modulo $p, (1+a)^p = (1+a^p)\,(\mathrm{mod}p)$. Applying the inductive hypothesis $a^p = a(\mathrm{mod}p)$ we see that $(1+a)^p = (1+a)(\mathrm{mod}p)$, as required.

There is a remarkable generalization of Fermat's little theorem due to Euler, based on the Euler φ function. $\varphi(n)$ is defined to be the number of positive integers less than n which are co-prime to n. As an example, note that all positive integers less than a prime p are co-prime to p, and thus $\varphi(p) = p-1$. The only integers less than p^α which are not co-prime to p^α are the multiples of $p : p, 2p, 3p, \ldots, (p^{\alpha-1}-1)\,p$, from which we deduce

$$\varphi\left(p^\alpha\right) = \left(p^\alpha - 1\right) - \left(p^{\alpha-1} - 1\right) = p^{\alpha-1}(p-1) \tag{A4.21}$$

Furthermore, if a and b are co-prime, then the Chinese remainder theorem can be used to show that

$$\varphi(ab) = \varphi(a)\varphi(b) \tag{A4.22}$$

To see this, consider the system of equations $x = x_a(\mathrm{mod}a), x = x_b(\mathrm{mod}b)$. Applying the Chinese remainder theorem to this set of equations we see that there is a one-to-one correspondence between pairs $(\ x_a, x_b\ )$ such that $1 \leq x_a < a, 1 \leq x_b < b, \gcd(x_a, a) = 1, \gcd(x_b, b) = 1$, and integers x such that $1 \leq x < ab, \gcd(x, ab) = 1$. There are $\varphi(a)\varphi(b)$ such pairs (x_a, x_b) and $\varphi(ab)$ such x, from which we deduce (A4.22).

Equations (A4.21) and (A4.22) together imply a formula for $\varphi(n)$ based on the prime factorization of $n, n = p_1^{\alpha_1}\cdots p_k^{\alpha_k}$:

$$\varphi(n) = \prod_{j=1}^{k} p_j^{\alpha_j - 1}\,(p_j - 1) \tag{A4.23}$$

Exercise A4.10: What is φ (187)?
Exercise A4.11: Prove that

$$n = \sum_{d|n} \varphi(d) \tag{A4.24}$$

where the sum is over all positive divisors d of n, including 1 and n. (Hint: Prove the result for $n = p^\alpha$ first, then use the multiplicative property (A4.22) of φ to complete the proof.)

Fermat's little theorem has the following beautiful generalization, due to Euler:
Theorem A4.9: Suppose a is co-prime to n. Then $a^{\varphi(n)} = 1(\mathrm{mod} n)$.

Proof

We first show by induction on α that $a^{\varphi(p^\alpha)} = 1\,(\mathrm{mod} p^\alpha)$. For $\alpha = 1$ the result is just Fermat's little theorem. Assume the result is true for $\alpha \geq 1$, so

$$a^{\varphi(p^\alpha)} = 1 + kp^\alpha \tag{A4.25}$$

for some integer k. Then by (A4.21),

$$\begin{aligned} a^{\varphi\left(p^{\alpha+1}\right)} &= a^{p^\alpha(p-1)} && \text{(A4.26)} \\ &= a^{p\varphi(p^\alpha)} && \text{(A4.27)} \\ &= (1 + kp^\alpha)^p && \text{(A4.28)} \\ &= 1 + \sum_{j=1}^{p} \binom{p}{j} k^j p^{j\alpha}. && \text{(A4.29)} \end{aligned}$$

Using Lemma A4.7 it is easy to see that $p^{\alpha+1}$ divides every term in the sum, so

$$a^{\varphi\left(p^{\alpha+1}\right)} = 1\left(\mathrm{mod} p^{\alpha+1}\right) \tag{A4.30}$$

which completes the induction. The proof of the theorem is completed by noting that for arbitrary $n = p_1^{\alpha_1} \cdots p_m^{\alpha_m}, a^{\varphi(n)} = 1\left(\mathrm{mod} p_j^{\alpha_j}\right)$ for each j, as $\varphi(n)$ is a multiple of $\varphi\left(p_j^{\alpha_j}\right)$. Applying the construction in the proof of the Chinese remainder theorem we find that any solution to the set of equations $x = 1\left(\mathrm{mod} p_j^{\alpha_j}\right)$ must satisfy $x = 1(\mathrm{mod} n)$, and thus $a^{\varphi(n)} = 1(\mathrm{mod} n)$.

Define $\mathbf{Z}_n^*$ to be the set of all elements in $\mathbf{Z}_n$ which have inverses modulo n, that is, the set of all elements in $\mathbf{Z}_n$ which are co-prime to n.$\mathbf{Z}_n^*$ is easily seen to form a group of size $\varphi(n)$ under multiplication, that is, it contains the multiplicative identity, products of elements in $\mathbf{Z}_n^*$ are in $\mathbf{Z}_n^*$, and $\mathbf{Z}_n^*$ is closed under the multiplicative inverse operation. (For an overview of elementary group theory, see Appendix 2.) What is not so obvious is the remarkable structure $\mathbf{Z}_n^*$ has when n is a power of an odd prime $p, n = p^\alpha$. It turns out that $\mathbf{Z}_{p^\alpha}^*$ is a cyclic group, that is, there is an element g in $\mathbf{Z}_{p^\alpha}^*$ which generates $\mathbf{Z}_{p^\alpha}^*$ in the sense that any other element x may be written $x = g^k(\mathrm{mod} n)$ for some non-negative integer k.

Theorem A4.10: Let p be an odd prime, α a positive integer. Then $\mathbf{Z}_{p^\alpha}^*$ is cyclic.

Proof

The proof of this fact is a little beyond the scope of this book. It can be found in many texts containing any considerable amount of number theory. See for example Section 3.2 of Knuth [Knu98a], especially pages 16 through 23.

Exercise A4.12: Verify that $\mathbf{Z}_n^*$ forms a group of size $\varphi(n)$ under the operation of multiplication modulo n.

Exercise A4.13: Let a be an arbitrary element of $\mathbf{Z}_n^*$. Show that $S \equiv \{1, a, a^2, \ldots\}$ forms a subgroup of $\mathbf{Z}_n^*$, and that the size of S is the least value of r such that $a^r = 1 (\mathrm{mod} n)$.

Exercise A4.14: Suppose g is a generator for $\mathbf{Z}_n^*$. Show that g must have order $\varphi(n)$.

Exercise A4.15: Lagrange's theorem (Theorem A2.1 on page 610) is an elementary result of group theory stating that the size of a subgroup must divide the order of the group. Use Lagrange's theorem to provide an alternate proof of Theorem A4.9, that is, show that $a^{\varphi(n)} = 1 (\mathrm{mod} n)$ for any $a \in \mathbf{Z}_n^*$.

A4.3 Reduction of factoring to order-finding

The problem of factoring numbers on a classical computer turns out to be equivalent to another problem, the order-finding problem. This equivalence is important as it turns out that quantum computers are able to quickly solve the order-finding problem, and thus can factor quickly. In this section we explain the equivalence between these two problems, focusing on the reduction of factoring to order-finding.

Suppose N is a positive integer, and x is co-prime to $N, 1 \leq x \leq N$. The order of x modulo N is defined to be the least positive integer r such that $x^r = 1 (\mathrm{mod} N)$. The order-finding problem is to determine r, given x and N.

Exercise A4.16: Use Theorem A4.9 to show that the order of x modulo N must divide $\varphi(N)$.

The reduction of factoring to order-finding proceeds in two basic steps. The first step is to show that we can compute a factor of n if we can find a non-trivial solution $x \neq \pm 1 (\mathrm{mod} N)$ to the equation $x^2 = 1 (\mathrm{mod} N)$. The second step is to show that a randomly chosen y co-prime to N is quite likely to have an order r which is even, and such that $y^{r/2} \neq \pm 1 (\mathrm{mod} N)$, and thus $x \equiv y^{r/2} (\mathrm{mod} N)$ is a solution to $x^2 = 1 (\mathrm{mod} N)$.

Theorem A4.11: Suppose N is a composite number L bits long, and x is a non-trivial solution to the equation $x^2 = 1 (\mathrm{mod} N)$ in the range $1 \leq x \leq N$, that is, neither $x = 1 (\mathrm{mod} N)$ nor $x = N - 1 = -1 (\mathrm{mod} N)$. Then at least one of $\gcd(x - 1, N)$ and $\gcd(x + 1, N)$ is a non-trivial factor of N that can be computed using $O(L^3)$ operations.

Proof

Since $x^2 = 1 (\mathrm{mod} N)$, it must be that N divides $x^2 - 1 = (x + 1)(x - 1)$, and thus N must have a common factor with one or the other of ($x + 1$) and ($x - 1$). But $1 < x < N - 1$ by assumption, so $x - 1 < x + 1 < N$, from which we see that the common factor can not be N itself. Using Euclid's algorithm we may compute $\gcd(x - 1, N)$ and $\gcd(x + 1, N)$ and thus obtain a non-trivial factor of N, using $O(L^3)$ operations. □

Lemma A4.12: Let p be an odd prime. Let 2^d be the largest power of 2 dividing $\varphi(p^\alpha)$. Then with probability exactly one-half 2^d divides the order modulo p^α of a randomly chosen element of $\mathbf{Z}_{p^\alpha}^*$.

Proof

Note that $\varphi(p^\alpha) = p^{\alpha-1}(p - 1)$ is even, since p is odd, and thus $d \geq 1$. By Theorem A4.10 there exists a generator g for $\mathbf{Z}_{p^\alpha}^*$, so an arbitrary element may be written in the form $g^k (\mathrm{mod} p^\alpha)$ for some k in the range 1 through $\varphi(p^\alpha)$. Let r be the order of g^k modulo p^α and consider two cases. The first case is when k is odd. From $g^{kr} = 1 (\mathrm{mod} p^\alpha)$ we deduce that $\varphi(p^\alpha) \mid kr$, and thus $2^d \mid r$, since k is odd. The second case is when k is even. Then

$$g^{k\varphi(p^\alpha)/2} = \left(g^{\varphi(p^\alpha)}\right)^{k/2} = 1^{k/2} = 1 (\mathrm{mod} p^\alpha). \tag{A4.31}$$

Thus $r \mid \varphi(p^\alpha)/2$ from which we deduce that 2^d does not divide r.

Summarizing, $\mathbf{Z}^*_{p^\alpha}$ may be partitioned into two sets of equal size: those which may be written g^k with k odd, for which $2^d \mid r$, where r is the order of g^k, and those which may be written g^k with k even, for which $2^d \nmid r$. Thus with probability 1/2 the integer 2^d divides the order r of a randomly chosen element of $\mathbf{Z}^*_{p^\alpha}$, and with probability 1/2 it does not.

Theorem A4.13: Suppose $N = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ is the prime factorization of an odd composite positive integer. Let x be chosen uniformly at random from $\mathbf{Z}^*_N$, and let r be the order of x, modulo N. Then

$$p\left(r \text{ is even and } x^{r/2} \neq -1(\mathrm{mod}N)\right) \geq 1 - \frac{1}{2^m} \tag{A4.32}$$

Proof

We show that

$$p\left(r \text{ is odd or } x^{r/2} = -1(\mathrm{mod}N)\right) \leq \frac{1}{2^m} \tag{A4.33}$$

By the Chinese remainder theorem, choosing x uniformly at random from $\mathbf{Z}^*_N$ is equivalent to choosing x_j independently and uniformly at random from $\mathbf{Z}^*_{p_j}$, and requiring that $x = x_j \left(\mathrm{mod} p_j^{\alpha_j}\right)$ for each j. Let r_j be the order of x_j modulo $p_j^{\alpha_j}$. Let 2^{d_j} be the largest power of 2 that divides r_j and 2^d be the largest power of 2 that divides r. We will show that to have r odd or $x^{r/2} = -1(\mathrm{mod}N)$ it is necessary that d_j takes the same value for all values of j. The result then follows, as from Lemma A4.12 the probability of this occurring is at most $1/2^m$.

The first case we consider is when r is odd. It is easy to see that $r_j \mid r$ for each j, and therefore r_j is odd, so $d_j = 0$ for all $i = 1, \ldots, k$. The second and final case is when r is even and $x^{r/2} = -1(\mathrm{mod}N)$. Then $x^{r/2} = -1 \left(\mathrm{mod} p_j^{\alpha_j}\right)$, so $r_j \nmid (r/2)$. Since $r_j \mid r$ we must have $d_j = d$ for all j.

Theorems A4.11 and A4.13 can be combined to give an algorithm which, with high probability, returns a non-trivial factor of any composite N. All the steps in the algorithm can be performed efficiently on a classical computer except (as far as is known today) an order-finding 'subroutine' which is used by the algorithm. By repeating the algorithm we may find a complete prime factorization of N. The algorithm is summarized below.

(1) If N is even, return the factor 2 .

(2) Use the algorithm of Exercise 5.17 to determine whether $N = a^b$ for integers $a \geq 1$ and $b \geq 2$, and if so return the factor a.

(3) Randomly choose x in the range 1 to $N-1$. If $\gcd(x, N) > 1$ then return the factor $\gcd(x, N)$.

(4) Use the order-finding subroutine to find the order r of x, modulo N.

(5) If r is even and $x^{r/2} \neq -1(\mathrm{mod}N)$ then compute $\gcd\left(x^{r/2} - 1, N\right)$ and $\gcd\left(x^{r/2} + 1, N\right)$, and test to see which is a non-trivial factor, returning that factor. Otherwise, the algorithm fails.

Steps 1 and 2 of the algorithm either return a factor, or else ensure that N is an odd integer with more than one prime factor. These steps may be performed using $O(1)$ and $O\left(L^3\right)$ operations, respectively. Step 3 either returns a factor, or produces a randomly chosen element x of $\mathbf{Z}^*_N$. Step 4 calls the order-finding subroutine, computing the order r of x, modulo N. Step 5 completes the algorithm, since Theorem A4.13 guarantees that with probability at least one-half r will be even and $x^{r/2} \neq -1(\mathrm{mod}N)$, and then Theorem A4.11 guarantees that either $\gcd\left(x^{r/2} - 1, N\right)$ or $\gcd\left(x^{r/2} + 1, N\right)$ is a non-trivial factor of N.

Exercise A4.17: (Reduction of order-finding to factoring) We have seen that an efficient order-finding algorithm allows us to factor efficiently. Show that an efficient factoring algorithm

would allow us to efficiently find the order modulo N of any x co-prime to N.

A4.4 Continued fractions

There are many remarkable connections between the continuum of real numbers and the integers. One such connection is the beautiful theory of continued fractions. In this section we develop a few elements of the theory of continued fractions, elements crucial to the application of the fast quantum algorithms for order-finding and factoring detailed in Chapter 5.

As an example of a continued fraction, consider the number s defined by the expression

$$s \equiv \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \ldots}}} \tag{A4.34}$$

Informally, note that $s = 1/(2+s)$, from which it is easy to satisfy oneself that $s = \sqrt{2} - 1$. The idea of the continued fractions method is to describe real numbers in terms of integers alone, using expressions such as (A4.34). A finite simple continued fraction is defined by a finite collection $a_0, \ldots, a_N$ of positive integers,

$$[a_0, \ldots, a_N] \equiv a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ldots + \frac{1}{a_N}}}} \tag{A4.35}$$

We define the nth convergent ($0 \leq n \leq N$) to this continued fraction to be $[a_0, \ldots, a_n]$.
Theorem A4.14: Suppose x is a rational number greater than or equal to one. Then x has a representation as a continued fraction, $x = [a_0, \ldots, a_N]$, which may be found by the continued fractions algorithm.

Proof

The continued fractions algorithm is best understood by example. Suppose we are trying to decompose 31/13 as a continued fraction. The first step of the continued fractions algorithm is to split 31/13 into its integer and fractional part,

$$\frac{31}{13} = 2 + \frac{5}{13} \tag{A4.36}$$

Next we invert the fractional part, obtaining

$$\frac{31}{13} = 2 + \frac{1}{\frac{13}{5}} \tag{A4.37}$$

These steps - split then invert - are now applied to 13/5, giving

$$\frac{31}{13} = 2 + \frac{1}{2 + \frac{3}{5}} = 2 + \frac{1}{2 + \frac{1}{\frac{5}{3}}} \tag{A4.38}$$

Next we split and invert 5/3 :

$$\frac{31}{13} = 2 + \frac{1}{2 + \frac{1}{1 + \frac{2}{3}}} = 2 + \frac{1}{2 + \frac{1}{1 + \frac{1}{\frac{3}{2}}}} \tag{A4.39}$$

The decomposition into a continued fraction now terminates, since $3/2 = 1 + 1/2$ may be written with a 1 in the numerator without any need to invert, giving a final continued fraction representation of 31/13 as

$$\frac{31}{13} = 2 + \frac{1}{2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2}}}} \tag{A4.40}$$

It's clear that the continued fractions algorithm terminates after a finite number of 'split and invert' steps for any rational number, since the numerators which appear ($31, 3, 2, 1$ in the example) are strictly decreasing. How quickly does this termination occur? We'll come back to that question shortly.

The theorem above has been stated for $x \geq 1$; however, in practice it is convenient to relax the requirement that a_0 to be positive and allow it to be any integer, which results in the restriction $x \geq 1$ becoming superfluous. In particular, if x is in the range 0 through 1 as occurs in applications to quantum algorithms, then the continued fraction expansion has $a_0 = 0$.

The continued fractions algorithm provides an unambiguous method for obtaining a continued fraction expansion of a given rational number. The only possible ambiguity comes at the final stage, because it is possible to split an integer in two ways, either $a_n = a_n$, or as $a_n = (a_n - 1) + 1/1$, giving two alternate continued fraction expansions. This ambiguity is actually useful, since it allows us to assume without loss of generality that the continued fraction expansion of a given rational number has either an odd or even number of convergents, as desired.

Exercise A4.18: Find the continued fraction expansion for $x = 19/17$ and $x = 77/65$.

Theorem A4.15: Let $a_0, \ldots, a_N$ be a sequence of positive numbers. Then

$$[a_0, \ldots, a_n] = \frac{p_n}{q_n}, \tag{A4.41}$$

where p_n and q_n are real numbers defined inductively by $p_0 \equiv a_0, q_0 \equiv 1$ and $p_1 \equiv 1 + a_0 a_1, q_1 \equiv a_1$, and for $2 \leq n \leq N$,

$$p_n \equiv a_n p_{n-1} + p_{n-2} \tag{A4.42}$$

$$q_n \equiv a_n q_{n-1} + q_{n-2}. \tag{A4.43}$$

In the case where a_j are positive integers, so too are the p_j and q_j.

Proof

We induct on n. The result is easily checked directly for the cases $n = 0, n = 1, 2$. By definition, for $n \geq 3$,

$$[a_0, \ldots, a_n] = [a_0, \ldots, a_{n-2}, a_{n-1} + 1/a_n]\,. \tag{A4.44}$$

Applying the inductive hypothesis, let $\tilde{p}_j/\tilde{q}_j$ be the sequence of convergents associated with the continued fraction on the right hand side:

$$[a_0, \ldots, a_{n-2}, a_{n-1} + 1/a_n] = \frac{\tilde{p}_{n-1}}{\tilde{q}_{n-1}} \tag{A4.45}$$

It is clear that $\tilde{p}_{n-3} = p_{n-3}, \tilde{p}_{n-2} = p_{n-2}$ and $\tilde{q}_{n-3} = q_{n-3}, \tilde{q}_{n-2} = q_{n-2}$, so

$$\frac{\tilde{p}_{n-1}}{\tilde{q}_{n-1}} = \frac{(a_{n-1} + 1/a_n)\, p_{n-2} + p_{n-3}}{(a_{n-1} + 1/a_n)\, q_{n-2} + q_{n-3}} \tag{A4.46}$$

$$= \frac{p_{n-1} + p_{n-2}/a_n}{q_{n-1} + q_{n-2}/a_n} \tag{A4.47}$$

Multiplying top and bottom of the right hand side by a_n we see that

$$\frac{\tilde{p}_{n-1}}{\tilde{q}_{n-1}} = \frac{p_n}{q_n} \tag{A4.48}$$

Combining Equations (A4.48), (A4.45) and (A4.44) gives

$$[a_0, \ldots, a_n] = \frac{p_n}{q_n} \tag{A4.49}$$

as required.

Exercise A4.19: Show that $q_n p_{n-1} - p_n q_{n-1} = (-1)^n$ for $n \geq 1$. Use this fact to conclude that $\gcd(p_n, q_n) = 1$. (Hint: Induct on n.)

How many values of a_n must be determined to obtain a continued fraction expansion for a rational number $x = p/q > 1$, where p and q are co-prime? Suppose $a_0, \ldots, a_N$ are positive integers. From the definition of p_n and q_n it follows that p_n and q_n are increasing sequences. Therefore $p_n = a_n p_{n-1} + p_{n-2} \geq 2p_{n-2}$ and similarly $q_n \geq 2q_{n-2}$, from which it follows that $p_n, q_n \geq 2^{\lfloor n/2 \rfloor}$. Thus the $2^{\lfloor N/2 \rfloor} \leq q \leq p$, and so $N = O(\log(p))$. It follows that if $x = p/q$ is a rational number, p and q are L bit integers, then the continued fraction expansion for x can be computed using $O(L^3)$ operations - $O(L)$ 'split and invert' steps, each using $O(L^2)$ gates for elementary arithmetic.

Theorem A4.16: Let x be a rational number and suppose p/q is a rational number such that

$$\left| \frac{p}{q} - x \right| \leq \frac{1}{2q^2} \tag{A4.50}$$

Then p/q is a convergent of the continued fraction for x.

Let $p/q = [a_0, \ldots, a_n]$ be the continued fraction expansion for p/q, and define p_j, q_j as in Theorem A4.15, so that $p_n/q_n = p/q$. Define δ by the equation

$$x \equiv \frac{p_n}{q_n} + \frac{\delta}{2q_n^2}, \tag{A4.51}$$

so $|\delta| < 1$. Define λ by the equation

$$\lambda \equiv 2 \left(\frac{q_n p_{n-1} - p_n q_{n-1}}{\delta} \right) - \frac{q_{n-1}}{q_n}. \tag{A4.52}$$

The reason we define λ this way is because with a little algebra we can see that it satisfies the equation

$$x = \frac{\lambda p_n + p_{n-1}}{\lambda q_n + q_{n-1}} \tag{A4.53}$$

and therefore $x = [a_0, \ldots, a_n, \lambda]$. Choosing n even we see from Exercise A4.19 that

$$\lambda = \frac{2}{\delta} - \frac{q_{n-1}}{q_n} \tag{A4.54}$$

By the increasing property of q_n it follows that

$$\lambda = \frac{2}{\delta} - \frac{q_{n-1}}{q_n} > 2 - 1 > 1 \tag{A4.55}$$

Therefore λ is a rational number greater than 1 , and so has a simple finite continued fraction, $\lambda = [b_0, \ldots, b_m]$, and so $x = [a_0, \ldots, a_n, b_0, \ldots, b_m]$ is a simple finite continued fraction for x with p/q as a convergent.

Problem 4.1: (Prime number estimate) Let $\pi(n)$ be the number of prime numbers which are less than n. A difficult-to-prove result known as the prime number theorem asserts that $\lim_{n\to\infty} \pi(n)\log(n)/n = 1$ and thus $\pi(n) \approx n/\log(n)$. This problem gives a poor man's version of the prime number theorem which gives a pretty good lower bound on the distribution of prime numbers.
(1) Prove that $n \leq \log\binom{2n}{n}$.
(2) Show that

$$\log\binom{2n}{n} \leq \sum_{p\leq 2n} \left\lfloor \frac{\log(2n)}{\log p} \right\rfloor \log p \tag{A4.56}$$

where the sum is over all primes p less than or equal to $2n$.
(3) Use the previous two results to show that

$$\pi(2n) \geq \frac{n}{\log(2n)} \tag{A4.57}$$

History and further reading

There are many excellent books on number theory. We have made considerable use of the excellent book by Koblitz [Kob94], which combines much introductory material about number theory, algorithms, and cryptography all in one location. A similar combination forming a small part of a much more comprehensive presentation oriented towards algorithms may be found in Chapter 33 of Cormen, Leiserson and Rivest [CLR90] . Our discussion of continued fractions is based upon Chapter 10 of the classic text on number theory by Hardy and Wright [HW60]. Problem 4.1 is adapted from Papadimitriou [Pap94].

B.0.6 NCh.5: Public key cryptography and the RSA cryptosystem

Cryptography is the art of enabling two parties to communicate in private. For example, a consumer wishing to make a purchase on the internet wants to transmit their credit card number over the internet in such a way that only the company they are purchasing from gains access to the number. Rather more ominously, in wartime each of the warring parties wants the means to carry on private communication. To achieve privacy a cryptographic protocol or cryptosystem is used. Effective cryptosystems make it easy for parties who wish to communicate to do so, but make it very difficult for third parties to 'eavesdrop' on the contents of the conversation.

A particularly important class of cryptosystems are the public key cryptosystems. The basic idea of public key cryptography is illustrated by the analogy depicted in Figure A5.1. Alice sets up a mailbox with the property that anybody can send her mail, by putting it into the mailbox, but only she can retrieve mail out of the mailbox. To achieve this she gives the mailbox two doors. On top of the mailbox is a locked trap door. Any person able to open the trap door can drop mail into the box. However, the chute from the trap door into the box is one way, so they can't reach into the box and fish mail out. Alice makes the key to the trapdoor freely available to the public - it is a public key - so that she can receive mail from absolutely anybody. On the front of the mail box is a second door, from which mail already inside the box can be retrieved. Alice is in possession of the sole key for that door; it is her own secret key. This arrangement - involving two keys, one secret and one public - allows anybody in the world to communicate with Alice while maintaining privacy.

Public key cryptosystems operate according to similar principles. Suppose Alice wishes to receive messages using a public key cryptosystem. She must first generate two cryptographic keys, one a public key, P, the other a secret key, S. The exact nature of these keys depends on the details of the cryptosystem being used. Some cryptosystems use simple objects like

numbers as keys, while other cryptosystems use much more complicated mathematical objects, like elliptic curves, as keys. Once Alice has generated her keys, she publishes the public key so that anybody can obtain access to the key.

Now suppose Bob wishes to send Alice a private message. He first obtains a copy of Alice's public key P, and then encrypts the message he wishes to send Alice, using Alice's public key to perform the encryption. Exactly how the encryption transformation is performed depends on the details of the cryptosystem in use. The key point is that in order to be secure against eavesdropping the encryption stage needs to be very difficult to reverse, even making use of the public key used to encrypt the message in the first place! It's like the trap door for mail - what you can put in you can't take back out, even if you have the key to the trap door. Since the public key and the encoded message is the only information available to an eavesdropper it won't be possible for the eavesdropper to recover the message. Alice, however, has an additional piece of information not available

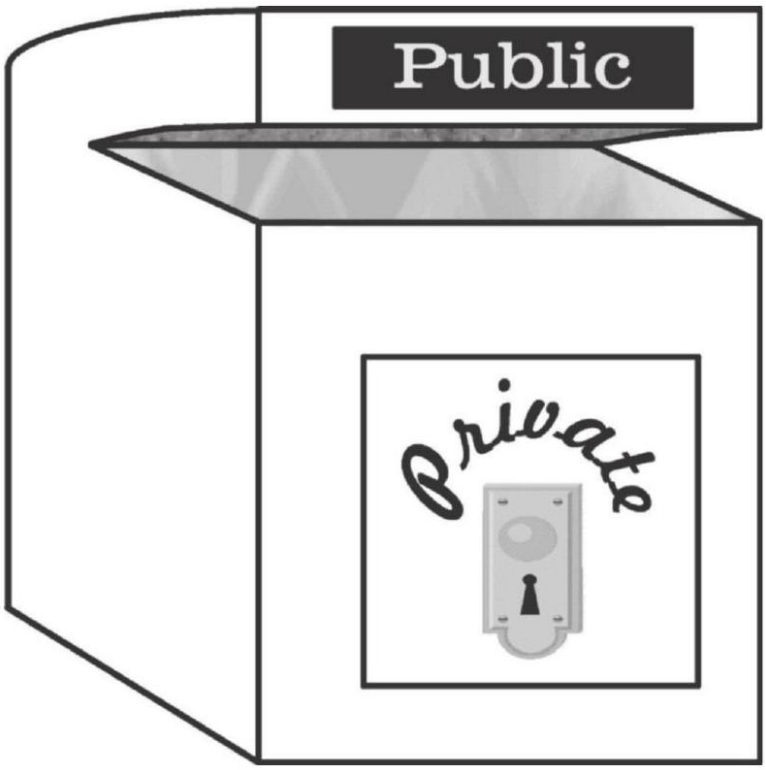


Figure A5.1. The key ideas of public key cryptography, illustrated in more familiar terms. Essentially the same scheme is implemented by the Post Office in many countries.

to an eavesdropper, the secret key, S. The secret key determines a second transformation, this time on the encrypted message. This transformation is known as decryption, and is inverse to encryption, allowing Alice to recover the original message.

In an ideal world that is how public key cryptography would work. Unfortunately, at the time of writing it is not known whether there are any such secure schemes for doing public key cryptography. There do exist several schemes which are widely believed to be secure, and which are in common use for applications such as internet commerce, but wide belief is not equivalent to a proof of security. The reason these schemes are believed to be secure is because so much effort has been devoted to finding a means for breaking these schemes (without success!), a sort of proof by attrition. The most widely used of these public key cryptosystems is the RSA cryptosystem, named RSA for the initials of its creators, Rivest, Shamir, and Adleman. The presumed security of the RSA cryptosystem is based, as we shall now see, on the apparent

difficulty of factoring on a classical computer. Understanding RSA requires a little background in number theory, which is covered in Appendix 4, notably Sections A4.1 and A4.2.

Suppose Alice wishes to create public and private keys for use with the RSA cryptosystem. She uses the following procedure:
(1) Select two large prime numbers, p and q.
(2) Compute the product $n \equiv pq$.
(3) Select at random a small odd integer, e, that is relatively prime to $\varphi(n) = (p-1)(q-1)$.
(4) Compute d, the multiplicative inverse of e, modulo $\varphi(n)$.
(5) The RSA public key is the pair $P = (e, n)$. The RSA secret key is the pair $S = (d, n)$.

Suppose a second party, Bob, wishes to encrypt a message M to send to Alice, using the public key (e, n). We assume the message M has only $\lfloor \log n \rfloor$ bits, as longer messages may be encrypted by breaking M up into blocks of at most $\lfloor \log n \rfloor$ bits and then encrypting the blocks separately. The encryption procedure for a single block is to compute:

$$E(M) = M^e (\mathrm{mod} n) \tag{A5.1}$$

$E(M)$ is the encrypted version of the message M, which Bob transmits to Alice. Alice can quickly decrypt the message using her secret key $S = (d, n)$, simply by raising the encrypted message to the d th power:

$$E(M) \rightarrow D(E(M)) = E(M)^d (\mathrm{mod} n) \tag{A5.2}$$

For the decryption to be successful we need $D(E(M)) = M(\mathrm{mod} n)$. To see that this is the case, note that by construction ed $= 1(\mathrm{mod}\varphi(n))$ and thus $ed = 1 + k\varphi(n)$ for some integer k. The proof now proceeds by considering two different cases. In the first case, M is co-prime to n. By Euler's generalization of Fermat's little theorem, Theorem A4.9, it follows that $M^{k\varphi(n)} = 1(\mathrm{mod} n)$ and thus,

$$\begin{aligned} D(E(M)) &= E(M)^d (\mathrm{mod} n) && \text{(A5.3)} \\ &= M^{ed} (\mathrm{mod} n) && \text{(A5.4)} \\ &= M^{1+k\varphi(n)} (\mathrm{mod} n) && \text{(A5.5)} \\ &= M \cdot M^{k\varphi(n)} (\mathrm{mod} n) && \text{(A5.6)} \\ &= M (\mathrm{mod} n), && \text{(A5.7)} \end{aligned}$$

which establishes that the decryption is successful when M is co-prime to n. Suppose next that M is not co-prime to n, so that one or both of p and q divide M. To be specific, we consider the case where p divides M and q does not divide M; the other possible cases requre only minor modifications. Because p divides M we have $M = 0(\mathrm{mod} p)$ and thus $M^{ed} = 0 = M(\mathrm{mod} p)$. Because q does not divide M we have $M^{q-1} = 1(\mathrm{mod} q)$ by Fermat's little theorem, and thus $M^{\varphi(n)} = 1(\mathrm{mod} q)$, since $\varphi(n) = (p-1)(q-1)$. Using $ed = 1 + k\varphi(n)$ we see that $M^{ed} = M(\mathrm{mod}\, q)$. By the Chinese remainder theorem it follows that we must have $M^{ed} = M(\mathrm{mod}\, n)$, and thus the decryption is also successful when M is not co-prime to n.

Exercise A5.1: Written examples of the application of RSA tend to be rather opaque. It's better to work through an example yourself. Encode the word 'QUANTUM' (or at least the first few letters!), one letter at a time, using $p = 3$ and $q = 11$. Choose appropriate values for e and d, and use a representation of English text involving 5 bits per letter.

How efficiently can RSA be implemented? There are two implementation issues to be considered. First is the generation of public and private keys for the cryptosystem. If this can't be done quickly then RSA won't be good for much. The main bottleneck is the generation of the prime numbers p and q. The way this is attacked is to randomly select a number of the

desired length, and then to apply a primality test to determine if the number is, in fact, prime. Fast primality tests such as the Miller-Rabin test can be used to determine whether a number is prime using roughly $O\left(L^3\right)$ operations, where L is the desired size of the cryptographic key. If the number is found to be composite
then we simply repeat the procedure until a prime is found. The prime number theorem (see Problem 4.1) implies that the probability of any given number being prime is about $1/\log\left(2^L\right) = 1/L$, so with high probability $O(L)$ trials are required to obtain a prime number, for a total cost of $O\left(L^4\right)$ operations to do key generation.

The second issue in the implementation of RSA is the efficiency of the encryption and decryption transformations. These are accomplished by modular exponentiation, which we know can be done efficiently using $O\left(L^3\right)$ operations - see Box 5.2 on page 228. Thus all the operations required to use the RSA cryptosystem can be done quite quickly on a classical computer, and in practice modest computing power can quite easily cope with keys up to a few thousand bits in length.

How can RSA be broken? We describe two methods by which one might hope to break RSA, one based on order-finding, the other based on factoring. Suppose Eve receives an encrypted message $M^e(\mathrm{mod}n)$, and knows the public key (e, n) used to encrypt the message. Suppose she can find the order of the encrypted message, that is, she can find the smallest positive integer r such that $(M^e)^r = 1(\mathrm{mod}n)$. (Without loss of generality, we may suppose such an order exists, that is, M^e is co-prime to n. If this is not the case, then $M^e(\mathrm{mod}n)$ and n have a common factor that may be extracted by Euclid's algorithm, which would allow us to break RSA, as in the second method described below.) Then Exercise A4.16 implies that r divides $\varphi(n)$. Since e is co-prime to $\varphi(n)$ it must also be co-prime to r, and thus has a multiplicative inverse modulo r. Let d' be such a multiplicative inverse, so $ed' = 1 + kr$ for some integer k. Then Eve can recover the original message M by raising the encrypted message to the d' th power:

$$\begin{aligned} \left(M^e\right)^{d'}(\mathrm{mod}n) &= M^{1+kr}(\mathrm{mod}n) && \text{(A5.8)} \\ &= M \cdot M^{kr}(\mathrm{mod}n) && \text{(A5.9)} \\ &= M(\mathrm{mod}n) && \text{(A5.10)} \end{aligned}$$

It is interesting that Eve never actually learns the secret key (d, n); she only learns (d', n). Of course, d' is closely related to d, since d' is the inverse of e modulo r, d is the inverse of e modulo $\varphi(n)$, and r divides $\varphi(n)$. Nevertheless, this example shows that it is possible to break RSA without necessarily determining the exact value of the secret key. Of course, this method only works if Eve has an efficient method for order-finding, and no such method is currently known for a classical computer. On a quantum computer, however, order-finding can be accomplished efficiently, as described in Section 5.3.1, and thus RSA can be broken.

Exercise A5.2: Show that d is also an inverse of e modulo r, and thus $d = d'(\mathrm{mod}r)$.
A second method for breaking RSA allows one to determine the secret key completely. Suppose Eve could factor $n = pq$, extracting p and q, and thus giving a means for efficiently computing $\varphi(n) = (p-1)(q-1)$. It is then an easy matter for Eve to compute d, the inverse of e modulo $\varphi(n)$, and thus completely determine the secret key (d, n). So, if factoring large numbers were easy then it would be easy to break RSA.

The presumed security of RSA rests on the fact that these attacks rely on having algorithms to solve problems which are believed (but not known) to be intractable on a classical computer, the order-finding and factoring problems. Unfortunately, it's not even known to be the case that RSA is secure if these problems are hard. It could be that these problems really are difficult, yet there is some other way of breaking RSA. Despite

these caveats, more than two decades of attempts to break RSA have resulted in failure, and it is widely believed that RSA is secure against attacks by classical computers.

Problem 5.1: Write a computer program for performing encryption and decryption using the RSA algorithm. Find a pair of 20 bit prime numbers and use them to encrypt a 40 bit message.

History and further reading

Public key cryptosystems were invented by Diffie and Hellman in 1976[DH76], and independently by Merkle at about the same time, although his work was not published until 1978[Mer78]. The RSA cryptosystem was invented shortly after by Rivest, Shamir, and Adleman [RSA78]. In 1997 it was disclosed that these ideas - public key cryptography, the Diffie-Hellman and RSA cryptosystems - were actually invented in the late 1960s and early 1970s by researchers working at the British intelligence agency GCHQ. An account of this work may be found at 'http://www.cesg.gov.uk/about/nsecret/'. Primality tests such as the Miller-Rabin and Solovay-Strassen tests are described in Koblitz's excellent book [Kob94] on number theory and cryptography, which contains a wealth of additional material on public key cryptography. These primality tests were two of the earliest indicators that randomized algorithms may be more efficient for some purposes than deterministic algorithms. The Solovay-Strassen algorithm is due to Solovay and Strassen [SS76], and the Miller-Rabin test is due jointly to Miller [Mil76] and Rabin [Rab80].

B.0.7 NCh.6: Proof of Lieb's theorem

One of the most important and useful results in quantum information theory is the strong subadditivity inequality for von Neumann entropies. This states that for a trio of quantum systems, A, B, C,

$$S(A,B,C) + S(B) \leq S(A,B) + S(B,C) \tag{A6.1}$$

Unfortunately, no transparent proof of strong subadditivity is known. Chapter 11 presents a relatively simple proof, based upon a deep mathematical result known as Lieb's theorem. In this appendix we prove Lieb's theorem. We begin with a few simple notations and definitions.

Suppose $f(A,B)$ is a real-valued function of two matrices, A and B. Then f is said to be jointly concave in A and B if for all $0 \leq \lambda \leq 1$,

$$f\left(\lambda A_1 + (1-\lambda)A_2, \lambda B_1 + (1-\lambda)B_2\right) \geq \lambda f\left(A_1, B_1\right) + (1-\lambda) f\left(A_2, B_2\right). \tag{A6.2}$$

For matrices A and B, we say $A \leq B$ if $B - A$ is a positive matrix. We say $A \geq B$ if $B \leq A$. Let A be an arbitrary matrix. We define the norm of A by

$$\|A\| \equiv \max_{\langle u|u\rangle = 1} |\langle u|A|u\rangle| \,. \tag{A6.3}$$

In our proof of Lieb's theorem we will have occasion to use the following easily verified observations:

Exercise A6.1: ($\leq$ is preserved under conjugation) If $A \leq B$, show that $XAX^\dagger \leq XBX^\dagger$ for all matrices X.

Exercise A6.2: Prove that $A \geq 0$ if and only if A is a positive operator.

Exercise A6.3: ($\leq$ is a partial order) Show that the relation $\leq$ is a partial order on operators - that is, it is transitive ($A \leq B$ and $B \leq C$ implies $A \leq C$), asymmetric ($A \leq B$ and $B \leq A$ implies $A = B$), and reflexive ($A \leq A$).

Exercise A6.4: Suppose A has eigenvalues λ_i. Define λ to be the maximum of the set $|\lambda_i|$. Prove that:
(1) $\|A\| \geq \lambda$.
(2) When A is Hermitian, $\|A\| = \lambda$.
(3) When

$$A = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \tag{A6.4}$$

$$\|A\| = 3/2 > 1 = \lambda$$

Exercise A6.5: (AB and BA have the same eigenvalues) Prove that AB and BA have the same eigenvalues. (Hint: For invertible A, show that $\det(xI - AB) = \det(xI - BA)$, and thus the eigenvalues of AB and BA are the same. By continuity this holds even when A is not invertible.)

Exercise A6.6: Suppose A and B are such that AB is Hermitian. Using the previous two observations show that $\|AB\| \leq \|BA\|$.

Exercise A6.7: Suppose A is positive. Show that $\|A\| \leq 1$ if and only if $A \leq I$.
Exercise A6.8: Let A be a positive matrix. Define a superoperator (linear operator on matrices) by the equation $\mathcal{A}(X) \equiv AX$. Show that $\mathcal{A}$ is positive with respect to the Hilbert-Schmidt inner product. That is, for all $X, \mathrm{tr}\left(X^\dagger \mathcal{A}(X)\right) \geq 0$.
Similarly, show that the superoperator defined by $\mathcal{A}(X) \equiv XA$ is positive with respect to the Hilbert-Schmidt inner product on matrices.

With these results in hand, we are now in a position to state and prove Lieb's theorem.
Theorem A6.1: (Lieb's theorem) Let X be a matrix, and $0 \leq t \leq 1$. Then the function

$$f(A, B) \equiv \mathrm{tr}\left(X^\dagger A^t X B^{1-t}\right) \tag{A6.5}$$

is jointly concave in positive matrices A and B.
Lieb's theorem is an easy corollary of the following lemma:
Lemma A6.2: Let $R_1, R_2, S_1, S_2, T_1, T_2$ be positive operators such that $0 = [R_1, R_2] = [S_1, S_2] = [T_1, T_2]$, and

$$R_1 \geq S_1 + T_1 \tag{A6.6}$$
$$R_2 \geq S_2 + T_2. \tag{A6.7}$$

Then for all $0 \leq t \leq 1$,

$$R_1^t R_2^{1-t} \geq S_1^t S_2^{1-t} + T_1^t T_2^{1-t} \tag{A6.8}$$

is true as a matrix inequality.

Proof

We begin by proving the result for $t = 1/2$, and then use this to establish the result for general t. It will be convenient to assume that R_1 and R_2 are invertible, and it is left as an exercise to make the minor technical modifications to the proof necessary to establish the result when this is not the case.

Let $|x\rangle$ and $|y\rangle$ be any two vectors. Applying the Cauchy-Schwarz inequality twice and performing some straightforward manipulations, we have

$$
\begin{aligned}
&\left|\langle x|\left(S_1^{1/2}S_2^{1/2}+T_1^{1/2}T_2^{1/2}\right)\Big|y\right\rangle| \\
\leq&\left|\langle x|S_1^{1/2}S_2^{1/2}\Big|y\right\rangle\right|+\left|\langle x|T_1^{1/2}T_2^{1/2}\Big|y\right\rangle| && \text{(A6.9)}\\
\leq&\|S_1^{1/2}|x\rangle\|\|S_2^{1/2}|y\rangle\|+\|T_1^{1/2}|x\rangle\|\|T_2^{1/2}|y\rangle\| && \text{(A6.10)}\\
\leq&\sqrt{\left(\|S_1^{1/2}|x\rangle\|^2+\|T_1^{1/2}|x\rangle\|^2\right)\left(\|S_2^{1/2}|y\rangle\|^2+\|T_2^{1/2}|y\rangle\|^2\right)} && \text{(A6.11)}
\end{aligned}
$$

$$
=\sqrt{\langle x|\left(S_1+T_1\right)|x\rangle\langle y|\left(S_2+T_2\right)|y\rangle}. \qquad \text{(A6.12)}
$$

By hypothesis, $S_1+T_1\leq R_1$ and $S_2+T_2\leq R_2$, so

$$
\left|\langle x|\left(S_1^{1/2}S_2^{1/2}+T_1^{1/2}T_2^{1/2}\right)\Big|y\right\rangle|\leq\sqrt{\langle x|R_1|x\rangle\langle y|R_2|y\rangle} \qquad \text{(A6.13)}
$$

Let $|u\rangle$ be any unit vector. Then applying (A6.13) with $|x\rangle\equiv R_1^{-1/2}|u\rangle$ and $|y\rangle\equiv R_2^{-1/2}|u\rangle$ gives

$$
\begin{aligned}
&\langle u|R_1^{-1/2}\left(S_1^{1/2}S_2^{1/2}+T_1^{1/2}T_2^{1/2}\right)R_2^{-1/2}|u\rangle \\
\leq&\sqrt{\langle u|R_1^{-1/2}R_1R_1^{-1/2}|u\rangle\langle u|R_2^{-1/2}R_2R_2^{-1/2}|u\rangle} && \text{(A6.14)}\\
=&\sqrt{\langle u\mid u\rangle\langle u\mid u\rangle}=1. && \text{(A6.15)}
\end{aligned}
$$

Thus

$$
\left\|R_1^{-1/2}\left(S_1^{1/2}S_2^{1/2}+T_1^{1/2}T_2^{1/2}\right)R_2^{-1/2}\right\|\leq 1 \qquad \text{(A6.16)}
$$

Define

$$
\begin{aligned}
A&\equiv R_1^{-1/4}R_2^{-1/4}\left(S_1^{1/2}S_2^{1/2}+T_1^{1/2}T_2^{1/2}\right)R_2^{-1/2} && \text{(A6.17)}\\
B&\equiv R_2^{1/4}R_1^{-1/4}. && \text{(A6.18)}
\end{aligned}
$$

Note that AB is Hermitian, so by Exercise A6.6 on page 646,

$$
\begin{aligned}
&\left\|R_1^{-1/4}R_2^{-1/4}\left(S_1^{1/2}S_2^{1/2}+T_1^{1/2}T_2^{1/2}\right)R_2^{-1/4}R_1^{-1/4}\right\| \\
=&\|AB\|\leq\|BA\| && \text{(A6.19)}\\
=&\left\|R_1^{-1/2}\left(S_1^{1/2}S_2^{1/2}+T_1^{1/2}T_2^{1/2}\right)R_2^{-1/2}\right\| && \text{(A6.20)}\\
\leq&1, && \text{(A6.21)}
\end{aligned}
$$

where the last inequality is just (A6.16). AB is a positive operator, so by Exercise A6.7 on page 646 and the previous inequality,

$$
R_1^{-1/4}R_2^{-1/4}\left(S_1^{1/2}S_2^{1/2}+T_1^{1/2}T_2^{1/2}\right)R_2^{-1/4}R_1^{-1/4}\leq I. \qquad \text{(A6.22)}
$$

Finally, by Exercise A6.1 on page 645, and the commutativity of R_1 and R_2,

$$
S_1^{1/2}S_2^{1/2}+T_1^{1/2}T_2^{1/2}\leq R_1^{1/2}R_2^{1/2}, \qquad \text{(A6.23)}
$$

which establishes that (A6.8) holds for $t = 1/2$.
Let I be the set of all t such that (A6.8) holds. By inspection, we see that 0 and 1 are elements of I, and we have just shown that $1/2$ is an element of I. We now use the $t = 1/2$ case to prove the result for any t such that $0 \leq t \leq 1$. Suppose μ and η are any two elements of I, so that

$$R_1^\mu R_2^{1-\mu} \geq S_1^\mu S_2^{1-\mu} + T_1^\mu T_2^{1-\mu} \tag{A6.24}$$
$$R_1^\eta R_2^{1-\eta} \geq S_1^\eta S_2^{1-\eta} + T_1^\eta T_2^{1-\eta} \tag{A6.25}$$

These inequalities are of the form (A6.6) and (A6.7) for which the $t = 1/2$ case has already been proved. Using the $t = 1/2$ result we see that

$$\left(R_1^\mu R_2^{1-\mu}\right)^{1/2} \left(R_1^\eta R_2^{1-\eta}\right)^{1/2} \geq \left(S_1^\mu S_2^{1-\mu}\right)^{1/2} \left(S_1^\eta S_2^{1-\eta}\right)^{1/2} + \left(T_1^\mu T_2^{1-\mu}\right)^{1/2} \left(T_1^\eta T_2^{1-\eta}\right)^{1/2} \tag{A6.26}$$

Using the commutativity assumptions $0 = [R_1, R_2] = [S_1, S_2] = [T_1, T_2]$, we see that for $\nu \equiv (\mu + \eta)/2$,

$$R_1^\nu R_2^{1-\nu} \geq S_1^\nu S_2^{1-\nu} + T_1^\nu T_2^{1-\nu} \tag{A6.27}$$

Thus whenever μ and η are in I, so is $(\mu+\eta)/2$. Since 0 and 1 are in I, it is easy to see that any number t between 0 and 1 with a finite binary expansion must be in I. Thus I is dense in $[0, 1]$. The result now follows from the continuity in t of the conclusion, (A6.8).

The proof of Lieb's theorem is a simple application of Lemma A6.2. The clever idea that makes this possible is to choose the operators in Lemma A6.2 to be superoperators - linear maps on operators. These will be chosen in such a way as to be positive with respect to the Hilbert-Schmidt inner product $(A, B) \equiv \mathrm{tr}\left(A^\dagger B\right)$.

Proof

(Lieb's theorem)

Let $0 \leq \lambda \leq 1$ and define superoperators $\mathcal{S}_1, \mathcal{S}_2, \mathcal{T}_1, \mathcal{T}_2, \mathcal{R}_1, \mathcal{R}_2$ as follows:

$$\mathcal{S}_1(X) \equiv \lambda A_1 X \tag{A6.28}$$
$$\mathcal{S}_2(X) \equiv \lambda X B_1 \tag{A6.29}$$
$$\mathcal{T}_1(X) \equiv (1-\lambda) A_2 X \tag{A6.30}$$
$$\mathcal{T}_2(X) \equiv (1-\lambda) X B_2 \tag{A6.31}$$
$$\mathcal{R}_1 \equiv \mathcal{S}_1 + \mathcal{T}_1 \tag{A6.32}$$
$$\mathcal{R}_2 \equiv \mathcal{S}_2 + \mathcal{T}_2 \tag{A6.33}$$

Observe that $\mathcal{S}_1$ and $\mathcal{S}_2$ commute, as do $\mathcal{T}_1$ and $\mathcal{T}_2$, and $\mathcal{R}_1$ and $\mathcal{R}_2$. Recall Exercise A6.8 on page 646, that all these operators are positive with respect to the Hilbert-Schmidt inner product. By Lemma A6.2,

$$\mathcal{R}_1^t \mathcal{R}_2^{1-t} \geq \mathcal{S}_1^t \mathcal{S}_2^{1-t} + \mathcal{T}_1^t \mathcal{T}_2^{1-t} \tag{A6.34}$$

Using the Hilbert-Schmidt inner product to take the $X \cdot X$ matrix element of the previous inequality gives

$$\begin{aligned}
&\operatorname{tr}\left[X^\dagger(\lambda\ A_1+(1-\lambda)A_2)^t\,X\,(\lambda B_1+(1-\lambda)B_2)^{1-t}\right] \\
&\qquad\geq \operatorname{tr}\left[X^\dagger\,(\lambda A_1)^t\,X\,(\lambda B_1)^{1-t}\right]+\operatorname{tr}\left[X^\dagger\,((1-\lambda)A_2)^t\,X\,((1-\lambda)B_2)^{1-t}\right] &\text{(A6.35)}\\
&\qquad=\lambda\operatorname{tr}\left(X^\dagger A_1^t X B_1^{1-t}\right)+(1-\lambda)\operatorname{tr}\left(X^\dagger A_2^t X B_2^{1-t}\right) &\text{(A6.36)}
\end{aligned}$$

which is the desired statement of joint concavity.

History and further reading

The history of Lieb's theorem is tied up with the proof of the strong subadditivity inequality for quantum entropies, and may be found together with the history of the proof of that inequality in the 'History and further reading' for Chapter 11.

B.1 Programming

(по идее тут много будет симуляций, так что мне понадобится код.)

Некоторые свойства тензорных произведений

Очень важно для доказательств теорем и преобразований формул владеть преобразованиями тензорного произведения.

(тут их список будет по актуальности)

C Bibliography

References

[1] Aharonov, Yakir, Albert, David Z., and Vaidman, Lev: *How the result of a measurement of a component of the spin of a spin-1/2 particle can turn out to be 100.* Physical review letters, 60(14):1351–1354, 1988, ISSN 0031-9007.

[2] Aharonov, Yakir. and Rohrlich, Daniel: *Quantum paradoxes: quantum theory for the perplexed.* Wiley-VCH, Weinheim, 2005, ISBN 3-527-40391-4.

Bibliography from Nielsen, Chang

Citations with 'ar Xive e-print quant-ph/ *xxxxxx* ' designations are available on the internet at http://www.arXiv.org

[ABO97] D. Aharonov and M. Ben-Or. Fault tolerant computation with constant error. In Proceedings of the Twenty-Ninth Annual ACM Symposium on the Theory of Computing, pages 176-188, 1997.

[ABO99] D. Aharonov and M. Ben-Or. Faulttolerant quantum computation with constant error rate. SIAM 7. Comp., page to appear, 1999. ar Xive e-print quantph/9906129.

[ABOIN96] D. Aharonov, M. Ben-Or, R. Impagliazzo, and N. Nisan. Limitations of noisy reversible computation. ar Xive e-print quant-ph/9611028, 1996.

[ADH97] L. Adleman, J. Demarrais, and M. A. Huang. Quantum computability. SIAM 7. Comp., 26(5):1524-1540, 1997.

[Ad194] L. M. Adleman. Molecular computation of solutions to combinatorial problems. Science, 266:1021, 1994.

[Ad198] L. M. Adleman. Computing with DNA. Sci. Am., 279:54-61, Aug. 1998.

[AE75] L. Allen and J. H. Eberly. Optical Resonance and Two-level Atoms. Dover, New York, 1975.

[Aha99a] D. Aharonov. Noisy Quantum Computation. Ph.D. thesis, The Hebrew Univesity, Jerusalem, 1999.

[Aha99b] D. Aharonov. Quantum computation. In D. Stauffer, editor, Annual Reviews of Computational Physics VI. World Scientific, Singapore, 1999.

[AKN98] D. Aharonov, A. Kitaev, and N. Nisan. Quantum circuits with mixed states. STOC 1997, 1998. arXive e-print quant-ph/9806029.

[AL70] H. Araki and E. H. Lieb. Entropy inequalities. Comm. Math. Phys., 18:160-170, 1970.

[AL97] D. S. Abrams and S. Lloyd. Simulation of many-body Fermi systems on a quantum computer. Phys. Rev. Lett., 79(13):2586-2589, 1997. ar Xive e-print quant-ph/9703054.

[AL99] A. Ashikhmin and S. Lytsin. Upper bounds on the size of quantum codes. IEEE Trans. Inf. Theory, 45(4):12061215, 1999.

[Alb83] P. M. Alberti. A note on the transitionprobability over c-* algebras. Lett. in Math. Phys., 7(1):25-32, 1983.

[Amb00] A. Ambainis. Quantum lower bounds by quantum arguments. arXive e-print quant-ph/0002066, 2000.

[And79] T. Ando. Concavity of certain maps on positive definite matrices and applications to Hadamard products. Linear Algebra Appl., 26:203-241, 1979.

[Ash97] A. Ashikhmin. Remarks on bounds for quantum codes. ar Xive e-print quantph/9705037, 1997.

[Bar78] E. Barton. A reversible computer using conservative logic. Unpublished MIT 6.895

term paper, 1978.
[BB84] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, pages 175-179, IEEE, New York, 1984. Bangalore, India, December 1984.
[BBB+92] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin. Experimental quantum cryptography. F. Cryptology, 5:3-28, 1992.
[BBB+98] E. Biham, M. Boyer, G. Brassard, J. van de Graaf, and T. Mor. Security of quantum key distribution against all collective attacks. ar Xive e-print quantph/9801022, 1998.
[BBBV97] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani. Strengths and weaknesses of quantum computing. SIAM $\mathcal{F}$. Comput., 26(5):1510-1523, 1997. ar Xive e-print quant-ph/9701001.
[BBC +93] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. Wootters. Teleporting an unknown quantum state via dual classical and EPR channels. Phys. Rev. Lett., 70:1895-1899, 1993.
[BBC +95] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter. Elementary gates for quantum computation. Phys. Rev. A, 52:3457-3467, 1995. ar Xive e-print quant-ph/9503016.
[BBC +98] R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf. Quantum lower bounds by polynomials. In Proceedings of the 39th Annual Symposium on Foundations of Computer Science (FOCS'98), pages 352-361, IEEE, Los Alamitos, California, November 1998. ar Xive e-print quant-ph/9802049.
[BBCM95] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer. Generalized privacy amplification. IEEE Trans. Inf. Theory, 41:1915-1923, 1995.
[BBE92] C. H. Bennett, G. Brassard, and A. K. Ekert. Quantum cryptography. Sci. Am., 267(4):50, Oct. 1992.
[BBHT98] M. Boyer, G. Brassard, P. Høyer, and A. Tapp. Tight bounds on quantum searching. Fortsch. Phys. - Prog. Phys., 46(4-5):493-505, 1998.
[BBM+98] D. Boschi, S. Branca, F. D. Martini, L. Hardy, and S. Popescu. Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein-Podolski-Rosen channels. Phys. Rev. Lett., 80:1121-1125, 1998. arXive e-print quant-ph/9710013.
[BBP ${ }^{+}$96] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters. Purification of noisy entanglement and faithful teleportation via noisy channels. Phys. Rev. Lett., 76:722, 1996. arXive e-print quantph/9511027.
[BBPS96] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher. Concentrating partial entanglement by local operations. Phys. Rev. A, 53(4):2046-2052, 1996. ar Xive e-print quant-ph/9511030.
[BBR88] C. H. Bennett, G. Brassard, and J. M. Robert. Privacy amplification by public discussion. SIAM . F. Comp., 17:210-229, 1988.
[BCDP96] D. Beckman, A. N. Chari, S. Devabhaktuni, and J. Preskill. Efficient networks for quantum factoring. Phys. Rev. A, 54(2):1034, 1996. ar Xive e-print quantph/9602016.
[BCF +96 H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacher. Noncommuting mixed states cannot be broadcast. Phys. Rev. Lett., 76(15):28282821, 1996. arXive e-print quantph/9511010.
[BCJ ${ }^{+}$99] S. L. Braunstein, C. M. Caves, R. Jozsa, N. Linden, S. Popescu, and R. Schack. Separability of very noisy mixed states and implications for NMR quantum computing. Phys. Rev. Lett., 83(5):1054-1057, 1999.
[BCJD99] G. K. Brennen, C. M. Caves, P. S. Jessen, and I. H. Deutsch. Quantum logic gates in optical lattices. Physical Review Letters, 82:1060-1063, 1999.

[BD00] C. H. Bennett and D. P. DiVincenzo. Quantum information and computation. Nature, 404:247-55, 2000.
[BDG88a] J. L. Balcázar, J. Diaz, and J. Gabarró. Structural Complexity, Volume I. Springer-Verlag, Berlin, 1988.
[BDG88b] J. L. Balcázar, J. Diaz, and J. Gabarró. Structural Complexity, Volume II. Springer-Verlag, Berlin, 1988.
[BDK92] R. G. Brewer, R. G. DeVoe, and R. Kallenbach. Planar ion microtraps. Phys. Rev. A, 46(11):R6781-4, 1992.
[BDS97] C. H. Bennett, D. P. DiVincenzo, and J. A. Smolin. Capacities of quantum erasure channels. Phys. Rev. Lett., 78(16):3217-3220, 1997. ar Xive e-print quant-ph/9701015.
[BDSW96] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters. Mixed state entanglement and quantum error correction. Phys. Rev. A, 54:3824, 1996. ar Xive e-print quant-ph/9604024.
[Bel64] J. S. Bell. On the Einstein-PodolsyRosen paradox. Physics, 1:195-200, 1964. Reprinted in J. S. Bell, Speakable and Unspeakable in Quantum Mechanics, Cambridge University Press, Cambridge, 1987.
[Ben73] C. H. Bennett. Logical reversibility
of computation. IBM 7. Res. Dev., 17(6):525-32, 1973.
[Ben80] P. Benioff. The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. 7. Stat. Phys., 22(5):563-591, 1980.
[Ben82] C. H. Bennett. The thermodynamics of computation - a review. Int. F. Theor. Phys., 21:905-40, 1982.
[Ben87] C. H. Bennett. Demons, engines and the second law. Sci. Am., 295(5):108, 1987.
[Ben89] C. H. Bennett. Time-space trade-offs for reversible computation. SIAM 7. Comput., 18:766-776, 1989.
[Ben92] C. H. Bennett. Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett., 68(21):3121-3124, 1992.
[Bet84] T. Beth. Methoden der Schnellen Fouriertransformation. Teubner, Leipzig, 1984.
[BFGL98] S. L. Braunstein, C. A. Fuchs, D. Gottesman, and H. Lo. A quantum analog of Huffman coding. ar Xive e-print quantph/9805080, 1998.
[BFJS96] H. Barnum, C. A. Fuchs, R. Jozsa, and B. Schumacher. General fidelity limit for quantum channels. Phys. Rev. A, 54:4707, 1996. arXive e-print quantph/9603014.
[Bha97] R. Bhatia. Matrix Analysis. SpringerVerlag, New York, 1997.
[BHT98] G. Brassard, P. Høyer, and A. Tapp. Quantum counting. ar Xive e-print quant-ph/9805082, 1998.
[BK92] V. B. Braginsky and F. Y. Khahili. Quantum Measurement. Cambridge University Press, Cambridge, 1992.
[BK98a] S. L. Braunstein and H. J. Kimble. Teleportation of continuous quantum variables. Phys. Rev. Lett., 80:869-72, 1998.
[BK98b] S. B. Bravyi and A. Y. Kitaev. Quantum codes on a lattice with boundary. ar Xive e-print quant-ph/9811052, 1998.
[BK99] S. L. Braunstein and H. J. Kimble. Dense coding for continuous variables. ar Xive e-print quant-ph/9910010, 1999.
[BKLW99] D. Bacon, J. Kempe, D. A. Lidar, and K. B. Whaley. Universal faulttolerant computation on decoherencefree subspaces. ar Xive e-print quantph/9909058, 1999.
[BKN98] H. Barnum, E. Knill, and M. A. Nielsen. On quantum fidelities and channel capacities. ar Xive e-print quant-ph/9809010, 1998.
[BL95] D. Boneh and R. J. Lipton. Quantum cryptoanalysis of hidden linear functions (extended abstract). In Don Coppersmith, editor, Lecture notes in computer science -

Advances in Cryptology CRYPTO'95, pages 424-437, SpringerVerlag, Berlin, 1995.
[BMP ${ }^{+}$99] P. O. Boykin, T. Mor, M. Pulver, V. Roychowdhury, and F. Vatan. On universal and fault-tolerant quantum computing. ar Xive e-print quant-ph/9906054, 1999.
[BNS98] H. Barnum, M. A. Nielsen, and B. W. Schumacher. Information transmission through a noisy quantum channel. Phys. Rev. A, 57:4153, 1998.
[Boh51] D. Bohm. Quantum Theory. PrenticeHall, Englewood Cliffs, New Jersey, 1951.
[BP93] S. M. Barnett and S. J. D. Phoenix. Information-theoretic limits to quantum cryptography. Phys. Rev. A, 48(1):R5R8, 1993.
[BPM $^{+}$97] D. Bouwmeester, J. W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger. Experimental quantum teleportation. *Na* ture, 390(6660):575-579, 1997.
[BR98] D. S. Bethune and W. P. Risk. An autocompensating quantum key distribution system using polarization splitting of light. In IQEC '98 Digest of Postdeadline Papers, pages QPD12-2, Optical Society of America, Washington, DC, 1998.
[BR00] D. S. Bethune and W. P. Risk. An autocompensating fiber-optic quantum cryptography system based on polarization splitting of light. 7. Quantum Electronics, 36(3):100, 2000.
[Bra93] G. Brassard. A bibliography of quantum cryptography. Université de Montréal preprint, pages 1-10, 3 December 1993. A preliminary version of this appeared in Sigact News, vol. 24(3), 1993, pages 1620.
[Bra98] S. L. Braunstein. Error correction for continuous quantum variables. Phys. Rev. Lett., 80:4084 4087, 1998. arXive eprint quant-ph/9711049.
[BS94] G. Brassard and L. Salvail. Secret-key reconciliation by public discussion. In T. Helleseth, editor, Lecture Notes in Computer Science: Advances in Cryptology - EUROCRYPT'93, Volume
765, pages 410-423, Springer-Verlag, New York, 1994.
[BS98] C. H. Bennett and P. W. Shor. Quantum information theory. IEEE Trans. Inf. Theory, 44(6):2724-42, 1998.
[BST98] H. Barnum, J. A. Smolin, and B. Terhal. Quantum capacity is properly defined without encodings. Phys. Rev. A, 58(5):3496-3501, 1998.
[BT97] B. M. Boghosian and W. Taylor. Simulating quantum mechanics on a quantum computer. ar Xive e-print quantph/9701019, 1997.
[BV97] E. Bernstein and U. Vazirani. Quantum complexity theory. SIAM F. Comput., 26(5):1411-1473, 1997. ar Xive e-print quant-ph/9701001.
[BW92] C. H. Bennett and S. J. Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. Phys. Rev. Lett., 69(20):2881-2884, 1992.
[CAK98] N. J. Cerf, C. Adami, and P. Kwiat. Optical simulation of quantum logic. Phys. Rev. A, 57:R1477, 1998.
[Cav99] C. M. Caves. Quantum error correction and reversible operations. Fournal of Superconductivity, 12(6):707-718, 1999.
[CD96] R. Cleve and D. P. DiVincenzo. Schumacher's quantum data compression as a quantum computation. Phys. Rev. A, 54:2636, 1996. ar Xive e-print quantph/9603009.
[CEMM98] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca. Quantum algorithms revisited. Proc. R. Soc. London A, 454(1969):339354, 1998.
[CFH97] D. G. Cory, A. F. Fahmy, and T. F. Havel. Ensemble quantum computing by NMR spectroscopy. Proc. Nat. Acad. Sci. USA, 94:1634-1639, 1997.
[CGK98] I. L. Chuang, N. Gershenfeld, and M. Kubinec. Experimental implementation of fast quantum searching. Phys. Rev. Lett., 18(15):3408-3411, 1998.
[CGKL98] I. L. Chuang, N. Gershenfeld, M. G. Kubinec, and D. W. Leung. Bulk quantum computation with nuclear-magneticresonance: theory and experiment. Proc. R. Soc. London A, 454(1969):447-467, 1998.

[Che68] P. R. Chernoff. Note on product formulas for operator semigroups. $\mathcal{F}$. Functional Analysis, 2:238-242, 1968.
[Cho75] M.-D. Choi. Completely positive linear maps on complex matrices. Linear Algebra and Its Applications, 10:285-290, 1975.
[CHSH69] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. Phys. Rev. Lett., 49:1804-1807, 1969.
[Chu36] A. Church. An unsolvable problem of elementary number theory. Am. 7. Math. (reprinted in [Dav65]), 58:345, 1936.
[CK81] I. Csiszár and J. Körner. Information Theory: Coding Theorems for Discrete Memoryless Systems. Academic Press, New York, 1981.
[CL83] A. O. Caldeira and A. J. Leggett. Quantum tunnelling in a dissipative system. Ann. Phys., 149(2):374 456, 1983.
[Cla89] M. Clausen. Fast generalized Fourier transforms. Theor. Comput. Sci., 67:5563, 1989.
[Cle99] R. Cleve. The query complexity of order-finding. ar Xive e-print quantph/9911124, 1999.
[CLR90] T. H. Cormen, C. E. Leiserson, and R. L. Rivest. Introduction to Algorithms. MIT Press, Cambridge, Mass., 1990.
[CM97] C. Cachin and U. M. Maurer. Linking information reconciliation and privacy amplification. 7. Cryptology, 10:97-110, 1997.
[CM00] I. L. Chuang and D. Modha. Reversible arithmetic coding for quantum data compression. IEEE Trans. Inf. Theory, 46(3):1104, May 2000.
[CMP ${ }^{+}$98] D. G. Cory, W. Mass, M. Price, E. Knill, R. Laflamme, W. H. Zurek, T. F. Havel, and S. S. Somaroo. Experimental quantum error correction. ar Xive e-print quantph/9802018, 1998.
[CN97] I. L. Chuang and M. A. Nielsen. Prescription for experimental determination of the dynamics of a quantum black box. F. Mod. Opt., 44(11-12):2455-2467, 1997. ar Xive e-print quant-ph/9610001.
[Con72] J. H. Conway. Unpredictable iterations. In Proceedings of the Number Theory Conference, pages 49-52, Boulder, Colorado, 1972.
[Con86] J. H. Conway. Fractran: a simple universal programming language. In T. M. Cover and B. Gopinath, editors, Open Problems in Communication and Computation, pages 4-26, Springer-Verlag, New York, 1986.
[Coo71] S. A. Cook. The complexity of theoremproving procedures. In Proc. 3rd Ann. ACM Symp. on Theory of Computing, pages 151-158, Association for Computing Machinery, New York, 1971.
[Cop94] D. Coppersmith. An approximate Fourier transform useful in quantum factoring. IBM Research Report RC 19642, 1994.
[CPZ96] J. I. Cirac, T. Pellizzari, and P. Zoller. Enforcing coherent evolution in dissipative quantum dynamics. Science, 273:1207, 1996.
[CRSS97] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction and orthogonal geometry. Phys. Rev. Lett., 78:405-8, 1997.
[CRSS98] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction via codes over GF(4). IEEE Trans. Inf. Theory, 44(4):1369-1387, 1998.
[CS96] A. R. Calderbank and P. W. Shor. Good quantum error-correcting codes exist. Phys. Rev. A, 54:1098, 1996. ar Xive e-print quant-ph/9512032.
[CST89] R. A. Campos, B. E. A. Saleh, and M. C. Tiech. Quantum-mechanical lossless beamsplitters: SU(2) symmetry and photon statistics. Phys. Rev. A, 40:1371, 1989.
[CT91] T. M. Cover and J. A. Thomas. Elements of Information Theory. John Wiley and Sons, New York, 1991.
[CTDL77a] C. Cohen-Tannoudji, B. Diu, and F. Laloë. Quantum Mechanics, Vol. I. John

Wiley and Sons, New York, 1977.
[CTDL77b] C. Cohen-Tannoudji, B. Diu, and F. Laloë. Quantum Mechanics, Vol. II. John Wiley and Sons, New York, 1977.
[CVZ+98] I. L. Chuang, L. M. K. Vandersypen, X. L. Zhou, D. W. Leung, and S. Lloyd. Experimental realization of a quantum algorithm. Nature, 393(6681):143-146, 1998.
[CW95] H. F. Chau and F. Wilczek. Simple realization of the Fredkin gate using a series of two-body operators. Phys. Rev. Lett., 75(4):748-50, 1995. ar Xive e-print quant-ph/9503005.
[CY95] I. L. Chuang and Y. Yamamoto. Simple quantum computer. Phys. Rev. A, 52:3489-3496, 1995. ar Xive e-print quant-ph/9505011.
[CZ95] J. I. Cirac and P. Zoller. Quantum computations with cold trapped ions. Phys. Rev. Lett., 74:4091, 1995.
[Dav65] M. D. Davis. The Undecidable. Raven Press, Hewlett, New York, 1965.
[Dav76] E. B. Davies. Quantum Theory of Open Systems. Academic Press, London, 1976.
[DBE95] D. Deutsch, A. Barenco, and A. Ekert. Universality in quantum computation. Proc. R. Soc. London A, 449(1937):669677, 1995.
[Deu83] D. Deutsch. Uncertainty in quantum measurements. Phys. Rev. Lett., 50(9):631-633, 1983.
[Deu85] D. Deutsch. Quantum theory, the Church-Turing Principle and the universal quantum computer. Proc. R. Soc. Lond. A, 400:97, 1985.
[Deu89] D. Deutsch. Quantum computational networks. Proc. R. Soc. London A, 425:73, 1989.
[DG98] L.-M. Duan and G.-C. Guo. Probabilistic cloning and identification of linearly independent quantum states. Phys. Rev. Lett., 80:4999-5002, 1998. arXive eprint quant-ph/9804064.
[DH76] W. Diffie and M. Hellman. New directions in cryptography. IEEE Trans. Inf. Theory, IT-22(6):644-54, 1976.
[DH96] C. Dürr and P. Høyer. A quantum algorithm for finding the minimum. ar Xive e-print quant-ph/9607014, 1996.
[Die82] D. Dieks. Communication by EPR devices. Phys. Lett. A, 92(6):271-272, 1982.
[DiV95a] D. P. DiVincenzo. Quantum computation. Science, 270:255, 1995.
[DiV95b] D. P. DiVincenzo. Two-bit gates are universal for quantum computation. Phys. Rev. A, 51(2):1015-1022, 1995.
[DiV98] D. P. DiVincenzo. Quantum gates and circuits. Proc. R. Soc. London A, 454:261276, 1998.
[DJ92] D. Deutsch and R. Jozsa. Rapid solution of problems by quantum computation. Proc. R. Soc. London A, 439:553, 1992.
[DL98] W. Diffie and S. Landau. Privacy on the Line: the Politics of Wiretapping and Encryption. MIT Press, Cambridge Massachusetts, 1998.
[DMB ${ }^{+}$93] L. Davidovich, A. Maali, M. Brune, J. M. Raimond, and S. Haroche. Phys. Rev. Lett., 71:2360, 1993.
[DR90] P. Diaconis and D. Rockmore. Efficient computation of the Fourier transform on finite groups. 7. Amer. Math. Soc., 3(2):297-332, 1990.
[DRBH87] L. Davidovich, J. M. Raimond, M. Brune, and S. Haroche. Phys. Rev. A, 36:3771, 1987.
[DRBH95] P. Domokos, J. M. Raimond, M. Brune, and S. Haroche. Simple cavity-QED two-bit universal quantum logic gate: The principle and expected performances. Phys. Rev. Lett., 52:3554, 1995.
[DS96] D. P. DiVincenzo and P. W. Shor. Fault-tolerant error correction with efficient quantum codes. Phys. Rev. Lett., 77:3260, 1996.
[DSS98] D. P. DiVincenzo, P. W. Shor, and J. Smolin. Quantum-channel capacities of very noisy channels. Phys. Rev. A, 57(2):830-839, 1998.

[Ear42] S. Earnshaw. On the nature of the molecular forces which regulate the constitution of the luminiferous ether. Trans. Camb. Phil. Soc., 7:97-112, 1842.
[EBW87] R. R. Ernst, G. Bodenhausen, and A. Wokaun. Principles of Nuclear Magnetic Resonance in One and Two Dimensions. Oxford University Press, Oxford, 1987.
[EH99] M. Ettinger and P. Høyer. On quantum algorithms for noncommutative hidden subgroups. In Symposium on Theoretical Aspects in Computer Science. University of Trier, 1999. ar Xive e-print quant-ph/9807029.
[EHK99] M. Ettinger, P. Høyer, and E. Knill. Hidden subgroup states are almost orthogonal. ar Xive e-print quant-ph/9901034, 1999.
[EHPP94] A. K. Ekert, B. Huttner, G. M. Palma, and A . Peres. Eavesdropping on quantum-cryptographical systems. Phys. Rev. A, 50(2):1047-1056, 1994.
[EJ96] A. Ekert and R. Jozsa. Quantum computation and Shor's factoring algorithm. Rev. Mod. Phys., 68:733, 1996.
[EJ98] A. Ekert and R. Jozsa. Quantum algorithms: Entanglement enhanced information processing. Proc. R. Soc. London A, 356(1743):1769-82, Aug. 1998. ar Xive eprint quant-ph/9803072.
[Eke91] A. K. Ekert. Quantum cryptography based on Bell's theorem. Phys. Rev. Lett., 67(6):661-663, 1991.
[EM96] A. Ekert and C. Macchiavello. Error correction in quantum communication. Phys. Rev.Lett., 77:2585, 1996. ar Xive e-print quant-ph/9602022.
[EPR35] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? Phys. Rev., 47:777-780, 1935.
[Eps73] H. Epstein. Commun. Math. Phys., 31:317-325, 1973.
[Fan73] M. Fannes. A continuity property of the entropy density for spin lattice systems. Commun. Math. Phys., 31:291294, 1973.
[FC94] C. A. Fuchs and C. M. Caves. Ensembledependent bounds for accessible information in quantum mechanics. Phys. Rev. Lett., 73(23):3047-3050, 1994.
[Fel68a] W. Feller. An Introduction to Probability Theory and its Applications, Volume 1. Wiley, New York, 1968.
[Fel68b] W. Feller. An Introduction to Probability Theory and its Applications, Volume 2. Wiley, New York, 1968.
[Fey82] R. P. Feynman. Simulating physics with computers. Int. F. Theor. Phys., 21:467, 1982.
[FG98] E. Farhi and S. Gutmann. An analog analogue of a digital quantum computation. Phys. Rev. A, 57(4):2403-2406, 1998. ar Xive e-print quant-ph/9612026.
[FLS65a] R. P. Feynman, R. B. Leighton, and M. Sands. Volume III of The Feynman Lectures on Physics. Addison-Wesley, Reading, Mass., 1965.
[FLS65b] R. P. Feynman, R. B. Leighton, and M. Sands. Volume I of The Feynman Lectures on Physics. Addison-Wesley, Reading, Mass., 1965.
[FM98] M. H. Freedman and D. A. Meyer. Projective plane and planar quantum codes. arXive e-print quant-ph/9810055, 1998.
[FS92] A. Fässler and E. Stiefel. Group Theoretical Methods and Their Applications. Birkhaüser, Boston, 1992.
[FSB $^{+}$98] A. Furusawa, J. L. Sorensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik. Unconditional quantum teleportation. Science, 282:706-709, 1998.
[FT82] E. Fredkin and T. Toffoli. Conservative logic. Int. Y. Theor. Phys., 21(3/4):219253, 1982.
[Fuc96] C. A. Fuchs. Distinguishability and Accessible Information in Quantum Theory. Ph.D. thesis, The University of New Mexico, Albuquerque, NM, 1996. ar Xive e-print quant-ph/9601020.

[Fuc97] C. A. Fuchs. Nonorthogonal quantum states maximize classical information capacity. Phys. Rev. Lett., 79(6):11621165, 1997.
[FvdG99] C. A. Fuchs and J. van de Graaf. Cryptographic distinguishability measures for quantum-mechanical states. IEEE Trans. Inf. Theory, 45(4):1216-1227, 1999.
[Gar91] C. W. Gardiner. Quantum Noise. Springer-Verlag, Berlin, 1991.
[GC97] N. Gershenfeld and I. L. Chuang. Bulk spin resonance quantum computation. Science, 275:350, 1997.
[GC99] D. Gottesman and I. L. Chuang. Quantum teleportation is a universal computational primitive. Nature, 402:390-392, 1999. arXive e-print quant-ph/9908010.
[GJ79] M. R. Garey and D. S. Johnson. Computers and Intractibility. W. H. Freeman and Company, New York, 1979.
[GN96] R. B. Griffiths and C.-S. Niu. Semiclassical Fourier transform for quantum computation. Phys. Rev. Lett., 76(17):3228-3231, 1996. ar Xive e-print quant-ph/9511007.
[Gor64] J. P. Gordon. Noise at optical frequencies; information theory. In P. A. Miles, editor, Quantum Electronics and Coherent Light, Proceedings of the International School of Physics 'Enrico Fermi' XXXI, Academic Press, New York, 1964.
[Got96] D. Gottesman. Class of quantum errorcorrecting codes saturating the quantum Hamming bound. Phys. Rev. A, 54:1862, 1996.
[Got97] D. Gottesman. Stabilizer Codes and Quantum Error Correction. Ph.D. thesis, California Institute of Technology, Pasadena, CA, 1997.
[Got98a] D. Gottesman. Fault-tolerant quantum computation with higher-dimensional systems. arXive e-print quantph/9802007, 1998.
[Got98b] D. Gottesman. Theory of fault-tolerant quantum computation. Phys. Rev. A, 57(1):127-137, 1998. arXive e-print quant-ph/9702029.
[GP10] D. Gottesman and J. Preskill. The Hitchiker's guide to the threshold theorem. Eternally in preparation, 1:1-9120, 2010.
[Gro96] L. Grover. In Proc. 28$^{\text{th}}$ Annual ACM
Symposium on the Theory of Computation, pages 212-219, ACM Press, New York, 1996.
[Gro97] L. K. Grover. Quantum mechanics helps in searching for a needle in a haystack. Phys.Rev.Lett., 79(2):325, 1997. ar Xive e-print quant-ph/9706033.
[Gru99] J. Gruska. Quantum Computing. McGraw-Hill, London, 1999.
[GS92] G. R. Grimmett and D. R. Stirzaker. Probability and Random Processes. Clarendon Press, Oxford, 1992.
[HAD $^{+}$95] R. J. Hughes, D. M. Alde, P. Dyer, G. G. Luther, G. L. Morgan, and M. Schauer. Quantum cryptography. Contemp. Phys., 36(3):149-163, 1995. ar Xive e-print quant-ph/9504002.
[Hal58] P. R. Halmos. Finite-dimensional Vector Spaces. Van Nostrand, Princeton, N.J., 1958.
[Ham89] M. Hammermesh. Group Theory and its Application to Physical Problems. Dover, New York, 1989.
[HGP96] J. L. Hennessey, D. Goldberg, and D. A. Patterson. Computer Architecture: A Quantitative Approach. Academic Press, New York, 1996.
[HHH96] M. Horodecki, P. Horodecki, and R. Horodecki. Separability of mixed states: necessary and sufficient conditions. Phys. Lett. A, 223(1-2):1-8, 1996.
[HHH98] M. Horodecki, P. Horodecki, and R. Horodecki. Mixed-state entanglement and distillation: is there a 'bound' entanglement in nature? Phys. Rev. Lett., 80(24):5239-5242, 1998.
[HHH99a] M. Horodecki, P. Horodecki, and R. Horodecki. General teleportation channel, singlet fraction, and quasidistillation. Phys. Rev. A, 60(3):1888-1898, 1999.
[HHH99b] M. Horodecki, P. Horodecki, and R. Horodecki. Limits for entanglement measures. arXive e-print quantph/9908065, 1999.
[HHH99c] P. Horodecki, M. Horodecki, and R. Horodecki. Bound entanglement can be acti-

vated. Phys. Rev. Lett., 82(5):1056-1059, 1999.
[HJ85] R. A. Horn and C. R. Johnson. Matrix Analysis. Cambridge University Press, Cambridge, 1985.
[HJ91] R. A. Horn and C. R. Johnson. Topics in Matrix Analysis. Cambridge University Press, Cambridge, 1991.
[HJS ${ }ˆ{+}$96] P. Hausladen, R. Jozsa, B. Schumacher, M. Westmoreland, and W. K. Wootters. Classical information capacity of a quantum channel. Phys. Rev. A, 54:1869, 1996.
[HJW93] L. P. Hughston, R. Jozsa, and W. K. Wootters. A complete classification of quantum ensembles having a given density matrix. Phys. Lett. A, 183:14-18, 1993.
[HK69] K.-E. Hellwig and K. Kraus. Pure operations and measurements. Commun. Math. Phys., 11:214-220, 1969.
[HK70] K.-E. Hellwig and K. Kraus. Operations and measurements. II. Commun. Math. Phys., 16:142-147, 1970.
[Hof79] D. R. Hofstadter. Gödel, Escher, Bach: an Eternal Golden Braid. Basic Books, New York, 1979.
[Hol73] A. S. Holevo. Statistical problems in quantum physics. In Gisiro Maruyama and Jurii V. Prokhorov, editors, Proceedings of the Second Fapan-USSR Symposium on Probability Theory, pages 104-119, Springer-Verlag, Berlin, 1973. Lecture Notes in Mathematics, vol. 330.
[Hol79] A. S. Holevo. Capacity of a quantum communications channel. Problems of Inf. Transm., 5(4):247-253, 1979.
[Hol98] A. S. Holevo. The capacity of the quantum channel with general signal states. IEEE Trans. Inf. Theory, 44(1):269273, 1998.
[Hor97] M. Horodecki. Limits for compression of quantum information carried by ensembles of mixed states. Phys. Rev. A, 57:3364-3369, 1997.
[HSM$^+$98] A. G. Huibers, M. Switkes, C. M. Marcus, K. Campman, and A. C. Gossard. Dephasing in open quantum dots. Phys. Rev. Lett., 82:200, 1998.
[HW60] G. H. Hardy and E. M. Wright. An Introduction to the Theory of Numbers, Fourth Edition. Oxford University Press, London, 1960.
[IAB $^+$99 A. Imamoglu, D. D. Awschalom, G. Burkard, D. P. DiVincenzo, D. Loss, M. Sherwin, and A. Small. Quantum information processing using quantum dot spins and cavity qed. Phys. Rev. Lett., 83(20):4204-7, 1999.
[IY94] A. Imamoglu and Y. Yamamoto. Turnstile device for heralded single photons: Coulomb blockade of electron and hole tunneling in quantum confined p-
i-n heterojunctions. Phys. Rev. Lett., 72(2):210-13, 1994.
[Jam98] D. James. The theory of heating of the quantum ground state of trapped ions. ar Xive e-print quant-ph/9804048, 1998.
[Jay57] E. T. Jaynes. Information theory and statistical mechanics. ii. Phys. Rev., 108(2):171-190, 1957.
[JM98] J. A. Jones and M. Mosca. Implementation of a quantum algorithm to solve Deutsch's problem on a nuclear magnetic resonance quantum computer. ar Xive eprint quant-ph/9801027, 1998.
[JMH98] J. A. Jones, M. Mosca, and R. H. Hansen. Implementation of a quantum search algorithm on a nuclear magnetic resonance quantum computer. Nature, 393(6683):344, 1998. arXive e-print quant-ph/9805069.
[Jon94] K. R. W. Jones. Fundamental limits upon the measurement of state vectors. Phys. Rev. A, 50:3682-3699, 1994.
[Joz94] R. Jozsa. Fidelity for mixed quantum states. F. Mod. Opt., 41:2315-2323, 1994.
[Joz97] R. Jozsa. Quantum algorithms and the Fourier transform. arXive e-print quant-ph/9707033, 1997.
[JP99] D. Jonathan and M. B. Plenio. Entanglement-assisted local manipulation of pure states.

Phys. Rev. Lett., 83:3566-3569, 1999.
[JS94] R. Jozsa and B. Schumacher. A new proof of the quantum noiseless coding theorem. 7. Mod. Opt., 41:2343-2349, 1994.
[Kah96] D. Kahn. Codebreakers: the Story of Secret Writing. Scribner, New York, 1996.
[Kan98] B. Kane. A silicon-based nuclear spin quantum computer. Nature, 393:133137, 1998.
[Kar72] R. M. Karp. Reducibility among combinatorial problems. In Complexity of Computer Computations, pages 85-103, Plenum Press, New York, 1972.
[KCL98] E. Knill, I. Chuang, and R. Laflamme. Effective pure states for bulk quantum computation. Phys. Rev. A, 57(5):33483363, 1998. arXive e-print quantph/9706053.
[Kit95] A. Y. Kitaev. Quantum measurements and the Abelian stabilizer problem. ar Xive eprint quant-ph/9511026,, 1995.
[Kit97a] A. Y. Kitaev. Fault-tolerant quantum computation by anyons. ar Xive e-print quant-ph/9707021, 1997.
[Kit97b] A. Y. Kitaev. Quantum computations: algorithms and error correction. Russ. Math. Surv., 52(6):1191-1249, 1997.
[Kit97c] A. Y. Kitaev. Quantum error correction with imperfect gates. In A. S. Holevo O. Hirota and C. M. Caves, editors, Quantum Communication, Computing, and Measurement, pages 181188, Plenum Press, New York, 1997.
[KL51] S. Kullback and R. A. Leibler. On information and sufficiency. Ann. Math. Stat., 22:79-86, 1951.
[KL97] E. Knill and R. Laflamme. A theory of quantum error-correcting codes. Phys. Rev. A, 55:900, 1997. ar Xive e-print quant-ph/9604034.
[KL99] E. Knill and R. Laflamme. Quantum computation and quadratically signed weight enumerators. ar Xive e-print quantph/9909094, 1999.
[Kle31] O. Klein. Z. Phys., 72:767-775, 1931.
[KLV99] E. Knill, R. Laflamme, and L. Viola. Theory of quantum error correction for general noise. ar Xive e-print quantph/9908066, 1999.
[KLZ98a] E. Knill, R. Laflamme, and W. H. Zurek. Resilient quantum computation. Science, 279(5349):342-345, 1998. ar Xive e-print quant-ph/9702058.
[KLZ98b] E. Knill, R. Laflamme, and W. H. Zurek. Resilient quantum computation: error models and thresholds. Proc. R. Soc. London A, 454(1969):365-384, 1998. ar Xive e-print quant-ph/9702058.
[KMSW99] P. G. Kwiat, J. R. Mitchell, P. D. D. Schwindt, and A. G. White. Grover's search algorithm: An optical approach. arXive e-print quantph/9905086, 1999.
[Kni95] E. Knill. Approximating quantum circuits. arXive e-print quantph/9508006, 1995.
[Knu97] D. E. Knuth. Fundamental Algorithms 3rd Edition, Volume 1 of The Art of Computer Programming. AddisonWesley, Reading, Massachusetts, 1997.
[Knu98a] D. E. Knuth. Seminumerical Algorithms 3rd Edition, Volume 2 of The Art of Computer Programming. AddisonWesley, Reading, Massachusetts, 1998.
[Knu98b] D. E. Knuth. Sorting and Searching 2nd Edition, Volume 3 of The Art of Computer Programming. AddisonWesley, Reading, Massachusetts, 1998.
[Kob94] N. Koblitz. A Course in Number The-
ory and Cryptography. Springer-Verlag, New York, 1994.
[KR99] C. King and M. B. Ruskai. Minimal entropy of states emerging from noisy quantum channels. ar Xive e-print quantph/9911079, 1999.
[Kra83] K. Kraus. States, Effects, and Operations: Fundamental Notions of Quantum Theory. Lecture Notes in Physics, Vol. 190. Springer-Verlag, Berlin, 1983.
[Kra87] K. Kraus. Complementary observables and uncertainty relations. Phys. Rev. D, 35(10):3070-3075, 1987.
[KSC +94 P. G. Kwiat, A. M. Steinberg, R. Y. Chiao, P. H. Eberhard, and M. D. Petroff.

Absolute efficiency and time-response measurement of single-photon detectors. Appl. Opt., 33(10):1844-1853, 1994.
[KU91] M. Kitagawa and M. Ueda. Nonlinearinterferometric generation of numberphase correlated Fermion states. Phys. Rev. Lett., 67(14):1852, 1991.
[Lan27] L. Landau. Das dämpfungsproblem in der wellenmechanik. Z. Phys., 45:430-441, 1927.
[Lan61] R. Landauer. Irreversibility and heat generation in the computing process. IBM $\mathcal{F}$. Res. Dev., 5:183, 1961.
[LB99] S. Lloyd and S. Braunstein. Quantum computation over continuous variables. Phys. Rev. Lett., 82:1784-1787, 1999. arXive e-print quant-ph/9810082.
[LBW99] D. A. Lidar, D. A. Bacon, and K. B. Whaley. Concatenating decoherence free subspaces with quantum error correcting codes. Phys. Rev. Lett., 82(22):45564559, 1999.
[LC99] H. Lo and H. F. Chau. Unconditional security of quantum key distribution over arbitrarily long distances. Science, 283:2050-2056, 1999. ar Xive eprint quant-ph/9803006.
[LCW98] D. A. Lidar, I. L. Chuang, and K. B. Whaley. Decoherence-free subspaces for quantum computation. Phys. Rev. Lett., 81(12):2594-2597, 1998.
[LD98] D. Loss and D. P. DiVincenzo. Quantum computation with quantum dots. Phys. Rev. A, 57:120-126, 1998.
[Lec63] Y. Lecerf. Machines de Turing réversibles. Comptes Rendus, 257:25972600, 1963.
[Leo97] U. Leonhardt. Measuring the Quantum
State of Light. Cambridge University Press, New York, 1997.
[Lev73] L. Levin. Universal sorting problems. Probl. Peredaci Inf., 9:115-116, 1973. Original in Russian. English translation in Probl. Inf. Transm. USSR 9:265-266 (1973).
[Lie73] E. H. Lieb. Convex trace functions and the Wigner-Yanase-Dyson conjecture. Ad. Math., 11:267-288, 1973.
[Lie75] E. H. Lieb. Bull. AMS, 81:1-13, 1975.
[Lin75] G. Lindblad. Completely positive maps and entropy inequalities. Commun. Math. Phys., 40:147-151, 1975.
[Lin76] G. Lindblad. On the generators of quantum dynamical semigroups. Commun. Math. Phys., 48:199, 1976.
[Lin91] G. Lindblad. Quantum entropy and quantum measurements. In C. Bendjaballah, O. Hirota, and S. Reynaud, editors, Quantum Aspects of Optical Communications, Lecture Notes in Physics, vol. 378, pages 71-80, Springer-Verlag, Berlin, 1991.
[Lip95] R. Lipton. DNA solution of hard computational problems. Science, 268:542-525, 1995.
[LKF99] N. Linden, E. Kupce, and R. Freeman. NMR quantum logic gates for homonuclear spin systems. ar Xive e-print quant-ph/9907003, 1999.
[LL93] A. K. Lenstra and H. W. Lenstra Jr., editors. The Development of the Number Field Sieve. Springer-Verlag, New York, 1993.
[Llo93] S. Lloyd. A potentially realizable quantum computer. Science, 261:1569, 1993.
[Llo94] S. Lloyd. Necessary and sufficient conditions for quantum computation. F. Mod. Opt., 41(12):2503, 1994.
[Llo95] S. Lloyd. Almost any quantum logic gate is universal. Phys. Rev. Lett., 75(2):346, 1995.
[Llo96] S. Lloyd. Universal quantum simulators. Science, 273:1073, 1996.
[Llo97] S. Lloyd. The capacity of the noisy quantum channel. Phys. Rev. A, 56:1613, 1997.
[LLS75] R. E. Ladner, N. A. Lynch, and A. L. Selman. A comparison of polynomial-time reducibilities. Theor. Comp. Sci., 1:103124, 1975.
[LMPZ96] R. Laflamme, C. Miquel, J.-P. Paz, and W. H. Zurek. Perfect quantum error correction code. Phys. Rev. Lett.,
77:198, 1996. ar Xive e-print quantph/9602019.
[LNCY97] D. W. Leung, M. A. Nielsen, I. L. Chuang, and Y. Yamamoto. Approximate

quantum error correction can lead to better codes. Phys. Rev. A, 56:2567-2573, 1997. ar Xive e-print quant-ph/9704002.
[Lo99] H. Lo. A simple proof of the unconditional security of quantum key distribution. ar Xive e-print quant-ph/9904091, 1999.
[Lom87] J. S. Lomont. Applications of Finite Groups. Dover, New York, 1987.
[Lou73] W. H. Louisell. Quantum Statistical Properties of Radiation. Wiley, New York, 1973.
[LP97] H.-K. Lo and S. Popescu. Concentrating local entanglement by local actions - beyond mean values. ar Xive e-print quantph/9707038, 1997.
[LP99] N. Linden and S. Popescu. Good dynamics versus bad kinematics. Is entanglement needed for quantum computation? arXive e-print quant-ph/9906008, 1999.
[LR68] O. E. Lanford and D. Robinson. Mean entropy of states in quantum-statistical mechanics. F. Math. Phys., 9(7):1120-1125, 1968.
[LR73a] E. H. Lieb and M. B. Ruskai. A fundamental property of quantum-mechanical entropy. Phys. Rev. Lett., 30(10):434436, 1973.
[LR73b] E. H. Lieb and M. B. Ruskai. Proof of the strong subadditivity of quantum mechanical entropy. 7. Math. Phys., 14:19381941, 1973.
[LR90] H. Leff and R. Rex. Maxwell's Demon: Entropy, Information, Computing. Princeton University Press, Princeton, NJ, 1990.
[LS93] L. J. Landau and R. F. Streater. On Birkhoff theorem for doubly stochastic completely positive maps of matrix algebras. Linear Algebra Appl., 193:107127, 1993.
[LS98] S. Lloyd and J. E. Slotine. Analog quantum error correction. Phys. Rev. Lett., 80:4088-4091, 1998.
[LSP98] H.-K. Lo, T. Spiller, and S. Popescu. Quantum information and computation. World Scientific, Singapore, 1998.
[LTV98] M. Li, J. Tromp, and P. Vitanyi. Reversible simulation of irreversible computation by pebble games. Physica *D*, 120:168-176, 1998.
[LV96] M. Li and P. Vitanyi. Reversibility and adiabatic computation: trading time and space for energy. Proc. R. Soc. London A, 452:769-789, 1996. arXive e-print quant-ph/9703022.
[LVZ +99] D. W. Leung, L. M. K. Vandersypen, X. Zhou, M. Sherwood, C. Yannoni, M. Kubinec, and I. L. Chuang. Experimental realization of a two-bit phase damping quantum code. Phys. Rev. A, 60:1924, 1999.
[Man80] Y. Manin. Computable and Uncomputable (in Russian). Sovetskoye Radio, Moscow, 1980.
[Man99] Y. I. Manin. Classical computing, quantum computing, and Shor's factoring algorithm. arXive e-print quantph/9903008, 1999.
[Mau93] U. M. Maurer. Secret key agreement by public discussion from common information. IEEE Trans. Inf. Theory, 39:733742, 1993.
[Max71] J. C. Maxwell. Theory of Heat. Longmans, Green, and Co., London, 1871.
[May98] D. Mayers. Unconditional security in quantum cryptography. ar Xive e-print quant-ph/9802025, 1998.
[ME99] M. Mosca and A. Ekert. The hidden subgroup problem and eigenvalue estimation on a quantum computer. ar Xive e-print quant-ph/9903071, 1999.
[Mer78] R. Merkle. Secure communications over insecure channels. Comm. of the ACM, 21:294-299, 1978.
[Mil76] G. L. Miller. Riemann's hypothesis and tests for primality. 7. Comput. Syst. Sci., 13(3):300-317, 1976.
[Mil89a] G. J. Milburn. Quantum optical Fredkin gate. Phys. Rev. Lett., 62(18):2124, 1989.
[Mil89b] D. A. B. Miller. Optics for low energy communications inside digital processors: quantum detectors, sources, and modulators as efficient impedance converters. Opt. Lett., 14:146, 1989.

[Mil96] G. J. Milburn. A quantum mechanical Maxwell's demon. Unpublished, 1996.
[Mil97] G. J. Milburn. Scrödinger's Machines: the Quantum Technology Reshaping Everyday Life. W. H. Freeman, New York, 1997.
[Mil98] G. J. Milburn. The Feynman Processor: Quantum Entanglement and the Computing Revolution. Perseus Books, Reading, Mass., 1998.
[Min67] M. L. Minsky. Computation: finite and infinite machines. Prentice-Hall, Englewood Cliffs, N.J., 1967.
[MM92] M. Marcus and H. Minc. A Survey of Matrix Theory and Matrix Inequalities. Dover, New York, 1992.
[MMK+95] C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano, and D. J. Wineland. Demonstration of a fundamental quantum logic gate. Phys. Rev. Lett., 75:4714, 1995.
[MO79] A. W. Marshall and I. Olkin. Inequalities: Theory of Majorization and its Applications. Academic Press, New York, 1979.
[MOL*99] J. E. Mooij, T. P. Orlando, L. Levitov, L. Tian, C. H. van der Waal, and S. Lloyd. Josephson persistent-current qubit. Science, 285:1036-1039, 1999.
[Mor98] T. Mor. No-cloning of orthogonal states in composite systems. Phys. Rev. Lett., 80:3137-3140, 1998.
[Mos98] M. Mosca. Quantum searching, counting and amplitude amplification by eigenvector analysis. In R. Freivalds, editor, Proceedings of International Workshop on Randomized Algorithms, pages 90-100, 1998.
[Mos99] M. Mosca. Quantum Computer Algorithms. Ph.D. thesis, University of Oxford, 1999.
[MR95] R. Motwani and P. Raghavan. Randomized Algorithms. Cambridge University Press, Cambridge, 1995.
[MS77] F. J. MacWilliams and N. J. A. Sloane. The Theory of Error-correcting Codes. North-Holland, Amsterdam, 1977.
[MU88] H. Maassen and J. H. B. Uffink. Generalized entropic uncertainty relations. Phys. Rev. Lett., 60(12):1103-1106, 1988.
[MvOV96] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. Handbook of Applied Cryptography. CRC Press, 1996.
[MWKZ96] K. Mattle, H. Weinfurter, P. G. Kwiat, and A . Zeilinger. Dense coding in experimental quantum communication. Phys. Rev. Lett., 76(25):4656-4659, 1996.
[MZG96] A. Muller, H. Zbinden, and N. Gisin. Quantum cryptography over 23 km in installed under-lake telecom fibre. Europhys. Lett., 33:334-339, 1996.
[NC97] M. A. Nielsen and C. M. Caves. Reversible quantum operations and their application to teleportation. Phys. Rev. A, 55(4):2547-2556, 1997.
[NCSB98] M. A. Nielsen, C. M. Caves, B. Schumacher, and H. Barnum. Informationtheoretic approach to quantum error correction and reversible measurement. Proc. R. Soc. London A, 454(1969):277-304, 1998.
[Nie98] M. A. Nielsen. Quantum Information Theory. Ph.D. thesis, University of New Mexico, 1998.
[Nie99a] M. A. Nielsen. Conditions for a class of entanglement transformations. Phys. Rev. Lett., 83(2):436-439, 1999.
[Nie99b] M. A. Nielsen. Probability distributions consistent with a mixed state. ar Xive *e* print quant-ph/9909020, 1999.
[NKL98] M. A. Nielsen, E. Knill, and R. Laflamme. Complete quantum teleportation using nuclear magnetic resonance. Nature, 396(6706):52-55, 1998.
[NPT99] Y. Nakamura, Y. A. Pashkin, and J. S. Tsai. Coherent control of macroscopic quantum states in a single-cooperpair box. Nature, 398:786-788, 1999.
[OP93] M. Ohya and D. Petz. Quantum Entropy and Its Use. Springer-Verlag, Berlin, 1993.
[Pai82] A. Pais. Subtle is the Lord: The Science and the Life of Albert Einstein. Oxford

University Press, Oxford, 1982.
[Pai86] A. Pais. Inward Bound: Of Matter and Forces in the Physical World. Oxford University Press, Oxford, 1986.
[Pai91] A. Pais. Niels Bohr's Times: In Physics, Philosophy, and Polity. Oxford University Press, Oxford, 1991.
[Pap94] C. M. Papadimitriou. Computational Complexity. Addison-Wesley, Reading, Massachusetts, 1994.
[Pat92] R. Paturi. On the degree of polynomials that approximate symmetric Boolean functions (preliminary version). Proc. 24th Ann. ACM Symp. on Theory of Computing (STOC '92), pages 468474, 1992.
[PCZ97] J. F. Poyatos, J. I. Cirac, and P. Zoller. Complete characterization of a quantum process: the two-bit quantum gate. Phys. Rev. Lett., 78(2):390-393, 1997.
[PD99] P. M. Platzman and M. I. Dykman. Quantum computing with electrons floating on liquid helium. Science, 284:1967, 1999.
[Pen89] R. Penrose. The Emperor's New Mind. Oxford University Press, Oxford, 1989.
[Per52] S. Perlis. Theory of Matrices. AddisonWesley, Reading, Mass., 1952.
[Per88] A. Peres. How to differentiate between non-orthogonal states. Phys. Lett. A, 128:19, 1988.
[Per93] A. Peres. Quantum Theory: Concepts and Methods. Kluwer Academic, Dordrecht, 1993.
[Per95] A. Peres. Higher order schmidt decompositions. Phys. Lett. A, 202:16-17, 1995.
[Pet86] D. Petz. Quasi-entropies for finite quantum systems. Rep. Math. Phys., 23(1):57-65, 1986.
[Phy92] Physics Today Editor. Quantum cryptography defies eavesdropping. Physics Today, page 21, November 1992.
[PK96] M. B. Plenio and P. L. Knight. Realistic lower bounds for the factorization time of large numbers on a quantum computer. Phys. Rev. A, 53:2986-2990, 1996.
[PK98] M. B. Plenio and P. L. Knight. The quantum-jump approach to dissipative dynamics in quantum optics. Rev. Mod. Phys., 70(1):101-144, 1998.
[Pop75] R. P. Poplavskii. Thermodynamical models of information processing (in Russian). Usp. Fiz. Nauk, 115(3):465-501, 1975.
[PRB98] M. Pueschel, M. Roetteler, and T. Beth. Fast quantum Fourier transforms for a class of non-abelian groups. ar Xive *e* print quant-ph/9807064, 1998.
[Pre97] J. Preskill. Fault-tolerant quantum computation. arXive e-print quantph/9712048, 1997.
[Pre98a] J. Preskill. Fault-tolerant quantum computation. In H.-K. Lo, T. Spiller, and S. Popescu, editors, Quantum information and computation. World Scientific, Singapore, 1998.
[Pre98b] J. Preskill. Physics 229: Advanced Mathematical Methods of Physics - Quantum Computation and Information. California Institute of Technology, 1998. URL: http://www.theory.caltech.edu/people/preskill/ph229/
[Pre98c] J. Preskill. Reliable quantum computers. Proc. R. Soc. London A, 454(1969):385410, 1998.
[Rab80] M. O. Rabin. Probabilistic algorithm for testing primality. I. Number Theory, 12:128-138, 1980.
[Rah99] H. Z. Rahim. Richard Feynman and Bill Gates: an imaginary encounter. 1999. URL: http://www.trnsoft.com/features/1rfbg.htm
[Rai98] E. M. Rains. Quantum weight enumerators. IEEE Trans. Inf. Theory, 44(4):1388-1394, 1998.
[Rai99a] E. M. Rains. Monotonicity of the quantum linear programming bound. IEEE Trans. Inf. Theory, 45(7):2489-2492, 1999.

[Rai99b] E. M. Rains. Nonbinary quantum codes. IEEE Trans. Inf. Theory, 45(6):18271832, 1999.
[Rai99c] E. M. Rains. Quantum shadow enumerators. IEEE Trans. Inf. Theory, 45(7):2361-2366, 1999.
[RB98] M. Roetteler and T. Beth. Polynomialtime solution to the hidden subgroup problem for a class of non-abelian groups. arXive e-print quant-ph/9812070, 1998.
[Res81] A. Ressler. The Design of a Conservative Logic Computer and A Graphical Editor Simulator. Master's thesis, Massachusetts Institute of Technology, 1981.
[RHSS97] E. M. Rains, R. H. Hardin, P. W. Shor, and N. J. A. Sloane. Nonadditive quantum code. Phys. Rev. Lett., 79(5):953954, 1997.
[Roy96] A. Royer. Reduced dynamics with initial correlations, and time-dependent environment and Hamiltonians. Phys. Rev. Lett., 77(16):3272-3275, 1996.
[RR67] D. W. Robinson and D. Ruelle. Commun. Math. Phys., 5:288, 1967.
[RSA78] R. L. Rivest, A. Shamir, and L. M. Adleman. A method of obtaining digital signatures and public-key cryptosystems. Comm. ACM, 21(2):120-126, 1978.
[Rus94] M. B. Ruskai. Beyond strong subadditivity: improved bounds on the contraction of generalized relative entropy. Rev. Math. Phys., 6(5A):1147-1161, 1994.
[RWvD84] S. Ramo, J. R. Whinnery, and T. van Duzer. Fields and waves in communication electronics. Wiley, New York, 1984.
[RZBB94] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani. Experimental realization of any discrete unitary operator. Phys. Rev. Lett., 73(1):58-61, 1994.
[Sak95] J. J. Sakurai. Modern Quantum Mechanics. Addison-Wesley, Reading, Mass., 1995.
[SC99] R. Schack and C. M. Caves. Classical model for bulk-ensemble NMR quantum computation. Phys. Rev. A, 60(6):43544362, 1999.
[Sch06] E. Schmidt. Zur theorie der linearen und nichtlinearen integralgleighungen. Math. Annalen., 63:433-476, 1906.
[Sch36] E. Schrödinger. Probability relations between separated systems. Proc. Cambridge Philos. Soc., 32:446-452, 1936.
[Sch95] B. Schumacher. Quantum coding. Phys. Rev. A, 51:2738-2747, 1995.
[Sch96a] B. Schneier. Applied Cryptography. John Wiley and Sons, New York, 1996.
[Sch96b] B. W. Schumacher. Sending entanglement through noisy quantum channels. Phys. Rev. A, 54:2614, 1996.
[Sha48] C. E. Shannon. A mathematical theory of communication. Bell System Tech. F., 27:379-423, 623-656, 1948.
[Sho94] P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In Proceedings, 35$^{\text{th}}$ Annual Symposium on Foundations of Computer Science, IEEE Press, Los Alamitos, CA, 1994.
[Sho95] P. Shor. Scheme for reducing decoherence in quantum computer memory. Phys. Rev. A, 52:2493, 1995.
[Sho96] P. W. Shor. Fault-tolerant quantum computation. In Proceedings, 37$^{\text{th}}$ Annual Symposium on Fundamentals of Computer Science, pages 56-65, IEEE Press, Los Alamitos, CA, 1996.
[Sho97] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM 7. Comp., 26(5):1484-1509, 1997.
[Sim79] B. Simon. Trace Ideals and Their Applications. Cambridge University Press, Cambridge, 1979.
[Sim94] D. Simon. On the power of quantum computation. In Proceedings, 35th Annual Symposium on Foundations of Computer Science, pages 116-123, IEEE Press, Los Alamitos, CA, 1994.
[Sim97] D. R. Simon. On the power of quantum computation. SIAM F. Comput.,

26(5):1474-1483, 1997.
[SL97] P. W. Shor and R. Laflamme. Quantum analog of the MacWilliams identities for classical coding theory. Phys. Rev. Lett., 78(8):1600-1602, 1997.
[SL98] D. Shasha and C. Lazere. Out of Their Minds: The Lives and Discoveries of 15 Great Computer Scientists. SpringerVerlag, New York, 1998.
[Sle74] D. Slepian, editor. Keys Papers in the Development of Information Theory. IEEE Press, New York, 1974.
[Sli96] C. P. Slichter. Principles of Magnetic Resonance. Springer, Berlin, 1996.
[SN96] B. W. Schumacher and M. A. Nielsen. Quantum data processing and error correction. Phys. Rev. A, 54(4):2629, 1996. ar Xive e-print quant-ph/9604022.
[SP00] P. W. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. ar Xive e-print quantph/0003004, 2000.
[SS76] R. Solovay and V. Strassen. A fast MonteCarlo test for primality. SIAM 7. Comput., 6:84-85, 1976.
[SS96] P. W. Shor and J. A. Smolin. Quantum error-correcting codes need not completely reveal the error syndrome. ar Xive e-print quant-ph/9604006, 1996.
[SS99] A. T. Sornborger and E. D. Stewart. Higher order methods for simulations on quantum computers. Phys. Rev. A, 60(3):1956-1965, 1999. ar Xive e-print quant-ph/9903055.
[ST91] B. E. A. Saleh and M. C. Teich. Fundamentals of Photonics. Wiley, NY, 1991.
[Ste96a] A. M. Steane. Error correcting codes in quantum theory. Phys. Rev. Lett., 77:793, 1996.
[Ste96b] A. M. Steane. Multiple particle interference and quantum error correction. Proc. R. Soc. London A, 452:2551-76, 1996.
[Ste97] A. Steane. The ion-trap quantum information processor. Appl. Phys. B-Lasers and Optics, 64(6):623-642, 1997.
[Ste99] A. M. Steane. Efficient fault-tolerant quantum computing. Nature, 399:124126, May 1999.
[STH ${ }ˆ{+}$99] S. Somaroo, C. H. Tseng, T. F. Havel, R. Laflamme, and D. G. Cory. Quantum simulations on a quantum computer. Phys. Rev. Lett., 82:5381-5384, 1999.
[Str76] G. Strang. Linear Algebra and Its Applications. Academic Press, New York, 1976.
[SV99] L. J. Schulman and U. Vazirani. Molecular scale heat engines and scalable quantum computation. Proc. 31st Ann. ACM Symp. on Theory of Computing (STOC '99), pages 322-329, 1999.
[SW49] C. E. Shannon and W. Weaver. The Mathematical Theory of Communication. University of Illinois Press, Urbana, 1949.
[SW93] N. J. A. Sloane and A. D. Wyner, editors. Claude Elwood Shannon: Collected Papers. IEEE Press, New York, 1993.
[SW97] B. Schumacher and M. D. Westmoreland. Sending classical information via
noisy quantum channels. Phys. Rev. A, 56(1):131-138, 1997.
[SW98] B. Schumacher and M. D. Westmoreland. Quantum privacy and quantum coherence. Phys. Rev. Lett., 80(25):56955697, 1998.
[SWW96] B. W. Schumacher, M. Westmoreland, and W. K. Wootters. Limitation on the amount of accessible information in a quantum channel. Phys. Rev. Lett., 76:3453, 1996.
[Szi29] L. Szilard. Uber die entropieverminderung in einen thermodynamischen system bei eingriffen intelligenter wesen. *Z*. Phys., 53:840-856, 1929.
[TD98] B. M. Terhal and D. P. DiVincenzo. The problem of equilibration and the computation of correlation functions on a quantum computer. ar Xive e-print quantph/9810063, 1998.
[THL $^{+}$95] Q. A. Turchette, C. J. Hood, W. Lange, H. Mabuchi, and H. J. Kimble. Measurement of conditional phase shifts for quantum logic. Phys. Rev. Lett., 75:4710, 1995.

[Tro59] H. F. Trotter. On the product of semigroups of operators. Proc. Am. Math. Soc., 10:545-551, 1959.
[Tsi80] B. S. Tsirelson. Quantum generalizations of Bell's inequality. Lett. Math. Phys., 4:93, 1980.
[Tur36] A. M. Turing. On computable numbers, with an application to the Entscheidungsproblem. Proc. Lond. Math. Soc. 2 (reprinted in [Dav65]), 42:230, 1936.
[Tur97] Q. A. Turchette. Quantum optics with single atoms and single photons. Ph.D. thesis, California Institute of Technology, Pasadena, California, 1997.
[Uhl70] A. Uhlmann. On the Shannon entropy and related functionals on convex sets. Rep. Math. Phys., 1(2):147-159, 1970.
[Uh171] A. Uhlmann. Sätze über dichtematrizen. Wiss. Z. Karl-Marx-Univ. Leipzig, 20:633-637, 1971.
[Uhl72] A. Uhlmann. Endlich-dimensionale dichtematrizen I. Wiss. Z. Karl-MarxUniv. Leipzig, 21:421-452, 1972.
[Uhl73] A. Uhlmann. Endlich-dimensionale dichtematrizen II. Wiss. Z. Karl-MarxUniv. Leipzig, 22:139-177, 1973.
[Uhl76] A. Uhlmann. The 'transition probability' in the state space of a *-algebra. Rep. Math. Phys., 9:273-279, 1976.
[Uhl77] A. Uhlmann. Relative entropy and the
Wigner-Yanase-Dyson-Lieb concavity in an interpolation theory. Commun. Math. Phys., 54:21-32, 1977.
[Ume62] H. Umegaki. Ködai Math. Sem. Rep., 14:59-85, 1962.
[Vai94] L. Vaidman. Teleportation of quantum states. Phys. Rev. A, 49(2):1473-6, 1994.
[van98a] W. van Dam. Quantum oracle interrogation: getting all information for half the price. In Proceedings of the 39$^{\text{th}}$ FOCS, 1998. arXive e-print quantph/9805006.
[van98b] S. J. van Enk. No-cloning and superluminal signaling. ar Xive e-print quantph/9803030, 1998.
[Ved99] V. Vedral. Landauer's erasure, error correction and entanglement. ar Xive *e* print quant-ph/9903049, 1999.
[Vid98] G. Vidal. Entanglement monotones. arXive e-print quant-ph/9807077, 1998.
[Vid99] G. Vidal. Entanglement of pure states for a single copy. Phys. Rev. Lett., 83(5):1046-1049, 1999.
[von27] J. von Neumann. Göttinger Nachrichten, page 245, 1927.
[von56] J. von Neumann. Probabilistic logics and the synthesis of reliable organisms from unreliable components. In Automata Studies, pages 329-378, Princeton University Press, Princeton, NJ, 1956.
[von66] J. von Neumann. Fourth University of Illinois lecture. In A. W. Burks, editor, Theory of Self-Reproducing Automata, page 66, University of Illinois Press, Urbana, 1966.
[VP98] V. Vedral and M. B. Plenio. Entanglement measures and purification procedures. Phys. Rev. A, 57(3):1619-1633, 1998.
[VR89] K. Vogel and H. Risken. Determination of quasiprobability distributions in terms of probability distributions for the rotated quadrature phase. Phys. Rev. A, 40(5):2847-2849, 1989.
[VYSC99] L. M. K. Vandersypen, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang. Realization of effective pure states for bulk quantum computation. Phys. Rev. Lett., 83:3085-3088, 1999.
[VYW ${ }^{+}$99] R. Vrijen, E. Yablonovitch, K. Wang, H. W. Jiang, A. Balandin, V. Roychowdhury, T. Mor, and D. DiVincenzo. Electron spin resonance transistors for quantum computing in silicon-germanium het-
erostructures. arXive e-print quantph/9905096, 1999.

[War97] W. Warren. The usefulness of NMR quantum computing. Science, 277(5332):1688, 1997.
[Wat99] J. Watrous. PSPACE has 2-round quantum interactive proof systems. ar Xive eprint cs/9901015, 1999.
[WC67] S. Winograd and J. D. Cowan. Reliable Computation in the Presence of Noise. MIT Press, Cambridge, MA, 1967.
[Weh78] A. Wehrl. General properties of entropy. Rev. Mod. Phys., 50:221, 1978.
[Wel88] D. J. A. Welsh. Codes and Cryptography. Oxford University Press, New York, 1988.
[Wie] S. Wiesner. Unpublished manuscript, circa 1969, appeared as [Wie83].
[Wie83] S. Wiesner. Conjugate coding. SIGACT News, 15:77, 1983.
[Wie96] S. Wiesner. Simulations of manybody quantum systems by a quantum computer. arXive e-print quantph/9603028, 1996.
[Wi191] D. Williams. Probability with Martingales. Cambridge University Press, Cambridge, 1991.
[Win98] E. Winfree. Algorithmic Self-Assembly of DNA. Ph.D. thesis, California Institute of Technology, Pasadena, California, 1998.
[WMI ${ }^{+}$98] D. J. Wineland, C. Monroe, W. M. Itano, D. Leibfried, B. E. King, and D. M. Meekhof. Experimental issues in coherent quantum-state manipulation of trapped atomic ions. 7. Res. Natl. Inst. Stand. Tech., 103:259, 1998.
[WS98] M. D. Westmoreland and B. Schumacher. Quantum entanglement and the nonexistence of superluminal signals. ar Xive e-print quant-ph/9801014, 1998.
[WY63] E. P. Wigner and M. M. Yanase. Proc. Natl. Acad. Sci. (U S.A.), 49:910-918, 1963.
[WY90] K. Watanabe and Y. Yamamoto. Limits on tradeoffs between third-order optical nonlinearity, absorption loss, and pulse duration in self-induced transparency and real excitation. Phys. Rev. A, 42(3):1699702, 1990.
[WZ82] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. Nature, 299:802-803, 1982.
[Yao93] A. C. Yao. Quantum circuit complexity. Proc. of the 34th Ann. IEEE Symp. on Foundations of Computer Science, pages 352-361, 1993.
[YK95] S. Younis and T. Knight. Non dissipative rail drivers for adiabatic circuits. In Proceedings, Sixteenth Conference on Advanced Research in VLSI 1995, pages 404-14, IEEE Computer Society Press, Los Alamitos, CA, 1995.
[YKI88] Y. Yamamoto, M. Kitagawa, and K. Igeta. In Proc. 3rd Asia-Pacific Phys. Conf., World Scientific, Singapore, 1988.
[YO93] H. P. Yuen and M. Ozawa. Ultimate information carrying limit of quantum systems. Physical Review Letters, 70:363366, 1993.
[YY99] F. Yamaguchi and Y. Yamamoto. Crystal lattice quantum computer. Appl. Phys. *A*, pages 1-8, 1999.
[Zal98] C. Zalka. Simulating quantum systems on a quantum computer. Proc. R. Soc. London A, 454(1969):313-322, 1998.
[Zal99] C. Zalka. Grover's quantum searching algorithm is optimal. Phys. Rev. A, 60(4):2746-2751, 1999.
[Zan99] P. Zanardi. Stabilizing quantum information. ar Xive e-print quant-ph/9910016, 1999.
[ZG97] P. Zoller and C. W. Gardiner. Quantum noise in quantum optics: the stochastic Schrödinger equation. In S. Reynaud, E. Giacobino, and J. Zinn-Justin, editors, Quantum Fluctuations: Les Houches Summer School LXIII, Elsevier, Amsterdam, 1997.
[ZHSL99] K. Zyczkowski, P. Horodecki, A. Sanpera, and M. Lewenstein. Volume of the set of separable states. Phys. Rev. A, 58(2):883892, 1999.
[ZL96] W. H. Zurek and R. Laflamme. Quantum logical operations on encoded qubits. Phys.

Rev. Lett., 77(22):4683-4686, 1996.
[ZLC00] X. Zhou, D. W. Leung, and I. L. Chuang. Quantum logic gate constructions with one-bit "teleportation". ar Xive e-print quant-ph/0002039, 2000.
[ZR98] P. Zanardi and M. Rasetti. Noiseless quantum codes. Phys. Rev. Lett., 79(17):3306-3309, 1998.
[Zur89] W. H. Zurek. Thermodynamic cost of computation, algorithmic complexity and the information metric. Nature, 341:119, 1989.
[Zur91] W. H. Zurek. Decoherence and the transition from quantum to classical. Phys. Today, October 1991.

Literature from Quantum Polarization States of Photon by Filippov

1. Aspect A., Dalibard J., Roger G. Experimental test of Bell's inequalities using time-varying analyzers // Physical Review Letters. - 1982. - V. 49. - P. 1804.

2. Bennett C.H., Brassard G. Quantum cryptography: Public key distribution and coin tossing // Proceedings of IEEE International Conference on Computers, Systems and Signal Processing. - 1984. V. 175.-P. 8.

3. Bennett C., Wiesner S. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states // Physical Review Letters. - 1992. - V. 69. - P. 2881.

4. Bennett C. H., Brassard G., Crépeau C., Jozsa R., Peres A., Wootters W. K. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels / / Physical Review Letters. - 1993. - V. 70. - P. 1895.

5. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация. - М.: Мир, 2006.

6. Фейнман Р., Лейтон Р., Сэндс М. Фейнмановские лекции по физике. Вып. 3. Излучение. Волны. Кванты. - М.: Либроком, 2014.

7. Фейнман Р., Лейтон Р., Сэндс М. Фейнмановские лекции по физике. Вып. 8, 9: Квантовая механика. - М.: Либроком, 2014.

8. Ландау Л. Д., Лифшиц Е. М. Курс теоретической физики. Т. 2. Теория поля. - М.: Физматлит, 2012.

9. Липкин Г. Квантовая механика. - М.: Мир, 1977.

10. Peres A. Separability criterion for density matrices // Physical Review Letters. - 1996. - V. 77. - P. 1413.

11. Horodecki M., Horodecki P., Horodecki R. Separability of mixed states: necessary and sufficient conditions // Physics Letters A. - 1996. - V. 223. - P. 1.

12. Filippov S. N., Man'ko V. I. Geometrical interpretation of density matrix: mixed and entangled states // Journal of Russian Laser Research. - 2008. - V. 29. - P. 564.

13. Бауместер Д., Экерт А., Цайлингер А. Физика квантовой информации. М.: Постмаркет, 2002.

14. Schuck C., Huber G., Kurtsiefer C., Weinfurter H. Complete deterministic linear optics Bell state analysis // Physical Review Letters. - 2006. - V. 96. - P. 190501.

15. Фейнман Р. Статистическая механика. - М.: Мир, 1978.

16. Söderholm J., Björk G., Klimov A. B., Sánchez-Soto L. L., Leuchs G. Quantum polarization characterization and tomography // New Journal of Physics. - 2012. - V. 14. - P. 115014.

17. Холево А. С. Квантовые системы, каналы, информация. - М.: МЦНМО, 2010.

18. Gisin N., Ribordy G., Tittel W., Zbinden H. Quantum cryptography // Reviews of Modern Physics. - 2002. - V. 74. - P. 145.

19. Filippov S. N., Rybár T., Ziman M. Local two-qubit entanglementannihilating channels // Physical Review A. - 2012. - V. 85. P. 012303 .

From The Physical Implementation of Quantum Computation by DiVincenzo

References

[1] J.I. Cirac and P. Zoller, Phys. Rev. Lett. **74**, 4091 (1995); T. Pellizzari, S.A. Gardiner, J.I. Cirac, and P. Zoller, Phys. Rev. Lett. **75**, 3788 (1995); C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano, and D. J. Wineland, "Demonstration of a fundamental quantum logic gate," Phys. Rev. Lett. **75**, 4714 (1995); A. Sorensen and K. Molmer, Phys. Rev. Lett. **82**, 1971 (1999); S. Schneider, D. F. V. James, and G. J. Milburn, "Method of quantum computation with 'hot' trapped ions," quant-ph/9808012.

[2] Q. A. Turchette, C. J. Hood, W. Lange, H. Mabuchi, and H. J. Kimble, "Measurement of conditional phase shifts for quantum logic," Phys. Rev. Lett. **75**, 4710 (1995); A. Imamoglu, D. D. Awschalom, G. Burkard, D. P. DiVincenzo, D. Loss, M. Sherwin, and A. Small, Phys. Rev. Lett. **83**, 4204 (1999) (quant-ph/9904096).

[3] N. Gershenfeld and I. Chuang, Science **275**, 350 (1997); D. Cory, A. Fahmy, and T. Havel, Proc. Nat. Acad. Sci. **94** (5), 1634 (1997).

[4] B. Kane, Nature **393**, 133 (1998); R. Vrijen *et al.*, "Electron spin resonance transistors for quantum computing in silicon-germanium heterostructures," Phys. Rev. A, in press (quant-ph/9905096).

[5] D. Averin, Solid State Commun. **105**, 659 (1998); A. Shnirman, G. Schön, and Z. Hermin, Phys. Rev. Lett. **79**, 2371 (1997); J. E. Mooij, T. P. Orlando, L. Levitov, L. Tian, C. H. van der Wal, and S. Lloyd, Science **285**, 1036 (1999).

[6] P. M. Platzman and M. I. Dykman, Science **284**, 1967 (1999).

[7] D. Loss and D. P. DiVincenzo, Phys. Rev. A **57**, 120 (1998) (cond-mat/9701055); M. Sherwin, A. Imamoglu, and T. Montroy, "Quantum computation with quantum dots and terahertz cavity quantum electrodynamics," Phys. Rev. A **60**, 3508 (1999) (quant-ph/9903065); T. Tanamoto, Phys. Rev. A **61**, 022305 (2000) (quant-ph/9902031).

[8] D. Deutsch Proc. R. Soc. London A **400**, 97 (1985); **425**, 73 (1989).

[9] R. P. Feynman, Int. J. Theor. Phys. **21**, 467 (1982); Found. Phys. **16**, 507 (1986). See also *Feynman Lectures on Computation*, eds. A. J. G. Hey and R. Allen (Perseus Press, 1996).

[10] R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf, "Quantum lower bounds by polynomials," *Proc. of the 39th Annual Symposium on the Foundations of Computer Science* (IEEE Press, Los Alamitos, 1998), p. 352; quant-ph/9802049.

[11] Y. Ozhigov, "Quantum computer cannot speed up iterated applications of a black box," quant-ph/9712051; B. Terhal, PhD Thesis, University of Amsterdam, 1999.

[12] L. K. Grover, "Quantum mechanics helps in searching for a needle in a haystack," Phys. Rev. Lett. **79**, 325 (1997).

[13] P. W. Shor, "Polynomial time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM J. Comput. **26**, 1484 (1997), and references therein.

[14] D. P. DiVincenzo and D. Loss, "Quantum Computers and Quantum Coherence," J. Magnetism Magn. Matl. **200**, 202-218 (1999).

[15] R. Cleve and H. Buhrman, Phys. Rev. A **56**, 1201 (1997).

[16] H. Buhrman, R. Cleve, and A. Wigderson, "Quantum vs. Classical Communication and Computation," in *Proc. of the 30th Ann. ACM Symp. on the Theory of Computing* (ACM Press, 1998), p. 63; eprint quant-ph/9802040.

[17] A. Ambainis, L. Schulman, A. Ta-Shma, U. Vazirani, and A. Wigderson, "The quantum communication complexity of sampling," in *Proc. of the 39th Annual Symposium on the Foundations of Computer Science* (IEEE Press, Los Alamitos, 1998); see http://www.icsi.berkeley.edu/~amnon/Papers/qcc.ps.

[18] C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.

[19] D. A. Meyer, "Quantum strategies," Phys. Rev. Lett. **82**, 1052 (1999) (quant-ph/9804010); J. Eisert, M. Wilkens, and M. Lewenstein, "Quantum games and quantum strategies," Phys. Rev. Lett. **83**, 3077 (1999) (quant-ph/9806088); L. Goldenberg, L. Vaidman, and S. Wiesner, "Quantum gambling," Phys. Rev. Lett. **82**, 3356 (1999) (quant-ph/9808001).

[20] A. M. Steane and W. van Dam, "Physicists Triumph at 'Guess my Number' ", Physics Today **53** (2), 35-39 (2000).

[21] D. Aharonov, "Quantum Computation," in *Annual Reviews of Computational Physics, vol. VI* (ed. Dietrich Stauffer, World Scientific, Singapore, 1998) (quant-ph/9812037).

[22] R. Cleve, "An Introduction to Quantum Complexity Theory," to appear in *Collected Papers on Quantum Computation and Quantum Information Theory* (eds. C. Macchiavello, G. M. Palma, and A. Zeilinger, World Scientific, 2000) (quant-ph/9906111).

[23] C. H. Bennett, Physics Today **48** (10), 24 (1995); D. P. DiVincenzo, Science **270**, 255 (1995); D. P. DiVincenzo, Proc. R. Soc. London A **454**, 261 (1998) (and quant-ph/9705009); A. Barenco, Contemp. Phys. **37**, 375 (1996); A. Steane, Rep. Prog. Phys. **61**, 117 (1998); C. H. Bennett and P. W. Shor, IEEE Trans. Info. Theory **44**, 2724 (1998).

[24] D. P. DiVincenzo, in *Mesoscopic Electron Transport*, eds. L. Sohn, L. Kouwenhoven, and G. Schön (Vol. 345, NATO ASI Series E, Kluwer, 1997), p. 657 (cond-mat/9612126); D. P. DiVincenzo and D. Loss, Superlattices and Microstructures **23**, 419 (1998) (cond-mat/9710259); D. P. DiVincenzo and D. Loss, J. Magn. Mag. Matl. **200**, 202 (1999) (cond-mat/9901137).

[25] B. Schumacher, Phys. Rev. A **54**, 2614 (1996).

[26] G. K. Brennen, C. M. Caves, P. S. Jessen, and I. H. Deutsch, Phys. Rev. Lett. **82**, 1060 (1999).

[27] D. Jaksch, H. J. Briegel, I. J. Cirac, C. Gardiner, and P. Zoller, Phys. Rev. Lett. **82**, 1975 (1999).

[28] I am grateful to R. Schoelkopf and M. Devoret for clarifying discussion on these points.

[29] M. B. Plenio and P. L. Knight, Phys. Rev. A **53**, 2986 (1996).

[30] M. B. Plenio and P. L. Knight, Proc. Roy. Soc. Lond. **A453**, 2017-2041 (1997).

[31] J. Preskill, Proc. R. Soc. Lond A **454**, 385 (1998) (quant-ph/9705031).

[32] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000); see also M. A. Nielsen, C. M. Caves, B. Schumacher, and H. Barnum, Proc. R. Soc. Lond. A **454**, 277-304 (1998) (quant-ph/9706064).

[33] P. Shor, Phys. Rev. A **52**, 2493 (1995); A. M. Steane, Phys. Rev. Lett. **77**, 793-797 (1996).

[34] P. Shor, in *Proceedings of the 37th Symposium on the Foundations of Computer Science* (IEEE Press, Los Alamitos, CA, 1996) (quant-ph/9605011); D. Aharonov and M. Ben-Or, in *Proceedings of the 29th Annual ACM Symposium on the Theory of Computing* (ACM Press, New York, 1997) (quant-ph/9611025); E. Knill, R. Laflamme, and W. Zurek, Science **279**, 342 (1998). These results are reviewed in [31].

[35] D. P. DiVincenzo, "Two-bit gates are universal for quantum computation," Phys. Rev. A **51**, 1015 (1995), cond-mat/9407022.

[36] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, "Elementary gates for quantum computation," Phys. Rev. A **52**, 3457 (1995), quant-ph/9503016.

[37] K. Molmer and A. Sorensen, Phys. Rev. Lett. **82**, 1835 (1999).

[38] D. W. Leung, I. L. Chuang, F. Yamaguchi, and Y. Yamamoto, "Efficient implementation of selective recoupling in heteronuclear spin systems using Hadamard matrices," quant-ph/9904100.

[39] G. Burkard, D. Loss, D.P. DiVincenzo, and J.A. Smolin, Phys. Rev. B **60**, 11404 (1999); cond-mat/9905230.

[40] G. Burkard, D. Loss, D. P. DiVincenzo, Phys. Rev. B **59**, 2070 (1999); cond-mat/9808026.

[41] D. Gottesman, "Fault-Tolerant Quantum Computation with Local Gates," J. Mod. Optics **47**, 333 (2000); quant-ph/9903099.

[42] D. Bacon, J. Kempe, D. A. Lidar, and K. B. Whaley, "Universal fault-tolerant computation on decoherence-free subspaces," quant-ph/9909058.

[43] D. P. DiVincenzo, G. Burkard, D. Loss, and E. V. Sukhorukov, "Quantum computation and spin electronics," in *Quantum Mesoscopic Phenomena and Mesoscopic Devices in Microelectronics*, eds. I. O. Kulik and R. Ellialtioglu (NATO Advanced Study Institute, Turkey, June 13-25, 1999), to be published; cond-mat/9911245.

[44] D. Gottesman and I. L. Chuang, Nature **402**, 390 (1999).

[45] D. Loss and E. V. Sukhorukov, Phys. Rev. Lett. **84**, 1035 (2000).

[46] J. I. Cirac, P. Zoller, H. J. Kimble, and H. Mabuchi, Phys. Rev. Lett. **78**, 3221 (1997) (quant-ph/9611017).

[47] S. Lloyd, Science **261**, 1569 (1993); **263**, 695 (1994).

[48] S. Benjamin, Phys. Rev. A **61**, 020301(R) (2000) (quant-ph/9909007).

[49] A. Yu. Kitaev, "Fault-tolerant quantum computation with anyons," quant-ph/9707021; see also J. Preskill, in *Introduction to Quantum Computation and Information* (eds. H.-K. Lo, S. Popescu, and T. Spiller, World Scientific, Singapore, 1998) pp. 213-269 (quant-ph/9712048).

[50] M. H. Freedman, M. Larsen, and Z. Wang, "A modular functor which is universal for quantum computation," quant-ph/0001108; M. H. Freedman, "Poly-locality in quantum computing," quant-ph/0001077; M. H. Freedman, A. Yu. Kitaev, and Z. Wang, "Simulation of topological field theories by quantum computers," quant-ph/0001071.

Refs from On temporal entropy and the complexity of computing the expectation value of local operators after a quench by Carignano, Ramos Marimón

References

[1] P. Calabrese and J. Cardy, Evolution of entanglement entropy in one-dimensional systems, Journal of Statistical Mechanics: Theory and Experiment **2005**, P04010 (2005).

[2] A. Laeuchli and C. Kollath, Spreading of correlations and entanglement after a quench in the one-dimensional Bose-Hubbard model, Journal of Statistical Mechanics: Theory and Experiment **2008**, P05018 (2008), arxiv:0803.2947 [cond-mat] .

[3] J. Dubail, Entanglement scaling of operators: A conformal field theory approach, with a glimpse of simulability of long-time dynamics in 1+1d, Journal of Physics A: Mathematical and Theoretical **50**, 234001 (2017), arxiv:1612.08630 [cond-mat, physics:hep-th, physics:quant-ph] .

[4] M. C. Bañuls, M. B. Hastings, F. Verstraete, and J. I. Cirac, Matrix Product States for Dynamical Simulation of Infinite Chains, Physical Review Letters **102**, 240603 (2009).

[5] A. Müller-Hermes, J. I. Cirac, and M. C. Bañuls, Tensor network techniques for the computation of dynamical observables in 1D quantum spin systems, New Journal of Physics **14**, 075003 (2012), arxiv:1204.5080 [cond-mat, physics:quant-ph] .

[6] M. B. Hastings and R. Mahajan, Connecting Entanglement in Time and Space: Improving the Folding Algorithm, Physical Review A **91**, 032306 (2015), arxiv:1411.7950 [cond-mat, physics:hep-th, physics:quant-ph] .

[7] A. Strathearn, P. Kirton, D. Kilda, J. Keeling, and B. W. Lovett, Efficient non-Markovian quantum dynamics using time-evolving matrix product operators, Nature Communications **9**, 3322 (2018).

[8] C. D. White, M. Zaletel, R. S. K. Mong, and G. Refael, Quantum dynamics of thermalizing systems, Physical Review B **97**, 035127 (2018), arxiv:1707.01506 [cond-mat] .

[9] T. Rakovszky, C. W. von Keyserlingk, and F. Pollmann, Dissipation-assisted operator evolution method for capturing hydrodynamic transport (2020), arxiv:2004.05177 [cond-mat] .

[10] M. Frías-Pérez and M. C. Bañuls, Light cone tensor network and time evolution, Physical Review B **106**, 115117 (2022), arxiv:2201.08402 [quant-ph] .

[11] A. Lerose, M. Sonner, and D. A. Abanin, Influence Matrix Approach to Many-Body Floquet Dynamics, Physical Review X **11**, 021040 (2021).

[12] A. Lerose, M. Sonner, and D. A. Abanin, Overcoming the entanglement barrier in quantum many-body dynamics via space-time duality, Physical Review B **107**, L060305 (2023).

[13] G. Giudice, G. Giudici, M. Sonner, J. Thoenniss, A. Lerose, D. A. Abanin, and L. Piroli, Temporal Entanglement, Quasiparticles, and the Role of Interactions, Physical Review Letters **128**, 220401 (2022).

[14] J. Thoenniss, A. Lerose, and D. A. Abanin, Nonequilibrium quantum impurity problems via matrix-product states in the temporal domain, Physical Review B **107**, 195101 (2023).

[15] E. Tirrito, N. J. Robinson, M. Lewenstein, S.-J. Ran, and L. Tagliacozzo, Characterizing the quantum field theory vacuum using temporal Matrix Product states (2022), arxiv:1810.08050 [cond-mat] .

[16] R. Feynman and F. Vernon, The theory of a general quantum system interacting with a linear dissipative system, Annals of Physics **24**, 118 (1963).

[17] M. Sonner, A. Lerose, and D. A. Abanin, Influence functional of many-body systems: Temporal entanglement and matrix-product state representation, Annals of Physics Special Issue on Philip W. Anderson, **435**, 168677 (2021).

[18] E. Ye and G. K.-L. Chan, Constructing Tensor Network Influence Functionals for General Quantum Dynamics, The Journal of Chemical Physics **155**, 044104 (2021), arxiv:2101.05466 [physics, physics:quant-ph] .

[19] T. Prosen and M. Žnidarič, Is the efficiency of classical simulations of quantum dynamics related to integrability?, Physical Review E **75**, 015202 (2007).

[20] I. Pižorn and T. Prosen, Operator space entanglement entropy in XY spin chains, Physical Review B **79**, 184416 (2009).

[21] V. Alba, J. Dubail, and M. Medenjak, Operator Entanglement in Interacting Integrable Quantum Systems: The Case of the Rule 54 Chain, Physical Review Letters **122**, 250603 (2019).

[22] B. Bertini, P. Kos, and T. Prosen, Operator Entanglement in Local Quantum Circuits I: Chaotic Dual-Unitary Circuits, SciPost Physics **8**, 067 (2020).

[23] B. Bertini, P. Kos, and T. Prosen, Operator Entanglement in Local Quantum Circuits II: Solitons in Chains of Qubits, SciPost Physics **8**, 068 (2020).

[24] L. Piroli, B. Bertini, J. I. Cirac, and T. Prosen, Exact dynamics in dual-unitary quantum circuits, Physical Review B **101**, 094304 (2020).

[25] G. Vidal, Efficient Simulation of One-Dimensional Quantum Many-Body Systems, Physical Review Letters **93**, 040502 (2004).

[26] S. R. White and A. E. Feiguin, Real-Time Evolution Using the Density Matrix Renormalization Group, Physical Review Letters **93**, 076401 (2004).

[27] S. Paeckel, T. Köhler, A. Swoboda, S. R. Manmana, U. Schollwöck, and C. Hubig, Time-evolution methods for matrix-product states, arXiv:1901.05824 [cond-mat, physics:quant-ph] (2019), arxiv:1901.05824 [cond-mat, physics:quant-ph] .

[28] M. C. Bañuls, Tensor Network Algorithms: A Route Map, Annual Review of Condensed Matter Physics **14**, 173 (2023).

[29] I. P. McCulloch, From density-matrix renormalization group to matrix product states, Journal of Statistical Mechanics: Theory and Experiment **2007**, P10014 (2007).

[30] B. Pirvu, V. Murg, J. I. Cirac, and F. Verstraete, Matrix product operator representations, New Journal of Physics **12**, 025012 (2010).

[31] Y. Nakata, T. Takayanagi, Y. Taki, K. Tamaoka, and Z. Wei, Holographic Pseudo Entropy, Physical Review D **103**, 026005 (2021), arxiv:2005.13801 [cond-mat, physics:hep-th, physics:quant-ph] .

[32] K. Doi, J. Harper, A. Mollabashi, T. Takayanagi, and Y. Taki, Pseudo Entropy in dS/CFT and Time-like Entanglement Entropy, Physical Review Letters **130**, 031601 (2023), arxiv:2210.09457 [cond-mat, physics:hep-th, physics:quant-ph] .

[33] K. Narayan, De Sitter space, extremal surfaces and "time-entanglement" (2023), arxiv:2210.12963 [hep-th] .

[34] X. Jiang, P. Wang, H. Wu, and H. Yang, Timelike entanglement entropy and $T\bar{T}$ deformation (2023), arxiv:2302.13872 [hep-th] .

[35] A. Coser, E. Tonni, and P. Calabrese, Entanglement negativity after a global quantum quench, Journal of Statistical Mechanics: Theory and Experiment **2014**, P12017 (2014).

[36] P. Calabrese, J. Cardy, and E. Tonni, Entanglement negativity in quantum field theory, Physical Review Letters **109**, 130502 (2012), arxiv:1206.3092 [cond-mat, physics:hep-th, physics:quant-ph] .

[37] G. Vidal and R. F. Werner, Computable measure of entanglement, Physical Review A **65**, 032314 (2002).

[38] P. Calabrese and J. Cardy, Entanglement and correlation functions following a local quench: A conformal field theory approach, Journal of Statistical Mechanics: Theory and Experiment **2007**, P10004 (2007).

[39] F. Verstraete and J. I. Cirac, Continuous Matrix Product States for Quantum Fields, Physical Review Letters **104**, 190405 (2010).

[40] W. Tang, F. Verstraete, and J. Haegeman, Matrix Product State Fixed Points of Non-Hermitian Transfer Matrices (2023), arxiv:2311.18733 [cond-mat, physics:quant-ph] .

[41] X. Wang and T. Xiang, Transfer-matrix density-matrix renormalization-group theory for thermodynamics of one-dimensional quantum systems, Physical Review B **56**, 5061 (1997).

[42] Y.-K. Huang, Biorthonormal transfer-matrix renormalization-group method for non-Hermitian matrices, Physical Review E **83**, 036702 (2011).

[43] M. J. Hartmann, J. Prior, S. R. Clark, and M. B. Plenio, Density Matrix Renormalization Group in the Heisenberg Picture, Physical Review Letters **102**, 057202 (2009), arxiv:0808.0666 [cond-mat, physics:quant-ph] .

[44] A. Foligno, T. Zhou, and B. Bertini, Temporal Entanglement in Chaotic Quantum Circuits, Physical Review X **13**, 041008 (2023).

[45] R. Orús and G. Vidal, Infinite time-evolving block decimation algorithm beyond unitary evolution, Physical Review B **78**, 155117 (2008).

[46] G. Evenbly, A Practical Guide to the Numerical Implementation of Tensor Networks I: Contractions, Decompositions and Gauge Freedom (2022), arxiv:2202.02138 [cond-mat, physics:quant-ph] .

From Quantum supremacy using a programmable SC processor by Google AI Quantum

References

[1] Arute, F. *et al.* Quantum supremacy using a programmable superconducting processor. *Nature* **574**, 505 (2019). URL https://doi.org/10.1038/s41586-019-1666-5

[2] Barends, R. *et al.* Superconducting quantum circuits at the surface code threshold for fault tolerance. *Nature* **508**, 500 (2014).

[3] Neill, C. *A path towards quantum supremacy with superconducting qubits*. Ph.D. thesis, University of California, Santa Barbara (2017).

[4] Yan, F. *et al.* Tunable coupling scheme for implementing high-fidelity two-qubit gates. *Phys. Rev. Applied* **10**, 054062 (2018).

[5] Chen, Y. *et al.* Qubit architecture with high coherence and fast tunable coupling. *Phys. Rev. Lett.* **113**, 220502 (2014).

[6] Neill, C. *et al.* A blueprint for demonstrating quantum supremacy with superconducting qubits. *Science* **360**, 195–199 (2018).

[7] Khezri, M., Dressel, J. & Korotkov, A. N. Qubit measurement error from coupling with a detuned neighbor in circuit QED. *Phys. Rev. A* **92**, 052306 (2015).

[8] Tucci, R. R. An introduction to Cartan's KAK decomposition for QC programmers. Preprint at https://arxiv.org/abs/quant-ph/0507171 (2005).

[9] Dunsworth, A. *High fidelity entangling gates in superconducting qubits*. Ph.D. thesis, University of California, Santa Barbara (2018).

[10] Dunsworth, A. *et al.* A method for building low loss multi-layer wiring for superconducting microwave devices. *Appl. Phys. Lett.* **112**, 063502 (2018).

[11] Rosenberg, D. *et al.* 3D integrated superconducting qubits. *npj Quantum Inf.* **3**, 42 (2017).

[12] Foxen, B. *et al.* Qubit compatible superconducting interconnects. *Quantum Sci. Tech.* **3**, 014005 (2017).

[13] Foxen, B. *et al.* High speed flux sampling for tunable superconducting qubits with an embedded cryogenic transducer. *Supercond. Sci. Technol.* **32**, 015012 (2018).

[14] Blais, A., Huang, R.-S., Wallraff, A., Girvin, S. M. & Schoelkopf, R. J. Cavity quantum electrodynamics for superconducting electrical circuits: An architecture for quantum computation. *Phys. Rev. A* **69**, 062320 (2004).

[15] Gambetta, J. *et al.* Qubit-photon interactions in a cavity: Measurement-induced dephasing and number splitting. *Phys. Rev. A* **74**, 042318 (2006).

[16] Bultink, C. C. *et al.* General method for extracting the quantum efficiency of dispersive qubit readout in circuit QED. *Appl. Phys. Lett.* **112**, 092601 (2018).

[17] Sank, D. *et al.* Measurement-induced state transitions in a superconducting qubit: Beyond the rotating wave approximation. *Phys. Rev. Lett.* **117**, 190503 (2016).

[18] Clerk, A. A., Devoret, M. H., Girvin, S. M., Marquardt, F. & Schoelkopf, R. J. Introduction to quantum noise, measurement, and amplification. *Rev. Mod. Phys.* **82**, 1155–1208 (2010).

[19] Caves, C. M. Quantum limits on noise in linear amplifiers. *Phys. Rev. D* **26**, 1817–1839 (1982).

[20] Mutus, J. Y. *et al.* Strong environmental coupling in a Josephson parametric amplifier. *Appl. Phys. Lett.* **104**, 263513 (2014).

[21] Ryan, C. A. *et al.* Tomography via correlation of noisy measurement records. *Phys. Rev. A* **91**, 022118 (2015).

[22] Jeffrey, E. *et al.* Fast accurate state measurement with superconducting qubits. *Phys. Rev. Lett.* **112**, 190504 (2014).

[23] Sank, D. What is the connection between analog signal to noise ratio and signal to noise ratio in the IQ plane in a quadrature demodulation system? Signal Processing Stack Exchange. URL https://dsp.stackexchange.com/questions/24372 (2015).

[24] Reed, M. D. *et al.* Fast reset and suppressing spontaneous emission of a superconducting qubit. *Appl. Phys. Lett.* **96**, 203110 (2010).

[25] Sete, E. A., Martinis, J. M. & Korotkov, A. N. Quantum theory of a bandpass purcell filter for qubit readout. *Phys. Rev. A* **92**, 012325 (2015).

[26] Chen, Y. *et al.* Multiplexed dispersive readout of superconducting phase qubits. *Appl. Phys. Lett.* **101**, 182601 (2012).

[27] Boixo, S. *et al.* Characterizing quantum supremacy in near-term devices. *Nat. Phys.* **14**, 595 (2018).

[28] Wootters, W. K. Random quantum states. *Found. Phys.* **20**, 1365–1378 (1990).

[29] Emerson, J., Livine, E. & Lloyd, S. Convergence conditions for random quantum circuits. *Phys. Rev. A* **72**, 060302 (2005).

[30] Aaronson, S. & Chen, L. Complexity-theoretic foundations of quantum supremacy experiments. In *32nd Computational Complexity Conference (CCC 2017)* (2017).

[31] Magesan, E., Gambetta, J. M. & Emerson, J. Characterizing quantum gates via randomized benchmarking. *Phys. Rev. A* **85** (2012).

[32] Magesan, E., Gambetta, J. M. & Emerson, J. Robust randomized benchmarking of quantum processes. *Phys. Rev. Lett.* **106** (2011).

[33] Popescu, S., Short, A. J. & Winter, A. Entanglement and the foundations of statistical mechanics. *Nat. Phys.* **2**, 754 (2006).

[34] Bremner, M. J., Mora, C. & Winter, A. Are random pure states useful for quantum computation? *Phys. Rev. Lett.* **102**, 190502 (2009).

[35] Gross, D., Flammia, S. T. & Eisert, J. Most quantum states are too entangled to be useful as computational resources. *Phys. Rev. Lett.* **102**, 190501 (2009).

[36] McClean, J. R., Boixo, S., Smelyanskiy, V. N., Babbush, R. & Neven, H. Barren plateaus in quantum neural network training landscapes. *Nat. Comm.* **9**, 4812 (2018).

[37] Ledoux, M. *The concentration of measure phenomenon.* 89 (American Mathematical Society, 2005).

[38] Markov, I. L., Fatima, A., Isakov, S. V. & Boixo, S. Quantum supremacy is both closer and farther than it appears. Preprint at https://arxiv.org/pdf/1807.10749 (2018).

[39] Cross, A. W., Bishop, L. S., Sheldon, S., Nation, P. D. & Gambetta, J. M. Validating quantum computers using randomized model circuits. *Phys. Rev. A* **100**, 032328 (2019).

[40] Kelly, J., O'Malley, P., Neeley, M., Neven, H. & Martinis, J. M. Physical qubit calibration on a directed acyclic graph. Preprint at https://arXiv.org/abs/1803.03226 (2019).

[41] Wallraff, A. *et al.* Strong coupling of a single photon to a superconducting qubit using circuit quantum electrodynamics. *Nature* **431**, 162 (2004).

[42] Chen, Z. *Metrology of quantum control and measurement in superconducting qubits*. Ph.D. thesis, University of California, Santa Barbara (2018).

[43] Chen, Z. *et al.* Measuring and suppressing quantum state leakage in a superconducting qubit. *Phys. Rev. Lett.* **116**, 020501 (2016).

[44] Klimov, P. V. *et al.* Fluctuations of energy-relaxation times in superconducting qubits. *Phys. Rev. Lett.* **121**, 090502 (2018).

[45] Kelly, J. *et al.* Optimal quantum control using randomized benchmarking. *Phys. Rev. Lett.* **112**, 240504 (2014).

[46] Bialczak, R. C. *et al.* Quantum process tomography of a universal entangling gate implemented with Josephson phase qubits. *Nat. Phys.* **6**, 409 (2010).

[47] Martinis, J. M. & Geller, M. R. Fast adiabatic qubit gates using only σ_z control. *Phys. Rev. A* **90**, 022307 (2014).

[48] DiCarlo, L. *et al.* Demonstration of two-qubit algorithms with a superconducting quantum processor. *Nature* **460**, 240 (2009).

[49] Kivlichan, I. D. *et al.* Quantum simulation of electronic structure with linear depth and connectivity. *Phys. Rev. Lett.* **120**, 110501 (2018).

[50] Villalonga, B. *et al.* A flexible high-performance simulator for the verification and benchmarking of quantum circuits implemented on real hardware. *npj Quantum Information* **5**, 1 (2019).

[51] Wallman, J., Granade, C., Harper, R. & Flammia, S. T. Estimating the coherence of noise. *New J. Phys.* **17**, 113020 (2015).

[52] Erhard, A. *et al.* Characterizing large-scale quantum computers via cycle benchmarking. Preprint at https://arxiv.org/pdf/1902.08543 (2019).

[53] Johnson, J. E. *et al.* Heralded state preparation in a superconducting qubit. *Phys. Rev. Lett.* **109**, 050506 (2012).

[54] Sank, D. T. *Fast, accurate state measurement in superconducting qubits*. Ph.D. thesis, University of California, Santa Barbara (2014).

[55] Experimental data repository URL https://doi.org/10.5061/dryad.k6t1rj8

[56] Babbush, R. *et al.* Low-depth quantum simulation of materials. *Phys. Rev. X* **8**, 011044 (2018).

[57] Boykin, P., Mor, T., Pulver, M., Roychowdhury, V. & Vatan, F. On universal and fault-tolerant quantum computing. *Proc. 40th Annual Symposium on Foundations of Computer Science, IEEE Computer Society Press* (1999).

[58] DiVincenzo, D. P. Two-bit gates are universal for quantum computation. *Phys. Rev. A* **51**, 1015–1022 (1995).

[59] Shor, P. W. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A* **52**, R2493(R) (1995).

[60] Knill, E. *et al.* Randomized benchmarking of quantum gates. *Phys. Rev. A* **77**, 012307 (2008).

[61] Lehmann, E. L. & Romano, J. P. *Testing Statistical Hypotheses* (Springer-Verlag New York, 2005).

[62] Jones, E., Oliphant, T., Peterson, P. *et al.* SciPy: Open source scientific tools for Python (2001). URL http://www.scipy.org/ (2016).

[63] R Core Team. *R: A Language and Environment for Statistical Computing*. R Foundation for Statistical Computing, Vienna, Austria (2017). URL https://www.R-project.org/

[64] Efron, B. Bootstrap methods: Another look at the jackknife. *Ann. Stat.* **7**, 1 (1979).

[65] Dyakonov, M. The case against quantum computing. *IEEE Spectrum* **56**, 3, 24-29 (2019).

[66] Kalai, G. The argument against quantum computers. Preprint at https://arxiv.org/pdf/1908.02499 (2019).

[67] Smelyanskiy, M., Sawaya, N. P. & Aspuru-Guzik, A. qHiPSTER: the quantum high performance software testing environment. Preprint at https://arxiv.org/pdf/1601.07195 (2016).

[68] Villalonga, B. *et al.* Establishing the quantum supremacy frontier with a 281 Pflop/s simulation. Preprint at https://arxiv.org/pdf/1905.00444 (2019).

[69] Markov, I. L. & Shi, Y. Simulating quantum computation by contracting tensor networks. *SIAM J. Comput.* **38**, 963–981 (2008).

[70] Boixo, S., Isakov, S. V., Smelyanskiy, V. N. & Neven, H. Simulation of low-depth quantum circuits as complex undirected graphical models. Preprint at https://arxiv.org/pdf/1712.05384 (2017).

[71] Lyakh, D. Tensor algebra library routines for shared memory systems. URL https://github.com/DmitryLyakh/TAL_SH (2019).

[72] Chen, J. *et al.* Classical simulation of intermediate-size quantum circuits. Preprint at https://arxiv.org/pdf/1805.01450 (2018).

[73] Guo, C. *et al.* General-purpose quantum circuit simulator with projected entangled-pair states and the quantum supremacy frontier. Preprint at https://arxiv.org/pdf/1905.08394 (2019).

[74] De Raedt, K. *et al.* Massively parallel quantum computer simulator. *Comput. Phys. Commun.* **176**, 121–136 (2007).

[75] De Raedt, H. *et al.* Massively parallel quantum computer simulator, eleven years later. *Comput. Phys. Commun.* **237**, 47–61 (2019).

[76] Krause, D. & Thörnig, P. Jureca: Modular supercomputer at Jülich supercomputing centre. *Journal of large-scale research facilities JLSRF* **4**, 132 (2018).

[77] Krause, D. Juwels: Modular tier-0/1 supercomputer at the Jülich supercomputing centre. *Journal of large-scale research facilities JLSRF* **5**, 135 (2019).

[78] Kalai, G. & Kindler, G. Gaussian noise sensitivity and bosonsampling. *arXiv:1409.3093* (2014).

[79] Bremner, M. J., Montanaro, A. & Shepherd, D. J. Achieving quantum supremacy with sparse and noisy commuting quantum computations. *Quantum* **1**, 8 (2017).

[80] Yung, M.-H. & Gao, X. Can chaotic quantum circuits maintain quantum supremacy under noise? *arXiv:1706.08913* (2017).

[81] Boixo, S., Smelyanskiy, V. N. & Neven, H. Fourier analysis of sampling from noisy chaotic quantum circuits. *arXiv:1708.01875* (2017).

[82] Nahum, A., Vijay, S. & Haah, J. Operator spreading in random unitary circuits. *Phys. Rev. X* **8**, 021014 (2018).

[83] Von Keyserlingk, C., Rakovszky, T., Pollmann, F. & Sondhi, S. L. Operator hydrodynamics, OTOCs, and entanglement growth in systems without conservation laws. *Phys. Rev. X* **8**, 021013 (2018).

[84] Gogate, V. & Dechter, R. A complete anytime algorithm for treewidth. In *Proceedings of the 20th Conference on Uncertainty in Artificial Intelligence*, 201–208 (2004).

[85] Zhang, F. *et al.* Alibaba cloud quantum development kit: Large-scale classical simulation of quantum circuits. Preprint at https://arxiv.org/pdf/1907.11217 (2019).

[86] Chen, M.-C. *et al.* Quantum teleportation-inspired algorithm for sampling large random quantum circuits. Preprint at https://arxiv.org/pdf/1901.05003 (2019).

[87] We assume 2 vCPUs per core.

[88] Koomey, J. & Naffziger, S. Energy efficiency of computing: What's next? *Electronic Design.* URL https://www.electronicdesign.com/microprocessors/ energy-efficiency-computing-what-s-next (2016).

[89] Preskill, J. Quantum computing and the entanglement frontier. *Rapporteur talk at the 25th Solvay Conference on Physics, Brussels* (2012).

[90] Aaronson, S. & Arkhipov, A. The computational complexity of linear optics. In *Proceedings of the Forty-third Annual ACM Symposium on Theory of Computing*, 333–342 (2011).

[91] Bremner, M. J., Montanaro, A. & Shepherd, D. J. Average-case complexity versus approximate simulation of commuting quantum computations. *Phys. Rev. Lett.* **117**, 080501 (2016).

[92] Bouland, A., Fefferman, B., Nirkhe, C. & Vazirani, U. On the complexity and verification of quantum random circuit sampling. *Nat. Phys.* **15**, 159 (2019).

[93] Movassagh, R. Cayley path and quantum computational supremacy: A proof of average-case #P-hardness of random circuit sampling with quantified robustness. Preprint at https://arxiv.org/pdf/1909.06210 (2019).

[94] Bremner, M. J., Jozsa, R. & Shepherd, D. J. Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy. *Proc. Royal Soc. A* **467**, 459–472 (2010).

[95] Harrow, A. W. & Montanaro, A. Quantum computational supremacy. *Nature* **549**, 203 (2017).

[96] Terhal, B. M. & DiVincenzo, D. P. Adaptive quantum computation, constant depth quantum circuits and Arthur-Merlin games. *Quant. Inf. Comp.* **4**, 134–145 (2004).

[97] Harrow, A. W. & Mehraban, S. Approximate unitary t-designs by short random quantum circuits using nearest-neighbor and long-range gates. Preprint at https://arxiv.org/pdf/1809.06957 (2018).

[98] Arora, S. & Barak, B. *Computational complexity: a modern approach* (Cambridge University Press, 2009).

[99] Huang, C., Newman, M. & Szegedy, M. Explicit lower bounds on strong quantum simulation. Preprint at https://arxiv.org/pdf/1804.10368 (2018).

[100] Dalzell, A. M., Harrow, A. W., Koh, D. E. & La Placa, R. L. How many qubits are needed for quantum computational supremacy? Preprint at https://arxiv.org/pdf/1805.05224.pdf (2018).

[101] Morimae, T. & Tamaki, S. Fine-grained quantum supremacy of the one-clean-qubit model. Preprint at https://arxiv.org/pdf/1901.01637 (2019).

[102] Aaronson, S. The equivalence of sampling and searching. *Theory of Computing Systems* **55**, 281–298 (2014).

[103] The variational distance is defined as $d_{\mathrm{VD}}(p,q) := \frac{1}{2}\sum_x |p(x) - q(x)|$ where the sum is over all output bitstrings x.

[104] Aaronson, S. Certifiable randomness from supremacy. *Manuscript in preparation.* (2019).

[105] Calabro, C., Impagliazzo, R. & Paturi, R. The complexity of satisfiability of small depth circuits. In *International Workshop on Parameterized and Exact Computation*, 75–85 (Springer, 2009).

[106] In terms of depth, the current construction gives a circuit U on n qubits of depth $n^{3k/2+5/2}$ for which it takes time $2^{(1-2/k)n}$ to estimate the transition probability to additive error $2^{-(n+1)}$, assuming a form of SETH stating that it takes time no less than $2^{(1-2/k)n}$ to solve k-SAT.

From Quantum Theory and Measurement Wheeler, Zurek

AAAS, 1961, 1970, 1980, Guide to Scientific Instruments, special numbers of Science. [Preface]
Ahmad, S.M.W. and Wigner, E. P., 1975. Invariant theoretic derivation of the connection between momentum and velocity, Nuovo Cimento 28A, 1-11. [II.2]
Aharonov, Y. and Albert, D. Z., 1980, States and observables in relativistic quantum field theories, Phys. Rev. D21,3316-3324. [II]
Aharonov, Y. and Albert, D. Z., 1981, Can we make sense out of the measurement process in relativistic quantum mechanics? Phys. Rev. D24, 359-370. [ii]
Aharonov, Y. and Bohm, D., 1961, Time in the quantum theory and the uncertainty relation for time and energy, Phys. Rev. 122, 1649-1658; reprinted here, VI.4. [VI, VI.4]
Aharonov, Y. and Vardi, M., 1980, Meaning of an individual "Feynman Path," Phys. Rev. D21, 2235-2240. [II]
Aharonov, Y., Bergmann, P. G., and Lebowitz, J. L., 1964, Time symmetry in the quantum process of measurement, Phys. Rev. 134B, 1410-1416; reprinted here, V.5. [V, V.5]
Allcock, G. R., 1969a, The time of arrival in quantum mechanics, 1. Formal considerations, Ann. Phys. 53, 253-285. [VI]
Alicock, G. R., 1969b, The time of arrival in quantum mechanics, 2. The individual measurement, Ann. Phys. 53, 286-310. [VI]
Allcock, G. R., 1969c, The time of arrival in quantum mechanics, 3. The measurement ensemble, Ann. Phys. 53, 311-348. [VI]
Alley, C. O., 1972, Apollo 11 laser ranging retro-reflector (LR^3) experiment, in Maglic, ed., 1972, pp. 127156. [III.13]
Anderson, P. W., 1972, More is different: broken symmetry and the nature of the hierarchical structure of science, Science 177, 393. [II]
Araki, H., 1980, On a characterization of the state space of quantum mcchanics, Commun. Math. Phys. (Germany), 75 , No. 1, 1-24. [II, V]
Araki, H. and Yanase, M. M., 1960, Measurement of quantum mechani-

This bibliography does not attempt to include references cited in papers photographically reproduced in the present collection. It does contain all references cited in papers freshly set in type, and also all references cited in the Preface and other introductory material, and in the section just prior to this one, the Guide to Some Further Literature. In the square bracket following each reference appears the place where it is cited: [III.2] means "cited in paper 2 of Section III"; [III] means "cited in Section IIII of Guide to Some Further Literature"; and [Refs.] typically means some edited collection or other book, one or more chapters of which are more specifically listed by author elsewhere in the bibliography. cal operators, Phys. Rev. 120, 622-

626; reprinted here, VI.2. [II.2, VI, V1.2]
Arnold, V. I. and Avez, A., 1968, Ergodic Problems of Classical Mechanics, Benjamin, New York. [V]
Aspect, A., 1975, Proposed experiment to test separable hidden-variable theories, Phys. Lett. 54A, 117-118. [III.13]
Aspect, A., 1976, Proposed experiment to test the non-separability of quantum mechanics, Phys. Rev. Dil4, 1944-1951; reprinted here, III 10. [III.10, III.13]
Aspect, A., Grangier, P., and Roger, G., 1981, Experimental tests of realistic local theories via Bell's theorem, Phys. Rev. Lett. 47, 460-463. [III]
Audi, Mi., 1973, The Inierpreiaion of Quantum Mechanics, University of Chicago Press. [II]
Ballentine, E., 1970, The statistical interpretation of quantum mechanics, Rev. Mod. Phys. 42, 358-381. [II]
Barnes, R. B. and Silverman, S., 1934, Brownian motion as a limit to measuring processes, Rev. Mod. Phys. 6, 162-192. [VI]
Bartell, L. S., 1980, Complementarity in the double-slit experiment: On simple realizable systems for observing intermediate particle-wave behavior, Phys Rev. D21, 1698-1699; reprinted here, III.12. [III.12]
Barut, A. O., ed., 1980, Foundations of Radiation Theory and Quantum Electrodynamics, Plenum, New York. [Refs.]
Bastin, T., ed., 1971, Quantum Theory and Beyond, Cambridge University Press. [II]
Bauer, E., see London, F. W.
Bekenstein, J., 1973, Black holes and entropy, Phys. Rev. D7, 2333-2346. [V]
Bekenstein, J., 1974, Generalized sec-
ond law of thermodynamics in blackhole physics, Phys. Rev. D19, 32923300. [V]
Bekenstein, J., 1975, The quantum mass spectrum of the Kerr black hole, Lett. Nuovo Cimento 11, 467-470. [V]
Bekenstein, J., 1981, Energy cost of information transfer, Phys. Rev. Lett. 40, 623-625. [VI]
Belinfante, F. J., 1973, A Survey of Hidden-Variable Theories, Pergamon, Oxford. [11.2, 111]
Belinfante, F. J., 1975, Measurements and Time Reversal in Objective Quantum Theory, Pergamon, Oxford; see page 39 for "indelible." [II, V]
Belinfante, F. J., 1978, Can individual elementary particles have individual properies?, Am. J. Phys. 4, 329336. [II]
Bell, J. S., 1964, On the Einstein Podolsky Rosen paradox, Physics 1, 195200; reprinted here, III.5 [II.2, III]
Bell, J. S., 1966, On the problem of hidden variables in quantum mechanics, Rev. Mod. Rhys. 38, 447452; reprinted here, III.4. [III]
Bell, J. S., 1971a, Introduction to the hidden variable question, in d'Espagnat, B., Foundations of Quantum Mechanics, Academic Press, New York and London. [III]
Bell, J. S., 1971b, On the hypothesis that the Schroedinger equation is exact. Contribution to the international colloquium on issues in contemporary physics and philosophy of science, and their relevance for our society, Pennsylvania State University, September 1971. [II]
Bell, J. S., 1975, On wave packet reduction in the Coleman-Hepp model, Helv. Phys. Acta 48, 93-98. [II, V]'
Bell, J. S., 1976, The theory of local beables, Epistemological Letters 9,
11; originally appeared as CERN preprint TH-2053, 1975. [III]
Bell, J. S., 1980a, Dermann's socks and the nature of reality, J. de Physique, Colloque C2, Supplement, tome 42, C2 41-62. [11i]
Bell, J. S., 1980b, De Broglie-Bohm, delayed-choice, double-slit experiment, and density matrix, Int. J. Quantum Chem.: A Symposium, 14, 155-159. [III]
Beltrametti, E. G. and Cassinelli, G., 1981, The Loyic of Quanium Mechanics, Addison-Wesley,

Reading, Mass. [Preface]
Bender, P. L., Currie, D. G., Dicke, K. H., Eckhardt, D. H., Faller, J. E., Kaula, W. M., Mulholland, J. D., Plotkin, H. H., Poultney, S. K., Silverberg, E. C., Wilkinson, D. T., Williams, J. G., and Alley, C. O., 1973, The lunar laser ranging experiment, Science 182, 229-238. [III.13]
Bennett, C. H., 1973, Logical reversibility of computation, $\bar{I}\bar{B}M\bar{J}$. Kes. Dev. 17, 525. [V, VI]
Bennett, C. H., 1982, The thermodynamics of computation-a review, presented at MIT Conference on Physics of Computation, Int. J. Theoret. Phys. 21, 905-940. [VI]
Bergi, S., Lugli, P., and Zamboni, ., 1980, Zero-point energy, Planck's Law, and the pre-history of stochastic electrodynamics, part II: Einstein and Stern's paper of 1913, Ann. Fond. L. de Broglie 5, 39-62. [III]
Berkeley, G., 1710, Treatise Concerning the Principles of Understanding (2nd ed., 1734) Dublin. [I]
Bertolini, G., Bettoni, M., Lazzarini, E., 1955, Angular correlation of scattered annihilation radiation, Nuovo Cimento 2, 661-662. [III]

Bialynicki-Birula, I., and Mycielski, J., 1976, Nonlinear wave mechanics, Ann. of Phys. (N.Y.) $\overline{100}, 62 - 93$. [11] Billingsley, P, 1965, Ergodic Theory and Information, Wiley, New York. [V] Birkoff, G. and von Neumann, J., 1936, The logic of quantum mechanics, Ann. Math. 37, reprinted in J. von Neumann, Collected Works, Vol. 4, 105-125. [II]
Bleuler. E. and Bradt, H. L., 1948, Correlation between the states of poiarization of the two quanta of annihilation radiation. Phys. Rev. 73, 1398. [III]
Bloch, E., 1930, L'ancienne et Nouvelle Thorie des Quanta, Hermann, Paris. [II.1]
ohm, D., 1951, The paradox of Einstein, Rosen and Podolsky, originally published as sections 15-19, Chapter 22 of Bohm, D., 1951, Quantum Theory, Prentice-Haji, Englewood Cliffs, N.J.; reprinted here, III.2. Bohm, D., 1952a, A suggested interpretation of the quantum theory in terms of "hidden variables": Part I, Phys. Rev. 85, 166-179, reprinted here, III.3. [II.2., III]

Bohm, D., 1952b, A suggested interpretation of the quantum theory in terms of "hidden variables": Part II, Phys. Rev. 85, 180-193, reprinted here, III.3. [II.2, III, III.3]
Bohm, D., 1953, Proof that probability density approaches $|\psi|^2$ in causal interpretation of quantum theory, Phys. Rev. 89, 458-466. [II]
Bohm, D. and Aharanov, Y., 1957, Discussion of experimental proof for the paradox of Einstein, Rosen and Podolsky, Phys. Rev. 108, 1070-1076. [II.2, III]
Bohm, D., and Aharonov, Y., 1960. Further discussion of possible experimental tests for the paradox of

Einstein, Podolsky and Rosen, Nuovo Cimento 17, 964-976. [III]
Bohm, D. and Bub, J., 1966a, A proposed solution of the measurement problem in quantum mechanics by a hidden variable theory, Rev. Mod. Phys. 38, 453-469. [II.2, III]
Bohm, D. and Bub, J., 1966b, A refutation of the proof by Jauch and Piron that hidden variables can be excluded in quantum mechanics, Rev. Mod. Phys. 38, 470-475. [II.2, III]
Bohm, D., and Hiliey, B. J., 1975, On the intuitive understanding of nonlocality as implied by quantum theory, Found. Phys. 5, 93-109. [III]
Bohm, D. and Hiley, B. J., 1976, Nonlocality and polarization correlations of annihilation quanta, Nuovo Cimento 35B, 137-144. [III]
Bohm. D. and Vigier, J.-P., 1954, Model of the causal interpretation of quantum theory in terms of a fluid with irregular fluctuations, Phys. Rev. 96, 208-216. [II.2, III]
Bohr, N., 1913a, On the constitution of atoms and molecules: Introduction and Part I-binding of electrons by positive nuclei, Phil. Mag. 26, 1-25. [II.2]
Bohr, N., 1913b, On the constitution of atoms and molecules: Part IIsystems containing only a single nucleus, Phil. Mag. 26, 476-508. [II.2]
Bohr, N., 1913c, On the constitution of atoms and molecules: Part IIIsystems containing several nuclei, Phil. Mag. 26, 857-871. [II.2]

Bohr, N., 1914, On the effect of electric and magnetic fields on spectral lines, Phil. Mag. 27, 506-524. [II.2]
Bohr, N., 1915a, On the series spectrum of hydrogen and the structure of the atom, Phil. Mag. 29, 332-335. [II.2]

Bohr, N. 1915b, On the quantum theory of radiation and the structure of the atom, Phil. Mag. 30, 394-415. [11.2]
Bohr, N., 1928, The quantum postulate and the recent development of atomic theory, Nature, 121, 580-590; reprinted here, I.4. [I.4]
Bohr, N., 1934, Atomic Theory and the Description of Nature, Cambridge University Press. [I.1]
Bohr, N., 1935a, Quantum mechanics and physical reality, Nature 121, 65; reprinted here, 1.9. [1.9]
Bohr, N., 1935h, Can quantummechanical description of physical reality be considered complete'? Phys. Rev. 48, 696-702, reprinted here, I.10. [I.10]

Bohr, N., 1939. The causality problem in atomic physics, in New Theories in Physics, International Institute of Intellectual Co-operation, Paris. [I.1] Bohr, ., 1958), Atomic Physics and Human Knowledge, Wiley, New York. [I,I.I]
Bohr, N., 1949, Discussion with Einstein on epistemological problems in atomic physics, in Schilpp, P. A., ed., 1949, 200-241; reprinted here. I.1. [III, III.13]
Bohr, N., 1963, Essays 1958-1962 on Atomic Physics and Human Knowledge, Wiley, New York. [i]
Bohr, N., Kramers, H. A., and Slater, J. C., 1924, The quantum theory of radiation, Phil. Mag. 47, 785-802. [II.2]
Bohr, N. and Rosenfeld, L., 1933, On the question of the measurability of the electromagnetic field quantities, original in German, Mat.-Fys. Medd. Dan. Vidensk. Selsk. 12, no. 8; English translation by A. Petersen, originally published in Cohen and Stachel, eds., 1979, 357-412; reprinted here, IV.2. [IV, II.2]

Bohr, N. and Rosenfeld, L., 1950, Field and charge measurements in quantum electrodynamics, Phys. Rev. 78, 794-798; reprinted here, IV.3. [II.2, IV, IV.3]
Boorse. H. A. and Motz, L., eds., 1966, The World of the Atom, Basic Books. New York. [Refs.]
Born, M. and Jordan, P, 1925, 7.ur Quantenmechanik, Z. Phys. 34, 858888; English translation, On quantum mechanics, in van der Waerden, 1967. [II.2]

Born, M., 1926, Zur Quantenmechanik der Stossvorgnge, Z. Phys. 37, 863867: reprinted in Dokumente der Naturwissenschaft, 1, 48-52, 1962; reprinted here, I.2. English translation hy I. A Wheeler and W. H. Zurek, 1981. [II.1]
Born, M., Heisenberg, W., and Jordan, P., 1926, Zur Quantenmechanik II, Z. Phys. 35, 557-615; English translation, On quantum mechanics II, in van der Waerden, 1967. [II.2]
Bothe, W. and Geiger, H., 1924, Ein Weg zur experimentellen Nachprfung der Theorie von Bohr, Kramers und Slater, Z, Phys. 26, 44. [II.2]
Boyer, T. H., 1968, Quantum electromagnetic zero-point energy of a conducting spherical shell and the Casimir model for a charged particle, Phys. Rev. 174, 1764-1776. [III]
Boyer, T. H., 1974, Van der Waals forces and zero-point energy for dielectric and permeable materials, Phys. Rev. A9, 2078–2084. [III]
Boyer, T. H., 1975, Random electrodynamics: The theory of classical electrodynamics with classical electromagnetic zero-point radiation, Phys. Rev. D11, 790-808. [III]
Boyer, T. H., 1980a, Thermal effects of acceleration through random classical radiation, Phys. Rev. D21, 21372148. [III]

Boyer, T. H., 1980b, A brief survey of stochastic electrodynamics, in Barut, 1980, pp. 49-63. [iii]

Braginsky, V. B. and Viatchanin, S. P., 1981, On the quantum-non-demolition measurement of the energy of optical quanta; preprint, Physical Dept., Moscow State University. [VI]
Braginsky, V. B. and Manukin, A. B., 1977, Measurement of Weak Forces in Physics Experiments, ed. D. H. Douglass, University of Chicago Press. [VI]
Braginsky, V. B., Vorontsov, Y. I., and Thorne, K. S., 1980, Quantum nondemolition measurements, Science 209, 547-557; reprinted here, VI.8. [VI, VI.8]
Brillouin, L., 1962, Science and Information Theory, 2nd ed., Academic Press, New York. [V]
Brittin, W. E., ed., 1966, Lectures in Theoretical Physics, vol. VIII A, Statistical Physics and Solid State Physics, University of Colorado Press, Boulder. [Refs.]
Bruno, M., d'Agostino, M., and Maroni, C., 1977, Measurement of linear polarization of positron annihilation photons, Nuovo Cimento 40B, 142152. [III]

Brush, S. G., 1966, Kinetic Theory: Vol. 2. Irreversible Processes, Pergamon, Oxford. [V]
Bub, J., 1968, The Daneri-LoingerProsperi quantum theory of measurement, Nuovo Cimento 57B, 503-520. [V]
Bub, J., 1969, What is a hidden variable theory of quantum phenomena?, Int. J. Theoret. Phys. 2, 101-123. [II.2, III]

Calkins, M. W., ed., 1929, Berkeley: Essays, Principles, Dialoys, with Selections from Other Writings, Scribner, New York; reprinted in 1957, pp. 125-126. [1]
Camphell, L. and Garnett, W., 1969, The Life of James Clerk Maxwell, Johnson Reprint Corporation, N. Y., p. 359. [II]

Casasent, D., ed., 1978, Optical Data Processing, in Vol. 23 of Topics in Applied Physics, Springer, New York. [VI]
Casati, G., Valz-Gris, F., and Guarnieri, ., 1980 , On the connection between quantization of non-integrable systems and statistical theory of spectra, Lett. Nuovo Cimento, 28, ser. 2, no. 8, 279-282. [V]
Cassirer, E., 1910, Substanzbegriff und Funktionsbegriff, Berlin; English translatio, 1923, Substnce and Function and Einstein's Theory of Relativity, Open Court, Chicago. [II.1]
Cassirer, F., 1936, Determinismus und Indeterminismus in der modernen Physik, Göteborg; English translation, 1956, Determinism and Indeterminism in Modern Physics, Yale University Press. [II.1]
Caves, C. M., 1982a, Quantum nondemolition measurements, in Meystre and Scully, eds., 1982. [VI]
Caves, C. M., 1982b, Quantum limits on noise in linear amplifiers, Phys. Rev. D., to appear. [VI]
Caves, C. M., Thorne, K. S., Drever, R.W.P., Sandberg, V. D., and Zimmermann, M., 1980, On the measurement of a weak classical force coupled to a quantum-mechanical oscillator., Rev. Mod. Phys. 52, 341-392. [VI]
Chaitin, G. J., 1975, Randomness and mathematical proof, Sci. Am. 232, No. 5, 47–52. [V]

Chaitin, G. J., 1981, Algorithmic information theory, in Encyclopedia of Statistical Sciences, S. Kotz and N. L. Johnson, eds., Wiley, New York. [V]
Chiao, R. Y., 1982, Interference and inertia: A superfluid helium interferometer using an internally porous powder and its inertial interactions, Phys. Rev. B25, 1655-1662.
[VI]
Ciauser, J. F., 1976, Experimental investigation of a polarization correlation anomaly, Phys. Rev. Lett. 36, 1223-1226. [Refs., II.2, III]
Clauser, J. F. and Horne, M. A., 1974, Experimental consequences of objective local theories, Phys. Rev. 10, 520-535. [III]
Clauser, J. F., Horne, M. A., Shimony, A., and Holt R. A., 1969, Proposed experiment to test local hidden-variable theories, Phys. Rev. Lett. 23, 880-884; reprinted here, III.6. [III, III.6, III.13]

Clauser, J. F. and Shimony, A., 1978, Bell's theorem. Experimental tests and implications Rep. Prog. Phys. 41, 1881-1927. [III]
Claverie, P. and Diner, S., 1977, Stochastic electrodynamics and quantum theory, Int. J. Quantum Chem. 12, Sun. 1, 41-82. [III]
Cohen, R. S. and Stachel, J. J., eds., 1979, Selected Papers of Lon Rosenfeld, Reidel, Dordrecht. [Refs.]
Colodny, R. G., ed., 1962, Frontiers of Science and Philosophy, University of Pittsburgh Press. [Refs.]
Comisar, G. G., 1965, Brownian-motion model of non-relativistic quantum mechanics, Phys. Rev. B138, 1332-1337. [III]
Compton, A. H. and Simon, A. W., 1925a, Measurements of the beta
rays excited by hard x-rays, Phys. Rev. 25, 107. [11.2]
Compton, A. H. and Simon, A. W., 1925b, Measurement of beta rays associated with scattered x-rays, Phys. Rev. 25, 306-313. [II.2]
Compton, A. H. and Simon, A. W., 1925c, Directed quanta of scattered x-rays, Phys. Rev. 26, 289-299. [11.2]
Cooper, L. N., 1973, A possible organization of animal memory and learning, in Lundqvist and Lundqvist, eds., 1973, pp. 252-264. [I]
Cooper, L. N., 1975, A theory for the acquisition of animal memory, in Zichichi, ed., 1975, pp. 808-839. [I]
Cooper, L. N., 1976, How possible becomes actual in the quantum theory, Proc. Am. Phil. Soc. 120, 37-45. [II]
Cooper, L. N., and Van Vechten, D., 1969, On the interpretation of measurement within the quantum theory, Am. J. Phys. 37, No. 12, 1212-1220. [II]
Corinaldesi, E., 1951, Charge fluctuations in quantum electrodynamics, Nuovo Cimento 8, 494-497. [IV]
Cornfeld, I. P., Fomin, S. V., and Sinai, Ya. G., 1981, Ergodic Theory, Springer, Berlin and New York. [V]
Currie, D. G., Steggerda, C. A., Rayner, J., and Buennagel, A., 1972, Second generation timing system for Apollo lunar laser ranging experiment, in Proceedings of the Fourth NASA and Department of Defense Precise Time and Time Interval Meeting, U.S. Government Printing Office, Washington, D.C., 41-45. [III.13]
Cutrona, L. J., 1970, Synthetic aperture radar, Chapter 23 in Skolnik, ed., 1970. [VI]
d'Abro, A., 1939, The Decline of Mechanism, Van Nostrand, New York. [I]
d'Abro, A., 1951, The Rise of the New Physics; Its Mthemacal un Rhysical Theories, Dover, New York. [I]
Daneri, A., Loinger, A., and Prosperi, G. Mi., 1902, Quantum theory of measurement and ergodicity conditions, Nucl. Phys. 33, 297-319; reprinted here, V.4. [II, V, V.4]
Daneri, A., Loinger, A. and Prosperi, G. M., 1966, Further remarks on the relations between statistical mechanics and quantum theory of measurement, Nuovo Cimento 44B, 119-128. [V]
davidson, M., 1979, A model for the stochastic origins of Schrödinger's equation, J. Math. Phys. 20, 18651869. [III]
Davies, E. B., 1976, Quantum Theory of Open Systems, Academic Press, London. [V]
Davies, P.C.W., 1974, The Physics of Time Asymmetry, University of California Press. [II]
Davis, J., and Tango, W. J., eds., High Angular Resolution Stellar Interferometry, IAU Colloquium No. 50, Chatterton Astronomy Department, School of Physics, University of Sydney, N.S.W. 2006, Australia, pp. 8-14. [Refs., III.13]
Davisson, C. and Germer, L., 1927, The scattering of electrons by a single crystal of nickel, Nature 119, 558560. [II.2]
Davydov, B., 1947, Quantum mechanics and thermodynamic irreversibility, J. Phys.

Moscow 11, 33. [II]
de Broglie, L., 1923a, Ondes et quanta, C. R. Acad. Sci. Paris 177, 517. [II.2] de Broglie, L., 1923b, Quanta de lumire, diffraction et interfrences, C. R. Acad. Sci. Paris 177, 548. [II.2]
de Broglie, L., 1923c, Les quanta, la thorie cintique des gaz et le prin-
cipe de Fermat, C. R. Acad. Sci. Paris 177, 630. [II.2]
de Broglie, L., 1924a, Thse, Masson et Cie., Paris. [II.2]
de Broglie, L., 1924b, A tentative theory of light quanta, Phil. Mag. 47, 446-458. [II.2]
de Broglie, L., 1924c, Sur la dfinition gnrale de la correspondance entre onde et mouvement, C. R. Acad. Sci. Paris 179, 39. [II.2]
de Broglie, L., 1924d, Sur un thorme de Bohr, C. R. Acad. Sci. Paris I79, 676. [II.2]
de Broglie, L., 1924e, Si l dynaique du quantum de lunire et les interfrence, C. R. Acad. Sci. Paris 179, 1029. [II.2]
de Broglie, L., 1925, Recherches sur la thorie des quanta, Ann. de Phys. 3, 22-128. [II.2]
de Broglie, L., 1926, Ondes et mouvements, Gauthier-Villars, Paris. [II.2]
de Broglie, L., 1928, La nouvelle dynamique des quanta, in Electrons et Photons -Rapports et Discussions du Cinquime Conseil de Physique tenu Bruxelles du 24 au 29 Octobre 1927 sous les Auspices de l'Institut International de Physique Solvay, Gauthier-Villars, Paris. [III]
de Broglie, L., 1930, Introduction l'tude de la Mcanique Ondulatoire, Hermann, Paris. [II.1]
de Broglie, L., 1941, Continu et discontinu en physique moderne, Michel, Paris. [II]
de Broglie, L., 1953, La physique quantique restera-t-elle indterministe?, Gauthier-Villars, Paris. [II]
de Broglie, L., 1962, New Perspectives in Physics, Basic Books, New York. [II]
Dehmelt, H., 1981, Invariant frequency ratios in electron and positron geonium spectra yield refined data on
electron structure, pp. 1-3 in D. Kleppner and F. Pipkin, cds., Atomic Physics 7, Plenum, New York. [VI] De La Pea-Auerbach, L., 1969, New formulation of stochastic theory and quantum mechanics, J. Math. Phys. I0, 1620-1630. [III]
De La Pea, L., and Cetto, A. M., 1977, Derivation of quantum mechanics from stochastic electrodynamics, *J*. Math. Phys. 18, 1612-1622. [III]
Espagnat, B., ed., 1971a, Foundations of Quantum Mechanics, Proceedings of the International School of Physics "Enrico Fermi," Course 49, Academic Press, New York and London. [II, Refs.]
d'Espagnat, B., 1971b, Conceptual Foundations of Quantum Mechanics, W. A. Benjamin, Menlo Park, Calif. (now Addison-Wesley, Reading, Mass.). [II]
d'Espagnat, B., 1979, The quantum theory and reality, Sci. Amer. 241 (Nov.), 158-181. [III, III.13]
Deutsch, D., 1981, Quantum theory as a universal physical theory; working paper, Center for Theoretical Physics, University of Texas at Austin and Department of Astrophysics, Oxford University. [II]
Deutsch, D., 1982, Is there a fundamental bound on the rate at which information can be processed? Phys. Rev. Lett. 48, 286-288. [VI]
DeWitt, B. S., 1962, The quantization of geometry, in Witten, 1962, pp. 266-381. [IV]
DeWitt, B. S., 1965, Dynamical Theory of Groups and Fields, Gordon and Breach, New York. [IV]
DeWitt, B. S., 1970, Quantum mechanics and reality, Physics Today 23, . Sept., 30-35. [II, II.2, IV]
DeWitt, B. S. and Graham, R. N., 1971, Resource letter IQM-1 on the
interpretation of quantum mechanics, Am. J. Phys. 39, 724-738. [Preface]
DeWitt, B. S, and Graham, N., eds., 1973, The Many-Worlds Interpretation of Quantum Mechanics, Princeton University Press. [II, II.2]

Dias, T. and Shimony, A., 1981, A critique of Jaynes' maximum entropy principle, Adv. Appl. Math. 2, 172211. [V]

Dicke, R. H., 1981, Interaction-free quantum measurements, a paradiox?, Am. J. Phys. 49, 925-929. [II]

Dirac, P.A.M., 1927, The physical interpretation of quantum dynamics, Proc. Roy. Soc. A113, 621-641. [II.1]

Dirac, P.A.M., 1971, The Development of Quantum Theory, Gordon and Breach, New York. [I]

Dontsov, Y. P. and Baz', A. I., 1967, Interference experiments with staiistically independent pinotons, Souv. Phys.-JETP 25, 1-5. [II]

Dushman, S., 1938, The Elements of Quantum Mechanics, Wiley, New York, and Chapman and Hall, London. [II.1]

Edwards, P., ed., 1972, The Encyclopedia of Philosophy, Macmillan Publishing Co. and The Free Press, New York. [Refs.]

Einstein, A., 1905, ber cinen dic Enzeugung und Verwandlung des Lichtes betreffenden heuristischen Gesichtspunkt, Ann. Physik 17, 132148; English translation, On a heuristic point of view about the creation and conversion of light, in Boorse and Motz, 1966, and in ter Haar, 1967. [II.2]

Einstein, A., 1916a, Quantentheorie des Strahlung, Physik. Gesell. Zurich Mitt. 16, 47-62; reprinted in Phys. Z. 19, 121-128, 1917; English translation, Quantum theory of radiation, in van der Waerden, 1967. [II.2]

Einstein, A., 1916b, Strahlungsemission und Absorption nach der Quantentheorie, Vern. D. Phys. Ges. 18, 318-323. [II.2]

Einstein, A., 1917a, Zur Quantentheorie der Strahlung, Phys. Z. 18, 121; English translation, On the quantum theory of radiation, in van der Waerden, 1967. [II.2]

Einstcin, A., 1917b, Zum Quantensatz von Sommerfeld und Epstein, Verh. D. Phys. Ges. 19, 82-92. [V]

Einsiein, A., 1920, Lettei t Niels Blii, May 2, 1920.

Einstein, A., 1936, Physics and reality, J. Frankiin Inst. 221, 349-382. [1.1.] Einstein, A., 1949, Autobiographical notes, in Schilpp, 1949, pp. 2-95. Einstein, A., before 1953, as quoted in Rosenfeld, 1953; reprinted in Cohen and Stachel, eds., 1979, p. 469. [I.1] Einstein, A. and Ehrenfest, P., 1922, Quantentheoretische Bemerkungen zum Experiment von Stern und Gerlach, Z. Phys. 11, 31-34. [II.2]

Einstein, . and Hopf., L., 1910, 2. ber einen Satz der Wahrscheinlichkeitsrechnung und seine Anwendung in der Strahlungstheorie, Ann. de Phys. 33, 1096-1105. [III]

Einstein, A. and Infeld, L., 1939, The Evolution of Physics: The Growth of Ideas from Early Concepts to Relativity and Quanta, Simon and Schuster, New York, [I]

Einstein, A., Podolsky, B., and Rosen, W., 1935, Can quantum mechanical description of physical reality be considered complete?, Phys. Rev. 47, 777-780; reprinted here, I.8. [III, I.8]

Einstein, A. and Stern, O., 1913, Einige Argumente fr die Annahme einer molekularen Agitation beim absoluten Nullpunkt, Ann. Physik 40, 551560; English translation in Bergia, Lugli, and Zamboni, 1980. [III]

Einstein, A., Tolman, R. C., and Podolsky, B., 1931, Knowledge of past and future in quantum mechanics, Phys. Rev. 37, 780-781; reprinted here, I. 7 [III]

Eisenbud, L., 1971, The Concepiual Foundations of Quantum Mechanics, Van Nostrand-Reinhold, New York. [1]

Emch, G. G., 1972, On quantum measuring processes, Helv. Phys. Acta, 45, 1049-1056. [II]

Epstein, P. S., 1945, The reality problem in quantum mechanics, Am. J. Phys. 13, 127-136. [II]

Evereti, H., III, 1957, Relative state formulation of quantum mechanics, Rev. Mod. Phys. 29,

454-462; reprinted here, II.3. [II, II.2, II.3]
Faraci, G., Gutkowski, D., Notarrigo, S., and Penisi, A. R., 1974, An experimental test of the EPR paradox, Lett. Nuovo Cimento 9, 607611. [II.2, III, III.13]
Farinelli, U. and Gamba, A., 1956, Entropy in quantum mechanics, Nuovo Cimento 3, 1033. [V]
Farnett, E. C., et. al., 1970, Pulse compression radar, Chapter 20 in Skolnik, ed., 1970. [VI]
Farquhar, I. E. and Landsberg, P. T., 1957, On the quantum statistical ergodic and H-theorems, Proc. Roy. Soc. A239, 134. [V]
Fnyes, I., 1952, Eine wahrscheinlich-keits-theoretische Begrndung und Interpretation der Quantenmechanik, Z. Phys. 132, 81-106. [III]
Fehrs, M. H. and Shimony, A., 1974, Approximate measurement in quantum mechanics, I, Phys. Rev. D9, 2317-2320. [III]
Fermi, E., 1923, Beweis, dass ein mechanisches Normalsystem im allgemeinen quasi-ergodisch ist, Phys. Z. 24, 261-264. [V]

Feyerabend, P. K., 1957, On the quantum theory of measurement, in Körnet and Piyce, 1957, pp. 121-130. [V]
Feyerabend, P. K., 1962, Problems of microphysics, in Colodny, ed., 1962. [i, ii]
Feynman, R. P., 1951, The concept of probability in quantum mechanics, Proceedings of the Second Berkeley
Symposium on Mathematical Statistics and Probability, University of
California Press, pp. 533-541. [II]
Fitz, M., 1955, Dei eigodensatz in dei Quantenmechanik, Helv. Phys. Acta 28, 705-715. [V]
Fiato, M.., ed., 1976, Quantum Mechanics, Determinism, Causality and Particles, Reidel, Dordrecht. [I]
Fleming, G. N., 1965, Nonlocal propperties of stable particles, Phys. Rev. I39B, 963-968. [II.2]
Follesdal, D., 1975, Meaning and expe???, ?? Gttenplain, ed., 1975, pp. 25-44. [I]
Forman, P., 1971, Weimar culture, causaiity and quantum theory 1918− 1927, Historical Studies in the Physical Sciences 3, 1-115. [II]
Forsee, A., 1963, Albert Einstein, Theoretical Physicist, Macmillan, New York.
Franck, J. and Hertz, G., 1914, ber die Eeguing der Quecksilberresonanzlinie 253.6$\mu\mu$ durch Elektronenstösse, Verh. D. Phys. Ges. 16, 512-517. [II.2]
Freedman, S. J. and Clauser, J. F., 1972, Experimental test of local hidden variable theories, Phys. Rev. Lett. 28, 938-941; reprinted here, III.7. [II.2, III, III.7, III.13]
Freedman, S. J. and Holt, R. A., 1975, Tests of local hidden-variable theories in atomic physics, Comments Atom. Molec. Phys. 5, 55-62. [III] Friedman, K. and Shimony, A., 1971,

Jaynes' maximum entropy prescription and probability theory, J. Stat. Phys., 3, 381-384. [V]
Frisch, O., 1965, Take a photon . . ., Contemp. Phys. 7, 45-53. [II]
Fry, E. S. and Thompson, R. C., 1976, Experimental test of local hiddenvariable theories, Phys. Rev. Lett. 37, 465-468; reprinted here, $\overline{111}.\overline{8}$. [III, III.8]
Fuller, R. W. and Putnam, P., 1966, On the origin of order in behavior, Gen. Sys. 11, 99-112. [I]
Furry, W. H., 1936, Note on the quan-tum-mechanical theory of measuremeni, Phys. Rev. 49, 393-399. [I]
Furry, W. H., 1966, Some aspects of the quantum theory of measurement, in Brittin, ed., 1966, pp. 1-64. [V, V.2]
Frth, R., 1933, ber einige Beziehungen zwichen klassischer Statistik und Quantenmechanik, Z. Phys. 81, 143162. [III]

Gamba, A., 1955, Thermodynamics and quantum mechanics, Nuovo Ci menio 1, 358-360. [V]

Gamow, G., 1966, Thirty Years That Shook Physics, Anchor Books, New York. [I]
Garuccio, A. and Selleri, F., 1976, Nonlocal interactions and Bell's inequality, Nuovo Cimento B36, 176-185. [III]
George, C., Prigogine, I., and Rosenfeld, L., 1972, The macroscopic level of quantum mechanics, Mat. -Fys. Medd. Dan. Vidensk. Selsk. 38, 1-44. [V]
Gerlach, W. and Stern, O., 1921, Der experimentelle Nachweis des magnetischen Moments des Silberatoms, Z. Phys. 8, 110. [II.2]

Gerlach, W. and Stern, O., 1922, Der experimentelle Nachweis der Richtungsquantelung im Magnetfeld, *Z*. Phys. 9, 349-352. [II.2]

Gleason, A. M., 1957, Measures on the closed subspaces of a Hilbert space, J. Math. and Mech. 6, 885-893. [II, II.2]

Gödel, K., 1931, ber formal unentscheidbare Stze der Principia Mathematica und verwandter Systeme I, Monatshefte fr Mathematik und Physik, 38, 173-198; English transiation by Meltzer, B., 1962, On Formally Undecidable Propositions of Principia Mathematica and Related Systems, with an introduction by R . B. Braithwaite, Basic Books, New York. [V]
Good, I. J., cd., 1961, The Scientist Speculates, Heinemann, London, and Basic Books, New York. [Refs.]
Green, H. S., 1958, Observationi in quantum mechanics, Nuovo Cimento 9, 880-889. [II, V]
Griffin, D. R., 1950, The navigation of bats, Sci, Amor. 183 (Aug.), 52-55. [VI]
Griffin, D. R., 1958, More about bat radaar, Sci. Amer. 199 (July), 40-44. [VI]
Groenewold, H. J., 1952, Information in quantum measurements, Proc. Kon. Ned. Akad. v. Wet. B55, 219227.[V]

Guttenplan, S., ed., 1975, Mind and Language, Clarendon Press, Oxford. [Refs.]
Haake, F. and Weidlich, W., 1968, A model for the measuring process in quantum theory, Z. Phys. 213, 451465. [V]

Halkias, C. C. and Alley, C. L., 1977, Amplifier, in McGraw-Hill Encyclopedia of Science and Technology, McGraw-Hill, New York. [VI]
Halverson, W. H., 1967, Phenomenalism, Chapter 22 in A Concise Introduction to Philosophy, Random House, New York, 200-208. [I]

Hanle, P. A., 1979, Indeterminism before Heisenberg: the case of Franz Exner and Erwin Schrödinger, Historical Studies in the Physical Sciences 10, 225-269. [II]
Hamaa, R. C., 1948, Polarization of annihilation radiation, Nature 102, 332. [III]

Hartshorne, C., and Weiss, P., 19311935, Collected Papers of Charles Sanders Peirce, Vol. 1, paragraphs 170, 172-175, Harvard University. [Refs.]
Haus, H. A. and Mullen, J. A., 1962, Quantum noise in linear amplifiers, Phys. Rev. 128, 2407-2413; reprinied here, VI.6. [VI]
Hawking, S. W., 1974, A variational principle for black holes, Commun. Math. Phys. (Germany) 33, No. 4, 323-334. [V]
Hawking, S. W., 1975, Particle creation by black holcs, Commuin. Math. Phys. (Germany) 43, 199-220. [V]
Hawking, S. W., 1976, Black holes and themmodyamics, Phys. Rev. Dis, 191-197. [V]
Hawking, S. W. and Israel, W., 1979, General Relativity-An Einstein Centenary Survey, Cambridge University Press. [Refs.]
Heath, P. L., 1972, Nothing, in Edwards, ed., 1972, Vol. 5, pp. 524525. [I]
Heffner, H., 1962, The fundamental noise limit of linear amplifiers, Proc. IRE 50, 1604-1608. Reprinted here, VI.5. [VI, VI.5]

Hegerfeldt, G. C., 1974, Remark on causality and particle localization, Phys. Rev. D10, 3320-3321. [II.2]
Heisenberg, W., 1925, ber quantentheoretische Umdeutung kinematischer und mechanischer Beziehungen, Z. Phys. 33, 879-893; English translation, Quantumtheoretical rein-

terpretation of kinematic and mechanical relations, in van der Wacrden, 1967, or, The interpretation of kinematic and mechanical relationships according to quantum theory, in Ludwig, 1968. [II.2].
Heisenberg, W., 1927, ber den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik, Z. Phys. 43, 172-198; reprinted in Dokumente der Naturwissenschaft 4, 9-35 (1935); English translation by J. A. Wheeler and W. II. Zurck printed here, I.3. [I.3, II.1, II.2] Heisenberg, W., 1930, The Physical Principies of the Quanium Theory, University of Chicago Press; reprinted by Dover, New York (1949, 1967). [I]
Heisenberg, W., 1967, Quantum theory and its interpretation, in Rozental, 1967, pp. 94-108. [I.1, I.3, I.4]
Helstrom, C. W., 1976, Quantum Detection and Estimation, Academic Press, New York. [VI]
Hepp, K., 1972, Quantum theory of measurement and macroscopic observables, Helv. Phys. Acta 45, 237248. [II, V]

Hereford, F., 1951, The angular correlation of photoelectrons ejected by annihilation quanta, Phys. Rev. 81, 482; see also 627-628. [111]
Hermann, A., 1979, The New Physics, Heinz Moos Verlag, Munich. [I]
Hiley, B. J., 1977, A review of Bernard d'Espagnat's "Conceptual Foundations of Quantum Mechanics," Contemp. Phys. 18, 411-414. [III]
Hoffmann, B., 1959, The Strange Story of the Quantum, Dover, New York. [I]
Hofstadter, D. R., 1979, Gödel, Escheri, Bach: An Eternal Golden Braid, Random House, New York. [V]

Holt, R. A., 1973, Atomic cascade experiments, doctoral dissertation, Harvard University, Cambridge, Mass.; available from University Microfilms, Inc., Ann Arbor, Michigan 48106. [III]
Holt, R. A. and Pipkin, F. M., 1974, Quantum mechanics vs. hidden variables: polarization correlation measurement on an atomic mercury cascade, Harvard University preprint, unpublished. [II.2]
Hooker, C. A., ed., 1975, The LogicoAlgebraic Approach to Quantum Mechanics, Reidel, Dordrecht. [II]
Hopf, E., 1937, Ergodentheorie, Springcr, Berlin. [V]
Houtappel, R.M.F., Van Dam, H., and Wigner, E. P., 1965, The conceptual basis and use of the geometric invariance principles, Rev. Mod. Phys. 37, 595-632. [II.2]
Hubel, 1978, Effects of deprivation on the visual cortex of cat and monkey, Harvey Lectures, series 72, Academic Press, New York. [I]
Hubel, D. and Wiesel, T., 1977, Functional architecture of Macaque monkey visual cortex, Ferrier Lectures, Proc. Roy. Soc. London B198, 1-59. [I]
Hume, D., 1779, Dialogues Concerning Naturai Religion, Robinson, London; 1947 reprint by Thomas Nelson, London; U.S. edition thereof, Bobbs-Merrill, Indianapolis and New York; p. 148 in latter edition [I].
Hund, F., 1974, The History of Quantum Theory, Harrap, London. [I] Hurst, G. S., Payne, M. G., Kramer, S. D., and Young, J. P., 1979, Resonance ionization spectroscopy and one-atom detection, Rev. Mod. Phys. 51, 767-819. [VI]
Husserl, E., 1900-1901, Logische Untersuchungen, 2 vols., N. Niemeyer,

Halle; English translation of 2nd edition, Logical Investigations, 1970, trans. J. N. Findlay, Humanities Press, New York and Routledge and Kegan Paul, London. [II.1]
Husserl, E., 1913, Ideen zu einer reinen Phnomenologie, Halle; English translation, Ideas: General Introduction to Pure Phenomenology, 1931, trans. W. R. Boyce, Gibson, London. [I, II.1]
Isham, C. J., Penrose, R., and Sciama, D. W., eds., 1981, Quantum Gravity 2, Oxford University Press, Oxford. [Refs.]
Jacobs, K., 1962-1963, Lecture Notes on Ergodic Theory, Vols. 1 and 2, University of Aarhus, Denmark. [V]

Jahn, R. G., ed., 1981, The Role of Consciousness in the Physical World, Westview, Boulder, Colorado. [Refs.]
Jammer, Mi., 1966, The Conceptuai Development of Quantum Mechanics, McGraw-Hill, New York. [I]
Jammer, M., 1974, The Philosophy of Quantum Mechanics, Wiley, New York. [Preface, I, II, II.2, III, V]
Jancel, R., 1955, Sur la thorie ergodique en mcanique quantique, *C. R.* Acad. Sci. Paris, 1693-1695. [V]
Janossy, L. and Naray, Z., 1957, The interference phenomena of light ai very low intensities, Acta Phys. Acad. Sci. Hung. 7, 403-424. [II]
auch, J. M., 1968, Foundations of Quantum Mechanics, Addison-Wesley, Reading, Mass. [Preface, I, II]
Jauch, J. M., 1973, Are Quanta Real? A Galilean Dialogue, Indiana University Press. [I]
auch, J. M. and Baron, J. G., 1972,
Entropy, information and Szilard's paradox, Helv. Phys. Acta 45, 220232. [V]
232. [V]
ch,
hidden variables be excluded in quantum mechanics? Helv. Phys. Acta 36, 827-837. [111]
Jauch, J. M., Wigner, E. P., and Yanase, M. M., 1967, Some comments concerning measurements in quantum mechanics, Nuovo Cimento 48B, 144151. [V]
Jaynes, E. T., 1957a, b, Information theory and statistical mechanics, Part I-Phys. Rev. 106, 620-630; Part II-Phys. Rev. 108, 171-190. [V]
Jaynes, E. T., 1979, Where do we stand on maximum entropy? in Levine and Tribus, eds., 1979, pp. 15-118. [V]
Jensen, H., Graham, L. C., Porcello, L. J., and Leith, E. N., 1977, Side looking radar, Sci. Amer. 237 (Oct.), 84-94. [VI]
Kalckar, J., 1967, Niels Bohr and his youngest disciples, in Rozental, 1967. pp. 227-239. [I, I.1]
Kalitsin, N. S., 1953, On the interaction of an electron with the fluctuating electromagnetic field of the vacuum, in Russian, Sov. Phys. -JETP 25, 407-409. [III]
Kangro, H., ed., 1972, Original Papers in Quantum Physics, trans. D. ter Haar and S. G. Brush, Taylor and Francis, London. [II.2]
Kasday, L., Experimental test of quantum predictions for widely separated photons, in d'Espagnat, ed., 1971. [III.13]
Kasday, L. R., Ullman, J., and Wu, C. S., 1970, The Einstein-PodolskyRosen argument: positron annihilation experiment, Bull. Am. Phys. Soc. 15, 586. [II.2, III]
Kasday, L. R., Ullman, J. D., and Wu, C. S., 1975, Angular correlation of Compton-scattered annihilation photons of hidden variables, Nuovo Cimento B25, 633-661. [III]
Kemble, E. C., 1937, The Fundamental
Principles of Quantum Mechanics, McGraw Hill, New York, London.
[II.1]
Kemble, E. C., 1939a, Fluctuations, thermodynamic equilibrium and entropy, Phys. Rev. 56, 1013-1023. [V] Kemble, E. C., 1939b, The quantum mechanical basis of statistical mechanics, Phys. Rev. 56, 1146-1164. [V]
Khinchin, A. I. 1957, Mathematical Foundations of Information Theory, Dover, New York. [V]
Klauder, J. R., Price, A. C., Darlington, S., and Albersheim, W. J., 1960, The theory and design of chirp radar, Bell Sys. Tech. J. 39, 809. [VI]
Klein, M. J., 1952, The ergodic theorem in quantum statistical mechanics, Phys. Rev. 87, 111-115. [V]
Klein, M. I, 1956, Entropy and the Ehrenfest urn model, Physica 22, 569-575. [V]

Klein, M. J., ed., 1959, Paul Ehrenfest. Collected Scientific Papers, North Holland, Amsterdam. [I]
Klein, M. J., 1970, Paul Ehrenfest. Volume 1: The Making of a Theoretical Physicist, North Holland, Amsterdam. [I]
Kochen, S. and Specker, E. P., 1967, The problem of hidden variables in quantum mechanics, J. Math. and Mech. 17, 59-87. [II.2]
Kocher, C. A. and Commins, E. D., 1967, Polarization correlation of photons emitted in an atomic cascade, Phys. Rev. Lett. 18, 575-577. [III]
Körner, S. and Pryce, M.H.L., eds., 1957, Observation and Interpretation in the Philosophy of Physics-With Special Reference to Quantum Mechanics, Constable and Co., London. [II, V]
Korsch, H. J. and Berry, M. V., 1981, Evolution of Wigner's phase-space
density under a nonintegrable quantum map, Physica $3D, 627$. [V]
Kracklauer, A. F., 1974, Comment on the derivation of the Schrödinger equation from Newtonian mechanics, Phys. Rev. 10, 1358-1360. [111]
Kramers, H. A., 1956, Collected Scientific Papers, North Holland, Amsterdam. [1]
Krylov, N. S., 1979, Works on the Foundations of Statistical Physics, Princeton University Press. [V]
Kuhin, T. S., 1978, Black-Body Theory and the Quantum Discontinuity, 18941912, Clarendon Press, Oxford. [ii.2]
Kuhn, T. S., Heilbron, J. L., Forman, P. L., and Allen, L., 1967, Sources for History of Quantum Physics, American Philosophical Society, Philadelphia, Pennsylvania. [Preface]
Lamb, W., 1969, An operational interpretation of nonrelativistic quantum mechanics, Physics Today 22 (April), 23-28. [Preface]
Lamehi-Rachti, Mi. and Miitiig, W., 1976, Quantum mechanics and hidden variables: A test of Bell's inequality by the measurement of the spin correlation in low-energy protonproton scattering, Phys. Rev. D14, 2543-2555; reprinted here, III.9. [II.2, III, III.O]
Landau, L. and Peierls, R., 1931, Erweiterung des Unbestimmtheitsprinzips fr die relativistiche Quantentheorie, Z. Phys., 69, 56; English translation by D. ter Haar, ed., 1965, Extension of the uncertainty principle to relativistic quantum theory, Collected Papers of L. D. Landau, Gordon and Breach, New York, 40-51. Reprinted here, IV.1. [IV, IV.1]
Landauer, R., 1961, Irreversibility and heat generation in the computing
process, IBM J. Res. Dev. 5, 183-191. [V]
Landauer, R., 1981a, Fundamental physical limitations of the computational process, in Meijer, Mountain, and Soule, 1981. [V, VI]
Landauer, R., 1981b, Uncertainty principle and minimal energy dissipation in computers, presented at the Massachusetts Institute of Technology Conference on Physics of Computation, May 6-8, 1981, and published in Int. I. Theoret. Phys. 21, 283-297. [VI]
Land, A., 1955, Foundations of Quaniurn Theory: A Study in Continuity and Symmetry, Yale University Press. [I]
Land, ., 19000, From Dualismi to Unity in Quantum Physics, Cambridge University Press. [I]
Land, A., 1965, New Founaations of Quantum Mechanics, Cambridge University Press. [I]
Langhoff, H., 1960, Die Linearpolarisation der Vernichtungsstrahlung von Positronen, Z. Phys. 160, 186-193. [III]
Leite Lopes, J. and Paty, M., eds., 1977, Quantum Mechanics, a Half Century Later, Reidel, Dordrecht, Holland. [Refs.]
Leith, E. N., 1978, Synthetic aperture radar, in Casasent, 1978, pp. 89-117. [VI]
Levine, R. D., and Tribus, M., eds., 1979, The Maximum Entropy Formalism, A Conference held at the Massachusetts Institute of Technology on May 2-4, 1978, MIT Press, Cambridge, Mass. [Refs.] Liewer, K. M., 1979, The prototype very long base line amplitude interferometer, in Davis and Tango, eds., 1979. [III.13]

Loinger, A., 1968, Comments on a recent paper concerning the quantum theory of measurement, Nucl. Phys. A108, 245-249. [V]
London, F. W. and Bauer, E., 1939, La inorie de observaiion en mcanique quantique. (No. 775 of Actualits scientifiques et industrielles: Exposs de physique gnrale, publis sous la direction de Paul Langevin; Hermann, Paris.) English translations done independently by Abner Shimony, by J. A. Whecler and W. H. Zurek, and by J. McGrath and S. McLean McGrath; reconciled, published for the first time in the present collection, II.1. [II, II.1, II.2]
Lotze, R. H., 1874-1879, Systeme der Philosophie, 2 vols. Hirzel, Leipzig. [I]
Louisell, W. H., 1964, Radiation and Noise in Quantum Electronics, McGraw-Hill, New York. [VI]
Lders, G., 1951, ber die Zustandsnderung durch den Miessprozess, Ann. Physik 8, 322-328. [V.2]
Ludwig, G., 1953, Der messprozess, Z. Phys. 135, 483-511. [II]
Ludwig, G., 1958a,b, Zum ergodensatz und zum begriff der makroskopischen Observablen, I and II, Z. Phys. 150, 346374 and 152, 99-115. [V]
Ludwig, G., ed., 1968, Wave Mechanics, Pergamon, Oxford. [Preface, Refs.]
Ludwig, G., 1970, Deutung des Begriffs "physikalische Theorie" und axiomatische Grundlegung der Hilbertraumstruktur der Quantenmechanik durch Hauptstze des Messens, Springer, Berlin. [II]
Mach, E., 1897, Contributions to the Analysis of the Sensations, pp. 191192, trans. C. M. Williams, Open
Court, Chicago; a second German edition appeared in 1900. [I]
Machida, S. and Namiki, M. 1990a, Theory of measurement in quantum mechanics: Mechanism of reduction of wave packet I, Prog. Theor. Fhys. 63, No. 5, 1457-1473. [II,V]
Machida, S. and Namiki, M., 1980b, Theory of measurement in quantum mechanics: Mechanism of reduction of wave packet II, Prog. Theor. Phys. 63, No. 6, 1833-1847. [II,V]
Mackey, G. W., 1963, Mthematical Foundations of Quantum Mechanics, Benjamin, New York. [Preface, II, iii.2]
Maglic, B., ed., 1972, Adventures in Experimental Physics, Alpha 1972, World Science Publications, Princeton, N.J. [III. 13 references]
Margenau, H., 1963, Measurements in quantum mechanics, Ann. Phys. 23, 469-485. [V]
Marshall, T. W., 1965, Statistical electrodynamics, Proc. Camb. Phil. Soc. 6i, 537-546. [iii]
Maxwell, J. C., 1871, Theory of Heat, Longmans, London, Chapter 22. [V]
McDonald, S. W. and Kaufman, A. N., 1979, Spectrum and eigenfunctions for a Hamiltonian with stochastic trajectories, Phys. Rev. Leti. 42, 1189-1191. [V]
McGuire, J. H. and Fry, E. S., 1973, Restrictions on nonlocal hiddenvariable theory. Phys. Rev. D7, 555557. [III]
Mehra, J., 1974, The Quantum Principle: Its Interpretation and Epistemology, Reidel, Dordrecht. [I] Meijer, P. H. E., Mountain, R. D., and Soulen, R. J., Jr., eds., 1981, Sixth † International Conference on Noise in Physical Systems, NBS Spec. Publ. 614, Washington D. C. [Refs.]
Mesenheimer, K., 1979, Thesis, University of Freiburg, unpublished. [III]
Meystre, P. and Scully, M. O, 1983, Quantur Optics, Experimental Gravitation, and Measurement Theory, Plenum, New York. [II, Refs.]
Misra, B., Prigogine, I., and Courbage, M., 1979a, Lyapounov variable: entropy and measurement in quantum mechanics, Proc. Natl. Acad. Sci. U.S.A. 76, 4768-4772; reprinted here, V.. [V, V.]
Misra, B.. Prigogine, I., Courbage, M., 1979b, From deterministic dynamics to probabilistic descriptions, Physica A98, 1-26. [V]
Mittelstaedt, P., 1978, Quantum Logic. Reidel, Dordrecht [Preface, II]

Mittelstaedt, P., 1979, Quantum logic, in Toraldo di Francia, ed., 1979, pp. 264-299. [II]
Migiler, C., 1972, The Theory of Reiativity, 2nd ed., Clarendon, Oxford, pp. 176-180. [II.2]
Moser, J., 1973, Stable and Random Motions in Dynamical Systems with Special Emphasis on Celestial Dynamics, Princeton University Press and University of Tokyo Press. [V]
Mott, N. F., 1929, The wave-mechanics of α-ray tracks, Proc. Roy. Soc. London A i 20, 79-84; reprinted here, I.6. [I.6]

Mott, N. F. and Massey, H.S.W., 1965, Magnetic moment of the electron, section 2, chapter IX of The Theory of Atomic Collisions, Clarendon, Oxford, pp. 214-219. Reprinted here, VI.1. [VI, VI.1]

Moyal, J. E., 1949, Quantum mechanics as a statistical theory, Proc. Camb. Phil. Soc. 45, 99. [II]
Nagel, E. and Newman, J. R., 1958, Gödel's Proof, New York University Press. [V]

Nass, M. M and Cooper, L. N., 1975. A theory for the development of feature-detecing cells in visual cortex, Bio. Cyb. 19, 1-18. [I]
Nelson, E., 1966, Derivation of Schrodinger equation from Newtonian mechanics, Phys. Rev. 150, 1079-1085. [III]
Nielsen, J. R., ed., 1977, Niels Bohr Collected Works 4: The Periodic System (1920-1923), North Holland, Amsterdam. [I]
O'Commell, R. F. and Wigner, E. P., 1977. On the relation between momentum and velocity in elementary systems, Fihys. Lett. 6IA, 353-354. [II.2]
O'Connell, R. F. and Wigner, E. P., 1978, Position operators for systems exhibiting the special relativistic relation between momentum and velocity, Phys. Lett. 67A, 319-321. [II.2]
Ornstein, D., 1974, Ergodic Theory, Randomness and Dynamical Systems, Yale niversity Press. [V]
Ovenden, M. W. and Roy, A. E., 1973, Disseminated storage of information with sequential coding, Bull. Math. Biol. 35, 663-688. [V]
Pais, A., 1979, Einstein and the Quantum Theory, Rev. Mod. Phys. 51, 863-914. [1]
Parmenides of Elea, $\sim$ 550 b.c., quoted from his poem, Nature, section on Truth, as summarized in article "Parmenides" in Encyclopedia Britannica, Vol. 17, Chicago, 1973, p. 394 [I].
Pauli, W., 1928a, discussion in Electrons et Photons-Rapports et Discussions du Cinquime Conseil de Physique tenu Bruxelles du 24 au 29 Octobre 1927 sous les Auspices de l'Institut International de Physique

Solvay, Gauthier-Villars, Paris, pp. 280-282. [III]
Pauli, W., 1928b, ber das H-theorem vom Anwachsen der Entropie vom standpunkt der neuen Quantenmechanik, in Probleme der modernen Physik, Arnold Sommerfeld zum 60. Geburtstage, gewidmet von seinen Schulern, Hirzel, Leipzig, pp. 30-45. [V]
Pauli, W., ed., 1955, Niels Bohr and the Development of Physics, Pergamon, New York. [Rets.]
Pauli, W., 1932, Les thories quantiques du magntisme, l'electron magntique, in Le Magntisme, Rapports et Discussions du Sixime Conscil de Physique Solvay, Bruxelles, 1930, pp. 175-238; discussion, pp. 239280, Paris. [VI]
Pauli, W., ed., 1955, Niels Bohr and the Development of Physics, Mc-Graw-Hill, New York. [Refs.]
Pauli, W. and Fierz, M., 1937, ber das H-Theorem in der Quantenmechanik, Z. Phys. 106, 572-587. [V]
Pearl, J. and A. Crolotte, 1980, Storage space versus validity of answers in probabilistic question-answering systems, IEEE Trans. Inf. The. IT-26, 633-640. [V]
Peirce, C. S., 1897, in Hartshorne and Weiss, pp. 1931-1935. [ii]
Penrose, R., 1979, Singularities and time asymmetry, in Hawking and Israel, 1979, pp. 581-638. [V]
Penrose, R., 1981, Time asymmetry and quantum gravity, in Isham, Penrose, and Sciama, 1981.

[II]
Percival, I. C., 1973, Regular and irregular spectra, J. Phys. B6, L229. [V]
Peres, A., 1980, Can we undo quantum measurements?, Phys. Rev. D22, 879-883; reprinted here, V.7. [V.7]

Peres, A. and 7urek, W. H., 1982, Is quantum theory universally valid? Am. J. Phys. 50, 807-809. [Refs.] Peterson, A., 1968, Quantum Physics and the Philosophical Tradition, M.I.T. Press, Cambridge, Mass. [I.1]
Pierce, J. R., 1961, Symbols, Signals and Noise: The Nature and Process of Communication, Harper, New York. [II]
Pierce, J. R., 1978, Optical channels: practical limits with photon counting, IEEE Trans. Com. COM-26, 1819-1821; reprinted here, VI.7. [VI.7]
Picrcc, J. R., 1981a, An Introduction to Information Theory: Symbols, Signals and Noise, 2nd rev. ed., Peter Smith, Magnolia, Mass. [VI] Pierce, J. R., 1981b, unpublished letter of June 17 to J. A. Wheeler (except for its opening and closing sentences). [VI]
Pierce, J. R. and Posner, E. C., 1980, Introduction to Communication Science and Systems, Plenum Press, New York. [VI]
Pipkin, F. M., 1978, Atomic physics tests of the basic concepts in quantum mechanics, Advances in Atomic and Molecular Physics 14, 281-340. [II.2, iii]
Piron, C., 1976, Foundations of Quantum Physics, Benjamin, Reading, Mass. [I]
Planck, M., 1900a, ber eine Verbesserung der Wien'schen Spektralgleichung, Verh. D. Phys. Ges. 2, 202 204; English translation, On an improvement of Wien's equation for the spectrum, in ter Haar, 1967, and Kangro, 1972. [II.2]

Planck, M., 1900b, Zur Theorie des Gesetzes der Energieverteilung im Normalspectrum, Verh. D. Phys. Ges. 2, 237-245; English translation, On the theory of the energy distribution law of the normal spectrum, in ter Haar, 1967, and Kangro, 1972. [II.2]

Poincar, H., 1893, Le mcanisme et l'exprience, Revue de Metaphysique et de Morale, 1, 534-537; English translation in Brush, 1966, pp. 203-207. [V]
Polanyi, M. and Wigner, F.., 1925, Bildung und Zerfall von Moleklen, Z. Phys. 38, 429-434. [11.2]

Popper, K. R., 1982a, The Open Universe: An Argument for Indeterminism, ed. W. W. Bartley, III, Rowan and Littlefield, Totowa, New Jersey (uncorrected advance page proof received January 1982). [I]
Popper, K. K., 1982b, Quantum Theory and the Schism in Physics, ed. W. W. Bartley, III, Rowan and Littlefield, Totowa, New Jersey (uncorrected advance page proof received January 1982). [I].

Popper, K. R., 1983, Realism and the Aim of Science, cd. W. W. Bartley, III, Rowan and Littlefield, Totowa, New Jersey (uncorrected advance page proof received January 1982). [I].

Popper, K. R., and Eccles, J. C., 1977, The Self and Its Brain, Springer, Berlin. [I]
Price, W. C. and Chissick, S. S., 1976, The Uncertainty Principle and Foundations of Quantum Mechanics, Wiley, New York. [I]
Prigogine, I., George C., Henin, F., and Rosenfeld, L., 1973, Unified approach to dynamics and thermodynamics, Chemica Scripta 4, 5-32. [II, V]

Prosperi, G. M., 1967, Quantum theory of measurement, in Encyclopedic Dictionary of Physics, supplementary volume 2, pp 275-280, Pergamon, Oxford. [V]
Prosperi, G. M. and Scotti, A., 1959, Ergodicity theorem in quantum mechanics; evaluation of the probability of an exceptional initial condition, Nuovo Cimento 13, 1007-1012. [V]
Prosperi, G. M. and Scotti, A., 1960, Ergodicity conditions in quantum mechanics, J. Main. Phys. i,.2i8221. [V]

Pryce, M.H.L., 1948, The mass-centre in the restricted theory of relativity and its connexion with the quantum theory of elementary particles, Proc. Roy. Soc. London A195, 62-81. [II.2]

Pryce, M.H.L., and Ward, J. C., 1947, Angular correlation effects with annihilation radiation, Nature 160, 435. [III]
Pugh, G. E., 1976, On the Origin of Human Values (chapter, Human values, free will, and the conscious mind), Basic Books, New York; preprinted in Zygon, 11, 2-24, 1976. [I]
Puligandla, R., 1966, Quantum Theory: An Examination of the Copenhagen Interpretation, Sterling Publishers, New Dchi. [1]
Rankin, B., 1965, Quantum mechanical time, J. Math. Phys. 6, 1057-1071. [V]
Renninger, M., 1960, Messungen ohne Störung des "Messobjekts," Z. Phys. 158, 417-421. [II]
Reynolds, G. T., Spartalian, K., and Scarl, D. B., 1969, Interference effects produced by single photons, Nuovo Cimento 10: 61B, 355-364. [II]
Richmond, P. G., 1971, An Introduction to Piaget, Basic Books, New York. [I]
Rietdijk, C. W., 1971, On Waves, Particles and Hidden Variables: A New Approach, Van Gorcum, ssen. [III]
Robertson, H. P., 1929, The uncertainty principle, Phys. Rev. 34, 163164; reprinted here, I.5. [II.2]
Rohlin, A., 1967, Lectures on the entropy theory of measure-preserving transformations (Russian), Uspekhi Mat. Nauk 22, No. 5, 3-56; for an early survey, by the author, of part of the material covered, translated into English, see Russian Maths. Surveys 15, No. 4, 1-22, 1960. [V]
Rosenfeld, L., 1953, Strife about complementarity, Science Progress 163, 393-410; reprinted in Cohen and Stachel, 1979. [Refs.]
Rosenfeld, L., 1955, On quantum electrodynamics, in Pauli, ed., 1955, pp. 114-136. [IV.2, IV]
Rosenfeld, L., 1963, Niels Bohr's contribution to epistemology, Physics Today 16, 47-54; reprinted in Cohen and Stachel, 1979, [I.4]
Rosenfeld, L., 1965, The measuring process in quantum mechanics, Supp. Prog. Theo. Phys., Commemoration Issue for the 30th Anniversary of the Meson Theory by Dr. H. Yukawa, pp. 222-231. [V]
Rosenfeld, L., 1967, Niels Bohr in the thirties: consolidation and extension of the conception of complementarity, in Rozental, 1967, pp. 114-136. [I.8, I.9, IV]
Rosenfeld, L., 1968a, in Fundamental Problems in Elementary Particle Physics, Proceedings of the Fourteeth Solvay Conference, Interscience, New York.
Rosenfeld, L., 1968b, Questions of method in the consistency problem
of quantum mechanics, Nucl. Phys. A108, 241-244. [V]
Rosenfeld, L., 1971a, Mien and ideas in the history of atomic theory, Arch. Hist. Exact Sci. 7, 69-90; reprinted in Cohen and Stachel, 1979. [I.2, I.3, I.4]
Rosenfeld, L., 1971b, Quantum theory in 1929: recollections from the first Copenhagen conference, Rhodos, Copenhagen: reprinted in Cohen and Stachel, 1979. [VI.1]
Rosenfeid, L. and Nieisen, J. R., edis., 1972, Niels Bohr. Collected Works 1: Early Work (1905-1911), North Holland, Amsterdam. [I]
Rosenfeld, L. and Nielsen, J. R., eds., 1976, Niels Bohr. Collected Works 3: The Correspondence Principle (1918-1923), North Holland, Amsterdam. [I]
Rozental, S., ed., 1967, Niels Bohr: His life and work as seen by his friends and colleagues, North-Holland, Amsterdam. [Refs.]
Ruark, A. E. and Urey, H. C., 1930, Atoms, Molecules and Quanta, Mc-Graw-Hill, New York. [I]
Salecker, H. and Wigner, E. P., 1958, Quantum limitations of the measurement of spacetime distances, Phys. Rev. 109, 571-577. [IV]
Saivini-Plawen, V. and Mayr, E., 1978, On the evolution of photoreceptors and eyes, Evol. Biol. 10, 207-263. [I] Santos, E., 1979, Coupled harmonic oscillators in stochastic electrodynamics, Lett. Nuovo Cimento, 25, 360-364. [III]

Schilpp, P. A., 1949, Albert Einstein: Philosopher-Scientist, Library of Living Philosophers, Evanston, Illinois. Schrödinger, E., 1926, Quantisierung als Eigenwert problem, Ann. Physik 79, 361-376; English translation,

Quantization as a problem of proper values, in Schrödinger, 1928, or Quantization as an cigenvalue problem, in Ludwig, 1968. [II. 2]

Schrödinger, E., 1928, Collected Papers on Wave Mechanics, Blackic and Son, London. [II.2, Refs.]

Schrödinger, E., 1935, Die gegenwrtige Situation in der Quantenmechanik, Naturwissenschaften 23, 807-812, 823-828, and 844-849; English translation by J. D. Trimmer, 1980, The present situation in quantum mechanics: a translation of Schrödinger's "cat paradox" paper, Proc. Arri. Phil. Soc. 124, 323-338, teprinted here. I.11.

Scully, M. O. and Drhl, K., 1982, The quantum eraser: a proposed photon correlation experiment concerning observation and "delayed choice" in quantum mechanics, preprint to appear in Meystre, P. and Scully, M. O., 1983, Quantum Optics, Plenum, New York. [III]

Scribci, R. and Townes, C. H., 1960, Limits on electromagnetic amplification due to complementarity, in Townes, ed., 1960. [VI]

Shannon, C. E. and Weaver, W., 1949, The Mathematical Theory of Communication, University of Illinois Press, Urbana. [VI]

Shimony, A., 1974, Approximate measurement in quantum mechanics, II, Phys. Rev. D9, 2321-2323. [III]

Shimony, A., 1979, Proposed neutron interferometer test of some nonlinear variants of wave mechanics, Phys. Rev. A20, 394-396. [II]

Shull, C. G., Atwood, D. K., Arthur, J., and Horne, M. A., 1980, Search for a nonlinear variant of the Schrödinger equation by neutron interferometry, Phys. Rev. Lett. 44, 765768. [II]

Silverberg, E. C., 1974, Operation and performance of a lunar ranging statio, Applied Optics 13, 505-574. [III.13]

Sinai, Ya. G., 1976, Introduction to Ergodic Theory, Princeton University Press, trans. V. Scheffer from the 1973 book published by Erevan State University. [V]

Skolnik, M. I., ed., 1970, Radar Handbook, McGraw Hill, New York. [Refs.]

Snced, J. S., 1966, Vo Neuman's argument for the projection postulate, Phil. Sci. 33, 22-39. [V]

Snyder, H. S., Pasternack, S., and Hornbostel, J., 1948, Angular correlation of scattered annihilation radiation, Phys. Rev. 73, 440-448. [III]

Stapp, H. P., The Copenhagen interpretation, 1972, Am. J. Phys. 40, 1098-1116. [III]

Stapp, H. P., 1977, Are superluminal connections necessary?, Nuovo Cimenio 40B, 191-204. [III.13]

Stapp, H. P., 1981, Mind, matter and quantum mechanics, preprint LBL-12631, Lawrence Berkeley Laboratory, Berkeley, California. [III]

Steggerda, C. A., 1973, A Precision Event Timer for Lunar Ranging, Technical Report 74-038, University of Maryland Department of Physics and Astronomy, College Park, Maryland. [III.13]

Stueckelberg, E.C.G., 1952, Thorme H et unitarit de S, Helv. Phys. Acta 25, 577-580. [V]

Stueckelberg, F.C.G., 1960, Quantum theory in real Hilbert space, Helv. Phys. Acta 33, 727-752. [V]

Suppes, P., ed., 1976, Logic and Probability in Quantum Mechanics, Reidel, Dordrecht. [II]

Szilard, L., 1929, ber die Entropieverminderung in einen thermodynamischen System bei Eingriffen intelligenter Wesen, Z. Phys. 53, 840-856; English translation, 1964, On the decrease of entropy in a thermodynamic system by the intervention of intelligent beings, Behav. Sci. 9, 301-310; reprinted here, V.1. [V, V.1]

Taylor, G. I., 1909, Interference fringes with feeble light, Proc. Camb. Phil. Soc. 15,

114-115. [11]
ter Haar, D., ed., 1967, The Old Quantum Theory, Pergamon, Oxford. [II.2, Refs.]
Thomas, E. E., 1921, Lotze's Theory of Reality, Longmans Green, London. [I]
Thomson, W., 1874, The kinetic theory of the dissipation of energy, Proc. Roy. Soc. Edinburgh, 8, 325-334; reprinted in Brush, ed., 1966, pp. 176-187. [V]
Tipler, F. J., 1981, Some thoughts on the analogy between quantum mcchanics and the Austrian theory of capital; draft preprint, Center for Theoretical Physics, University of Texas, Austin and Depts. of Mathematics and Physics, Tulane University, New Orleans. [V]
Toraido di Francia, N., ed., 1979, Problems in the Foundations of Physics, Proceedings of the International School of Physics "Enrico Fermi," Course 72, North-Holland, Amsterdam. [Refs.]
Townes, C. H., 1960, Quantum Electronics, A Symposium, Columbia University Press, New York. [VI] Unruh, W. G. and Wald, R. M., 1982, Acceleration radiation and the generalized second law of thermodynamics; scheduled to appear in Phys. Rev. D25, 942-958. [VI]

Van der Waerden, B. L., ed., 1967, Sources of Quantum Mechanics, North-Hoiland, Amsterdam; paperback reprint, Dover, New York, 1968. [Preface, II.2]

Van Dyck, Jr., R. S., Ekstrom, P., and Dehmelt, H. G., 1976, Axial, magnetron and spin-cyclotron-beat frequencies measured on single electron almost at rest in frec space (geonium) Nature 262, 776-777. [VI]
Van Dyck, Jr., R. S., Schwinberg, P. B., and Dehmelt, H. G., 1981, Electron magnetic moment from geonium spectra, pp. 4-36 in $\overline{\mathbf{D}}$. Kleppner and F. Pipkin, eds., Atomic Physics 7, Plenum, New York. [VI] van Hove, L., 1955, Quantum-mechanical perturbations giving rise to a statistical transport equation, Physica 21, 517-540. [V]
van Hove, L., 1957, The approach to equilibrium in quantum statistics, Physica 23, 441-480. [V]
van Hove, L., 1959, The ergodic behaviour of quantum many-body systems, Physica 25, 268-276; reprinted here, V.3. [V, V.3]
Van Kampen, N. G., 1954, Quantum statistics of irreversible processes, Physica 20, 603-622. [V]
Van Kampen, N. G., 1958, Contespondence principle in quantum statistics, Proc. Int. Symposium on Transport Processes in Statistical Mechanics (Brussels, 1956), Interscience, New York. [V]
Vigier, J. P., 1951, Introduction gometrique de l'onde pilote en thorie unitaire affine, C. R. Acad. Sci. Paris 233, 1010-1012. [II.2, III]
Vigier, J. P., 1954, Structure des microobjets dans l'interprtation causale de la thorie des quanta, These, Paris. [II.2]

Vigier, J. P., 1956, Stucture des microobjets dans l'interprtation causale de ia thorie des quanta, GauihierVillars, Paris. [II 2, III]
Vigier, J. P., 1979, Model of quantum statistics in terms of a fluid with irregular stochastic fluctuations propagating at the velocity of light: A derivation of Nelson's equations, Lett. Nuovo Cimento 24, 265-272. [III]
Vlasov, N. A. and Dzeljepov, B. S., 1949, Puljarizaizija amigiljaizionnikh gammakvantov, Dokl. Akad. Nauk U.S.S.R. 69, 777-779. [III]
von Haye, F. ., 1948, ndividualism and Economic Order, University of Chicago Press, especially Essay 4, The use of knowledge in society. [V] von Hayek, F. A., 1975, Pure Theory of Capital, University of Chicago Press, paperback reprint. [V]
von Mises, L., 1960, Hurrian Action, 3rd revised ed., Contemporary Books, Chicago. [V]
von Neumann, J., 1927, Wahrschein-lichkeits-theoretischer Aufbau der Quantenmechanik, Göttinger Nachrichten I, No. 10, 245-272. [II.1]
von Neumann, J., 1929, Beweis des Ergodensatzes und des H-Theorems in der neuen Mechanik, Z. Phys. 57, 30-70. [II, V]

von Neumann, J., 1932, "Measurement and reversibility" and "The measuring process," chapters V and VI of Mathematische Grundlagen der Quantenmechanik, Springer, Berlin; translation into English by R. T. Beyer, 1955, Mathematical Foundations of Quantum Mechanics, Princeton University Press, pp. 347-445; reprinted here, V.2. [II, II.1, II.2, III, V, V.2]
von Neumann, J., 1958, The Computer
and the Brain, Yale University Press, pp. 60-61. [I]
on Neumann, j., 1981, Continuous geometries with a transition probability, ed. Israel Halpern, Memoirs of the American Mathematical Society 34, No. 262, November 1981.
[II]
Vonsovsky, S., 1946, Derivation of fundamental kinetic equations in quantum mechanics, J. Phys. Moscow 10, 367-376. [V]
Wannier, G. H., 1965, Quantummechanical proof of the second law; Am. J. Phys. 33, 222-225. [V]
Wax, N., ed., 1954, Selected Papers on Noise and Stochastic Processes, Dover, New York. [VI]
Weidlich, W., 1967, Problems of the quantum theory of measurement, Z. Phys. 205, No. 3, 199-220. [V] Weidlich, W. and Haake, F., 1969, On the quantumstatistical theory of the measuring process, J. Phys. Soc. Japan 26, Supplement, 231232. [V]

Weizscker, K. F. v., 1931, Ortbestimmung eines Elektrons durch ein Mikroskop, Z. Phys. 70, 114130. [III]

Weyl, H., 1927, Quantenmechanik und Gruppentheorie, Z. Phys. 46, 1-46. [11.2]
Wheeler, J. A., 1946, Polyelectrons, Ann. N.Y. Acad. Sci. 48, 219-238; excerpt reprinted here, III.1. [II.2, III, III.1]
Wheeler, J. A., 1957, Assessment of Everett's "relative state" formulation of quantum theory, Rev. Mod. Phys. 29, No. 3, 463-465. [II, II.2]
Wheeler, J. A., 1977, Include the observer in the wave function? in Leite Lopes and Paty, eds., 1977, pp. 1-18. [II, II.2, III.13]

Wheeler, J. A., 1978, The "past" and the "delayed-choice" double-slit experimeni, in A. R. Mariow, ed., 1978, Mathematical Foundations of Quantum Theory, Academic Press, New York. [IIII, IIII.13]
Wheeler, J. A. 1979, Frontiers of time, in Toraldo di Francia, ed., 1979, pp. 395-497. [I.13, II, III.13]
Wheeler, J. A., 1980, Bcyond the black hole, in Woolf, ed., 1980, pp. 341375. [I.13, II]

Whecler, J. A., 1981a, Delayed-choice experiments and the Bohr-Einstein dialog, in The American Philosophicai Society and The Royal Society: Papers read at a meeting, June 5, 1980, American Philosophical Society, Philadelphia. [I, I.13, II]
Wheeler, J. A., 1981b, This participatory universe, in Overbye, D., 1981, Messenger at the gates of time, Science '81, 2, o. 5, 60-607; lasi paragraph reprinted here, I.13.
Wheeler, J. A., 1981c, Not consciousness, but the distinction between the probe and the probed, as central to the elemental quantum act of observation, in Jahn, ed., 1981, pp. 87-111. [I, II]
Wheeler, J. A., 1979-1981, Law without law, excerpts reprinted here as section I. 13 appeared in Wheeler, 1981a, 1979, 1980, 1981b. [I.13, II]
Whittaker, E. T., 1953, History of the Theories of Aether and Electricity, 1900-1926, Nelson, London. [I]
Whitten-Wolfe, B. and Emch, G. G., 1976, A mechanical quantum measuring process, Helv. Phys. Acta, 49, 45-55. [II]
Whyte, L. L., 1974, The Universe of Experience, Harper and Row, New York. [II]

Wickes, W. C., Alley, C. O., and Jakubowicz, O., 1981, A delayedchoice quantum mechanics experiment, University of Maryland working paper; reprinted here, III.13. [III.13]
Wightman, A. S., 1962, On the localizability of quantum mechanical systems, Rev. Mod. Phys.

34, 845-872. [II.2]
Wigner, E. P., 1952, Die Messung quantenmechanischer Operatoren, Z. Phys. 133, 101-108. [11.2]

Wigner, F. P., 1959, Group Theory and Its Applications to the Quantum Mechanics of Atomic Spectra, Academic Press, New York. [II.2]
Wigner, E. P., 1961, Remarks on the mind-body question, in Good, 1961, pp. 284-302; reprinted in Wigner, 1967, pp. 171-184, from which this paper is reprinted here, I.12. [I.12, ii]
Wigner, F. P., 1963, The problem of measurement, Am. J. Phys. 31, 6-15; reprinted here II.4. [II, II.2, II.4]
Wigner, E. P., 1967, Symmetries and Reflections, Indiana University Press. [I.12, Refs.]
Wigncr, E. P., 1969, Are we machines?, Proc. Amer. Phil. Soc. 113, 95-101. [I]
Wigner, E. P., 1971, The philosophical problem, in d'Espagnat, ed., 1971, pp. 1-3. [I]
Wigner, E. P., 1972, On the timeenergy uncertainty relation, pp. 237247 in A. Salam and E. P. Wigner, eds., Aspects of Quantum Theory, Cambridge University Press, 1972. [VI]
Wigner, E. P., 1976, Interpretation of quantum mechanics, mimeographed notes of E. P. Wigner, revised and printed here for the first time, II.2. [II, II.2, VI]

Williams, J. G., Dicke, R. H., Bender, P. L., Alley, C. O., Carter, W. E., Crie, D. G., Eckhardi, D. H., Faller, J. F., Kaula, W. M., Mulholland, J. D., Plotkin, H. H., Poultney, S. K., Shelas, P. J., Siiverberg, E. C., Sinclair, W. S., Slade, M. A., and Wilkinson, D. T., 1976, New test of the equivalence principle from lunar laser ranging, Phys. Rev. Lett. 36, 551-554. [III.13]
Wilson, A. R., Lowe, J., and Butt, D. K., 1976, Measurement of the relative planes of polarization of annihilation quanta as a function of separation distance, J. Phys. G2, 613-624. [III]
Witten, L., 1962, Gravitation, Wiley, New York. [Refs.]
Woolf, H., ed., 1980, Some Strangeness in the Proportion: A Centennial Symposium to Celebrate the Achievements of Alberi Einsiein, AddisonWesley, Reading, Mass. [Refs.]
Wootters, W. K., 1980, The acquisition of information from quantum measurements, Ph.D. dissertation, University of Texas at Austin. [V]
Wootters, W. K., 1981, Statistical distribution and Hilbert space, Phys. Rev. 23, 357-362. [V]
Wootters, W. K. and Zurek, W. II., 1979, Complementanty in the double-slit experiment: quantum non-separability and a quantitative statement of Bohr's principle, Phys. Rev. D19, 473-484; reprinted here, III.11. [III.13]

Wu, C. S. and Shaknov, I., 1950, The angular correlation of scattered annihilation radiation, Phys. Rev. 77, 136. [II.2, III]

Yanase, M. M., 1961, Optimal mea-
suring apparatus, Phys. Rev. 123, 666-668; reprinted here, VI.3. [II.2, Vi, Vi.3]
Yourgrau, W. and van der Merve, A., eds., 1971, Perspectives in Quantum Theory, Essays in Honor of Alfred Land, M.I.T. Press, Cambridge, Mass. [I]
Zeh, H. D., 1970, On the interpretation of measurement in quantum theory, Found. Phys. 1, 69-76; reprinted here, II.5. [II.5]
Zen, H. D., 1971, On the irreversibility of time and observation in quantum theory, in d'Espagnat, ed., 1971, pp. 263-273. [11]
Zeh, H. D., 1975, Connections between quantum theory, thermodynamics, cosmology and subjective perception, paper presented at Fourth International Conference on the Unity of Sciences, New York. [II]
Zichichi, A., ed., 1975, Lepton and Hadron Structure, 1974 International School of Subnuclear Physics, Erice, Trapani, Sicily, 14-21 July. [Refs.]
Zurek, W. H., 1981, Pointer basis of quantum apparatus: Into what mixture does the wave packet collapse? Phys. Rev. D24, 1516-1525. [II, V]
Zurck, W. H., 1982a, Information transfer in quantum measurements: Irreversibility and

amplification, California Institute of Technology preprint; to appear in Meystre and Scully, 1983. [II]
Zurek, W. H., 1982b, Environmentinduced superselection rules, California Institute of Technology preprint, to appear in Phys. Rev. D. [II, V]

Literature from Amosov's lectures

1. Амосов Г.Г., Коренной Я.А., Манъко В.И. О вычислении средних значений квантовых наблюдаемых в представлении оптической томографии // ТМФ. 2012. Т. 171. С. 475-482.

2. Амосов Г.Г. Оценка выходной энтропии тензорного произведения двух квантовых каналов // ТМФ. 2015. Т. 182, № 3. С. 453-464.

3. Бройер Х.-П., Петруччионе Ф. Теория открытых квантовых систем. Москва-Ижевск : РХД, 2010.

4. Вальд А. Статистические решающие функции // Позиционные игры. Москва: Наука, 1967.

5. Гохберг И.Ц., Крейн М.А. Введение в теорию линейных несамосопряженных операторов в гильбертовом пространстве. Москва: Наука, 1965.

6. Лидский В.Б. Несамосопряженные операторы, имеющие след // ДАН. 1959. Т. 125, № 3. С. 485-488.

7. Макки Дж. Лекции по математическим основам квантовой механики. Москва: Мир, 1965.

8. Наймарк М.А. Положительно-определенные операторные функции на коммутативной группе // Изв. АН СССР. Серия: математика. 1943. Т. 7, вып. 5. С. 237-244.

9. фон Нейман И. Математические основания квантовой механики. Москва: Наука, 1964.

10. Рид М., Саймон Б. Методы современной математической физики. Т. 1. Функциональный анализ. Москва: Мир, 1977.

11. Рид М., Саймон Б. Методы современной математической физики. Т. 2. Гармонический анализ. Самосопряженность. Москва: Мир, 1978.

12. Хида Т. Броуновское движение. Москва: Наука, 1987.

13. Холево А.С. Вероятностные и статистические аспекты квантовой теории Москва: Наука, 1980.

14. Холево А.С. Каналы, разрушающие сцепленность, в бесконечных размерностях // Пробл. передачи информ. 2008. Т. 44, вып. 3. С. 3-18.

15. Холево А.С. Квантовые системы, каналы, информация. Москва: МЦНМО, 2010.

16. Холево А.С. Математические основы квантовой информатики // Лекц. курсы НОЦ. 2018. Вып. 30. С. 3-117. Москва : МИАН, 2018.

17. Amosov G.G. On tomographic representation on the plane of the space of Schwartz operators and its dual // Lobachevskii J. Math. 2017. V. 38. P. 595-599.

18. Amosov G.G., Filippov S.N. Spectral properties of reduced fermionic density operators and parity superselection rule // Quantum Inf. Process. 2017. V. 16. P. 16.

19. Amosov G.G., Mokeev A.S. On non-commutative operator graphs generated by covariant resolutions of identity // Quantum Inf. Process. 2018. V. 17. P. 11 .

20. Amosov G.G., Mokeev A.S. On non-commutative operator graphs generated by reducible unitary representation of the Heisenberg-Weyl group // Internat. J. Theor. Phys. 2018. doi: 10.1007/s10773-018-3963-4, URL: https://arxiv.org/abs/1812.02515

21. Bertrand J., Bertrand P. A tomographic approach to Wigner's function // Foundations of Physics. 1987. V. 17. P. 397-405.

22. Choi M.D., Effros E.G. Injectivity and operator spaces // J. Funct. Anal. 1977. V. 24. P. 156-209.

23. Cirel'son B.S. Quantum generalizations of Bell's inequality // Lett. Math. Phys. 1980. V. 4, N 2. P. 93-100.

24. Cahill K.E., Glauber R.G. Density operators and quasiprobability distributions // Physical Review. 1969. V. 177, N 5. P. 1882-1902.

25. D'Ariano G.M., Maccone L., Paris M.G.A. Quarum of observables for universal quantum estimation // J. Phys. A: Math. and General. 2001. V. 34, N 1. P. 93-104.

26. Duan R. Super-Activation of Zero-Error Capacity of Noisy Quantum Channels // arXiv.org. 2009. URL: https://arxiv.org/abs/0906.2527

27. Duan R., Severini S., Winter A. Zero-error communication via quantum channels, noncommutative graphs and a quantum Lovasz theta function // IEEE Trans. Inf. Theory. 2013. V. 59. P. 1164-1174.

28. Filippov S.N., Man'ko V.I. Spin tomography and star-product kernel for qubits and qutrits // J. Russ. Laser Res. 2009. V. 30. P. 129-145.

29. Filippov S.N., Man'ko V.I. Symmetric informationally complete positive operator valued measure and probability representation of quantum mechanics // J. Russ. Laser Res. 2010. V. 31. P. 211-231.

30. Glauber R.G. Coherent and incoherent states of the radiation field // Phys. Rev. 1963. V. 131, N 6. P. 2766-2788.

31. Gleason A.M. Measures on the closed subspaces of a Hilbert space // J. Math. Mech. 1957. V. 6. P. 885-893.

32. Hudson R.L., Parthasarathy K.R. Quantum Ito's formula and stochastic evolutions // Commun. Math. Phys. 1984. V. 93, N 3. P. 301-323.

33. Ibort A., Man'ko V.I., Marmo G., Simoni A., Ventriglia F. An introduction to the tomographic picture of quantum mechanics // Phys. Scr. 2009. V. 79. P. 065013 .

34. Keyl M., Kiukas J., Werner R.F. Schwartz operators // Rev. Math. Phys. 2016. V. 28, N 3. P. 1630001.

35. Kolmogoroff *A*. Grundbegriffe der Wahrscheinlichkeitsrechnung. Berlin: Springer, 1933.

36. Knill E., Laflamme R., Theory of quantum error-correcting codes // Phys. Rev. A. 1997. V. 55. P. 900-911.

37. Knill E., Laflamme R., Viola L. Theory of quantum error correction for general noise // Phys. Rev. Lett. 2000. V. 84. P. 2525-2528.

38. Manko O.V., Manko V.I., Marmo G. Alternative commutation relations, star products and tomography // J. Phys. A: Math. and General. 2002. V. 35, N 3. P. 699-720.

39. Moyal J.E. Quantum mechanics as a statistical theory // Proc. Cambridge Philos. Soc. 1949. V. 45. P. 99-124.

40. Namias *V*. The fractional order Fourier transform and its application to quantum mechanics // J. Inst. Math. Appl. 1980. V. 25. P. 241-265.

41. Pauli W. Handbuch der physik / Eds. Geiger, Scheel. V. XXIV. Part 1. 1933.

42. Rudin *W*. Real and complex analysis. McGraw-Hill, 1987.

43. Shor *P*. Scheme for reducing decoherence in quantum computer memory // Phys. Rev. A. 1995. V. 52. P. R2493(R).

44. Stinespring W.F. Positive functions on C^*-algebras // Proc. Amer. Math. Soc. 1955. V. 6. P. 211-216.

45. Sudarshan E.C.G. Equivalence of semiclassical and quantum mechanical descriptions of statistical light beams // Phys. Rev. Lett. 1963. V. 10, N 7. P. 277-279.

46. Weaver N. A "quantum" Ramsey theorem for operator systems // Proc. Amer. Math. Soc. 2017. V. 145, N 11. P. 4595-4605.

47. Wigner E.P. On the quantum correction for thermodynamic equilibrium // Phys. Rev. 1932. V. 40, N 5. P. 749-759.

From (???)

References

[1] Einarsson, T. (1990). Fractional statistics on a torus. *Phys. Rev. Lett.*, **64**(17), 1995–1998.

[2] Fradkin, E. and Shenker, S. H. (1979). Phase diagrams of lattice gauge theories with higgs fields. *Phys. Rev. D*, **19**(12), 3682–3697.

[3] Hastings, M. B. and Wen, X. G. (2005). Quasiadiabatic continuation of quantum states: The stability of topological ground-state degeneracy and emergent gauge invariance. *Phys. Rev. B*, **72**(4), 045141.

[4] Kitaev, A. (2000). Unpaired majorana fermions in quantum wires. *arXiv*, **cond-mat/0010440v2**.

[5] Kitaev, A. (2003). Fault-tolerant quantum computation by anyons. *Ann. Phys.*, **303**(1), 2 – 30.

[6] Kitaev, A. (2006). Anyons in an exactly solved model and beyond. *Ann. Phys.*, **321**(1), 2 – 111.

[7] Lieb, E. H. (1994). Flux phase of the half-filled band. *Phys. Rev. Lett.*, **73**(16), 2158–2161.

[8] Read, N. and Chakraborty, B. (1989). Statistics of the excitations of the resonating-valence-bond state. *Phys. Rev. B*, **40**(10), 7133–7140.

[9] Tupitsyn, I. S., Kitaev, A., Prokof'ev, N. V., and Stamp, P. C. E. (2008). Topological multicritical point in the toric code and 3d gauge higgs models. *arXiv*, **0804.3175v1**.

[10] Yao, H. and Kivelson, S. A. (2007). Exact chiral spin liquid with non-abelian anyons. *Phys. Rev. Lett.*, **99**(24), 247203.

From What limits the simulation of quantum computers Zhou

References

[1] John Preskill, "Quantum Computing in the NISQ era and beyond," Quantum **2**, 79 (2018).

[2] John Preskill, "Quantum computing and the entanglement frontier," arXiv e-prints , arXiv:1203.5813 (2012), arXiv:1203.5813 [quant-ph] .

[3] Sergio Boixo, Sergei V Isakov, Vadim N Smelyanskiy, Ryan Babbush, Nan Ding, Zhang Jiang, Michael J Bremner, John M Martinis, and Hartmut Neven, "Characterizing quantum supremacy in near-term devices," Nature Physics **14**, 595 (2018).

[4] Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C. Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando G. S. L. Brandao, David A. Buell, and et al., "Quantum supremacy using a programmable superconducting processor," Nature **574**, 505–510 (2019).

[5] Edwin Pednault, John A. Gunnels, Giacomo Nannicini, Lior Horesh, and Robert Wisnieff, "Leveraging secondary storage to simulate deep 54-qubit sycamore circuits," (2019), arXiv:1910.09534 .

[6] Guifré Vidal, "Efficient classical simulation of slightly entangled quantum computations," Phys. Rev. Lett. **91**, 147902 (2003).

[7] Jianxin Chen, Fang Zhang, Cupjin Huang, Michael Newman, and Yaoyun Shi, "Classical simulation of intermediate-size quantum circuits," (2018), arXiv:1805.01450 [quant-ph] .

[8] Chu Guo, Yong Liu, Min Xiong, Shichuan Xue, Xiang Fu, Anqi Huang, Xiaogang Qiang, Ping Xu, Junhua Liu, Shenggen Zheng, He-Liang Huang, Mingtang Deng, Dario Poletti, Wan-Su Bao, and Junjie Wu, "General-purpose quantum circuit simulator with projected entangled-pair states and the quantum supremacy frontier," Phys. Rev. Lett. **123**, 190501 (2019).

[9] Feng Pan, Pengfei Zhou, Sujie Li, and Pan Zhang, "Contracting arbitrary tensor networks: general approximate algorithm and applications in graphical models and quantum circuit simulations," (2019), arXiv:1912.03014 [physics.comp-ph] .

[10] Scott Aaronson and Daniel Gottesman, "Improved simulation of stabilizer circuits," Phys. Rev. A **70**, 052328 (2004).

[11] Sergio Boixo, Sergei V. Isakov, Vadim N. Smelyanskiy, and Hartmut Neven, "Simulation of low-depth quantum circuits as complex undirected graphical models," (2017), arXiv:1712.05384 [quant-ph] .

[12] Bjarni Jónsson, Bela Bauer, and Giuseppe Carleo, "Neural-network states for the classical simulation of quantum computing," (2018), arXiv:1808.05232 [quant-ph] .

[13] Ulrich Schollwöck, "The density-matrix renormalization group in the age of matrix product states," Annals of Physics **326**, 96 – 192 (2011), january 2011 Special Issue.

[14] Igor L. Markov and Yaoyun. Shi, "Simulating quantum computation by contracting tensor networks," SIAM Journal on Computing **38**, 963–981 (2008), https://doi.org/10.1137/050644756 .

[15] Akira SaiToh, "A multiprecision c++ library for matrix-product-state simulation of quantum computing: Evaluation of numerical errors," Journal of Physics: Conference Series **454**, 012064 (2013).

[16] Steven R. White, "Density matrix formulation for quantum renormalization groups," Phys. Rev. Lett. **69**, 2863–2866 (1992).

[17] Sebastian Paeckel, Thomas Köhler, Andreas Swoboda, Salvatore R. Manmana, Ulrich Schollwöck, and Claudius Hubig, "Time-evolution methods for matrix-product states," Annals of Physics **411**, 167998 (2019).

[18] F. Verstraete, V. Murg, and J.I. Cirac, "Matrix product states, projected entangled pair states, and variational renormalization group methods for quantum spin systems," Advances in Physics **57**, 143–224 (2008), https://doi.org/10.1080/14789940801912366 .

[19] G. Vidal, "Entanglement renormalization," Phys. Rev. Lett. **99**, 220405 (2007).

[20] Andrew J. Ferris and Guifre Vidal, "Perfect sampling with unitary tensor networks," Phys. Rev. B **85**, 165146 (2012).

[21] Nai-Hui Chia, András Gilyén, Tongyang Li, Han-Hsuan Lin, Ewin Tang, and Chunhao Wang, "Sampling-based sublinear low-rank matrix arithmetic framework for dequantizing quantum machine learning," arXiv e-prints , arXiv:1910.06151 (2019), arXiv:1910.06151 [cs.DS] .

[22] M.L. Mehta, *Random matrices (3e éd.), Pure and Applied Mathematics*, 3rd ed. (Elsevier, London, UK, 2004).

[23] C. W. J. Beenakker, "Random-matrix theory of quantum transport," Rev. Mod. Phys. **69**, 731–808 (1997).

[24] Xavier Waintal, "What determines the ultimate precision of a quantum computer," Phys. Rev. A **99**, 042318 (2019).

[25] Christopher Bäuerle, D Christian Glattli, Tristan Meunier, Fabien Portier, Patrice Roche, Preden Roulleau, Shintaro Takada, and Xavier Waintal, "Coherent control of single electrons: a review of current progress," Reports on Progress in Physics **81**, 056503 (2018).

[26] Michael A. Nielsen and Isaac L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*, 10th ed. (Cambridge University Press, New York, NY, USA, 2011).

[27] ITensor Library, Julia version 0.1, https://itensor.org.